Avaya Aura® Application Server 5300
Using the Provisioning Client
© 2008-2017, Avaya Inc. All Rights Reserved.

Notice

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

Documentation disclaimer

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

Link disclaimer

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

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya’s standard warranty language, as well as any information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456561010 under the link “Warranty & Product Lifecycle” or such successor site as designated by Avaya. Please note that if you acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

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

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE). THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE: HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK “Avaya Terms of Use for Hosted Services” OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACQUIRES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS “YOU” AND “END USER”), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF OF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZ ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

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

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

License types

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. “Named User”, means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya’s sole discretion, a “Named User” may be, without limitation, designated by name, corporate function (e.g., warehouse or helpdesk), physical or virtual office mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Heritage Nortel Software

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Avaya is a registered trademark of Avaya Inc.

AVAYA

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

Java is a registered trademark of Oracle and/or its affiliates.
# Contents

## Chapter 1: New in this release
- Features ........................................................................................................ 16
- Document changes since last issue .......................................................... 17
- Other changes ........................................................................................... 17

## Chapter 2: Introduction ........................................................................ 19

## Chapter 3: Provisioning Client fundamentals ........................................ 20
- Provisioning Client overview .................................................................... 20
- Software and hardware requirements and recommendations ............... 21
- Provisioning Client access ....................................................................... 22
- Provisioning Client administrative and provisioning tasks ..................... 22
- Provisioning Client layout ........................................................................ 23
  - Provisioning portlets ........................................................................... 23
- Other provisioning mechanisms ............................................................ 24

## Chapter 4: Provisioning Client security ............................................... 25
- Understanding administration and provisioning ..................................... 25
- Understanding provisioning roles and rights .......................................... 25
  - Limit access to a domain ...................................................................... 27
  - System administrator provisioning role ................................................. 27
- Provisioning rights and tasks ................................................................... 28
- Password changes .................................................................................. 32
- Password complexity rules ...................................................................... 33

## Chapter 5: Domain management ......................................................... 35
- Introduction to domains ........................................................................... 36
  - Default domain .................................................................................... 36
  - Root domain ....................................................................................... 38
  - Subdomain .......................................................................................... 38
  - Foreign domain ................................................................................... 39
  - Multisite domain ................................................................................. 39
- Domain naming conventions and restrictions ......................................... 40
- Domain password policy .......................................................................... 40
  - Password policy association with domains ........................................... 41
  - Changes to password policy domain associations ............................... 42
  - Subscriber password validation ......................................................... 42
  - Password policy validation when a subscriber moves between domains . 42
- Domain data copy .................................................................................. 43
- Nodes ....................................................................................................... 43
- Gateways ................................................................................................. 43
- Logical Entities ....................................................................................... 44
- Services management .............................................................................. 45

October 2017

Avaya Aura® Application Server 5300 Using the Provisioning Client

Comments on this document? infodev@avaya.com
## Chapter 6: Provisioning for telephony routing and translations

### Service profile and service set management

- Managing user functions .......................................................... 54
- Mailbox usage reports ................................................................. 54
- Hotline ...................................................................................... 57
  - Hotline modes ........................................................................ 57
  - Hotline indicators ................................................................... 58
- Malicious Call Trace ................................................................. 58
- TDM Message Waiting Indicator .............................................. 59
- Location management ............................................................... 59
  - Create a domain default location ............................................. 59
  - Add, modify, or delete a location ............................................. 60
  - Associate a user with a location ............................................. 60
  - Assign a default location for an Avaya IP Deskphone .............. 61
  - Foreign domains location .................................................... 62
- Service interactions ................................................................. 62
  - Interactions when assigning multiple services ....................... 62

### Telephony routing concepts

- Subdomains ............................................................................. 65
- Class of Service ........................................................................ 66
- AS 5300 Session Manager routing stages ................................. 67

### Configuring translation for one system

- Configuring translation for two systems .................................... 68

### Telephony routing terminology

- LDAP synchronization (LDAP Sync) .......................................... 47
  - LDAP synchronization functionality ...................................... 47
  - LDAP sync server configuration .......................................... 49
  - Server configuration .............................................................. 49
  - Schema configuration ........................................................... 50
  - Sync Filter option .................................................................. 52
  - User Defaults for LDAP ....................................................... 52
  - Syncing Scheduler for LDAP ............................................... 52
  - Query Test Tool for LDAP ................................................... 53
- Hybrid routing ......................................................................... 53
- User management ..................................................................... 54
  - Managing user functions ...................................................... 54
  - Converged Desktop ............................................................... 54
  - Mailbox usage reports ........................................................... 54
- SIP clients .............................................................................. 55
- Voice Mail servers provisioning ............................................. 55
  - Voice mail server types ......................................................... 56
- Service nodes configuration .................................................... 56
- Telephony routes configuration ............................................. 57
- Border Control Point 7000 Series provisioning ....................... 57
- Hotline .................................................................................... 57
- Malicious Call Trace ............................................................... 58
- TDM Message Waiting Indicator ............................................ 59
- Location management ............................................................ 59
- Service interactions ............................................................... 62
  - Interactions when assigning multiple services ....................... 62

## Contents

- Service profile and service set management .............................. 45
- Resource management ............................................................ 46
- LDAP synchronization (LDAP Sync) .......................................... 47
- LDAP synchronization functionality ...................................... 47
- LDAP sync server configuration .......................................... 49
- Server configuration .............................................................. 49
- Schema configuration ........................................................... 50
- Sync Filter option .................................................................. 52
- User Defaults for LDAP ....................................................... 52
- Syncing Scheduler for LDAP ............................................... 52
- Query Test Tool for LDAP ................................................... 53
- Hybrid routing ......................................................................... 53
- User management ..................................................................... 54
  - Managing user functions ...................................................... 54
  - Converged Desktop ............................................................... 54
  - Mailbox usage reports ........................................................... 54
- SIP clients .............................................................................. 55
- Voice Mail servers provisioning ............................................. 55
  - Voice mail server types ......................................................... 56
- Service nodes configuration .................................................... 56
- Telephony routes configuration ............................................. 57
- Border Control Point 7000 Series provisioning ....................... 57
- Hotline .................................................................................... 57
  - Hotline modes ........................................................................ 57
  - Hotline indicators .................................................................. 58
- Malicious Call Trace ............................................................... 58
- TDM Message Waiting Indicator ............................................ 59
- Location management ............................................................ 59
  - Create a domain default location ............................................. 59
  - Add, modify, or delete a location ............................................. 60
  - Associate a user with a location ............................................. 60
  - Assign a default location for an Avaya IP Deskphone .............. 61
  - Foreign domains location .................................................... 62
- Service interactions ............................................................... 62
  - Interactions when assigning multiple services ....................... 62

**Chapter 6: Provisioning for telephony routing and translations**

- Telephony routing concepts .................................................... 65
  - Subdomains ............................................................................. 65
  - Class of Service ........................................................................ 66
  - AS 5300 Session Manager routing stages ................................. 67
- Configuring translation for one system ..................................... 67
- Configuring translation for two systems .................................... 68
- Telephony routing terminology .............................................. 71
Contents

Chapter 7: Administrative user management procedures ................................................. 78
  Starting the Provisioning Client.................................................................................. 79
  Configuring a new Provisioning Client role.............................................................. 79
  Copying Provisioning Client roles........................................................................... 80
  Changing the password for the Provisioning Client admin account........................... 81
  Modifying a Provisioning Client role........................................................................ 81
  Deleting a Provisioning Client role.......................................................................... 82
  Configuring a new Provisioning Client Admin......................................................... 83
  Listing Provisioning Client users............................................................................. 84
  Deleting a Provisioning Client user.......................................................................... 84
  Listing and deleting inactive Admin accounts......................................................... 85
  Resetting an administrator password...................................................................... 85
  Recovering a session after it times out.................................................................... 86
  Using the online help............................................................................................... 86
  Exiting the Provisioning Client................................................................................ 87

Chapter 8: Domain management procedures ................................................................. 88
  Creating the default Demo domain........................................................................... 88
  Configuring a multisite domain................................................................................ 89
    Subscriber Lookup and Routing.......................................................................... 90
  Configuring a root domain with defaults................................................................. 91
  Configuring a subdomain......................................................................................... 92
  Copying services and profiles to a new domain....................................................... 93
  Copying service sets to a new domain..................................................................... 93
  Copying routable services to a new domain............................................................ 94
  Modifying an existing domain................................................................................. 94
  Defining the default Personal Agent URL properties............................................. 95
  Deleting a local domain or subdomain.................................................................... 96
  Configuring domain locales.................................................................................... 96
  Adding a network identifier to a domain................................................................. 97
  Using the Single to Multi-site Migration Tool......................................................... 97

Chapter 9: Foreign domain management procedures ................................................... 99
  Adding a foreign domain.......................................................................................... 99
  Listing or modifying a foreign domain.................................................................... 100
  Deleting a foreign domain...................................................................................... 101

Chapter 10: SIP client provisioning............................................................................... 102
Chapter 1: Password policy procedures ................................................................. 105
Adding a subscriber password policy ................................................................. 105
Assigning a subscriber password policy to a domain ......................................... 109
Listing, modifying, or deleting a subscriber password policy ............................. 110
Modifying per-user password policies ............................................................... 114
  Modifying per-user password policies job aid .................................................. 114
Subscriber Audit ............................................................................................... 115
  Enabling or disabling Password Expiry Audit ................................................ 115

Chapter 12: Resource management procedures ............................................... 116
Listing system resources .................................................................................... 116
Assigning resources to a domain ...................................................................... 116
Viewing user count ........................................................................................... 117

Chapter 13: Service nodes configuration ............................................................ 118
Adding a node .................................................................................................... 118
Listing nodes ...................................................................................................... 120
Assigning a domain to a node .......................................................................... 120
Adding a logical entity ....................................................................................... 120
Listing, modifying, deleting a logical entity ...................................................... 122
Assigning a node or a logical entity to a domain or subdomain ....................... 122

Chapter 14: System services management procedures ...................................... 124
Viewing service dependencies ......................................................................... 125
Banned User service configuration ................................................................... 125
  Banning users .................................................................................................. 125
  Viewing a list of banned users ........................................................................ 126
Branding announcements configuration ................................................................ 126
  Configuring access to branding routable services information ..................... 127
  Assigning branding files .................................................................................. 128
  Branding Media Management ......................................................................... 128
Creating, reviewing, and deleting domain bulletins .......................................... 129
Configuring the Call Processing Language service ......................................... 129
Configuring a profile for a domain ................................................................... 130
Configuring PPND for a domain ...................................................................... 131
  Configuring PPND for a domain ................................................................... 131
Enabling the Global Address Book for a domain ............................................. 132
LDAP synchronization procedures .................................................................... 132
  Configuring the LDAP server ....................................................................... 132
  Configuring the LDAP schema ..................................................................... 134
  Using the Sync Filter Criteria ....................................................................... 135
  Adding user defaults ....................................................................................... 136
Using the LDAP Scheduler ................................................................. 137
Adding the Global Address Book Schema ...................................... 138
Configuring directories for a domain .............................................. 139
Using the Query Test Tool .............................................................. 140
Commercial Cost Avoidance and Hybrid Routing configuration ........ 141
  Configuring the SLR LDAP server .................................................. 141
  Configuring LDAP operation timeouts ......................................... 142
  Configuring the SLR LDAP schema .............................................. 143
  Configuring CCA feature translations .......................................... 145
Configuring Destination Code Controls service ............................. 147
Location management procedures ................................................. 149
  Modifying the default location of a domain ................................. 149
  Modifying the default location of a subdomain ........................... 150
  Adding a location ..................................................................... 150
  Modifying a location .................................................................. 151
  Deleting a location .................................................................... 152
  Viewing and deleting deprecated locations ................................. 152
  Associating a user with a location .............................................. 153
Border Control Point 7000 Series provisioning procedures ............. 154
Miscellaneous Groups service configuration ................................ 154
Provider Managed Clients service configuration .......................... 154
Ring Tone service configuration ................................................... 154
  Creating ring tones .................................................................. 154
  Listing, modifying, or deleting ring tones .................................. 155
  Configuring ring tone profiles .................................................... 156
  Listing, modifying, and deleting ring tone profiles ..................... 156
  Assigning ring tone profiles to a domain ................................. 157
Security service configuration ....................................................... 158
  Configuring the Media Security Profile for a domain ................. 158
  Configuring Signaling Security for a domain ............................. 159
Status Reasons service configuration .......................................... 160
  Configuring domain status reasons ......................................... 160
  Viewing a status reason ............................................................ 161
  Deleting a status reason ........................................................... 161
Configuring TR87 Client Control .................................................. 161
  Assigning resources for TR87 Client Control ............................. 162
  Assigning the TR87 Client Control profile to a Domain .............. 162
  Setting up the TR87 Client Control profile ................................ 162
  Assigning TR87 Client Control to a Domain .............................. 164
  Assigning TR87 Client Control to users ..................................... 164
Treatments service configuration ................................................ 165
  Assigning a pool to a domain or subdomain ............................. 165
  Treatment Media Management .................................................. 167
Chapter 15: Service set procedures ................................................................. 180
  Adding a service set.................................................................................. 180
  Listing and modifying service sets.......................................................... 181
  Deleting a service set.............................................................................. 181

Chapter 16: User services management procedures .................................... 182
  Configuring system profiles for services................................................ 184
  Copying service profiles......................................................................... 191
  Listing, modifying and deleting system profiles...................................... 191
  Assigning or removing a system profile from a domain......................... 192
  Assigning services to a domain............................................................. 192
  Listing and modifying user system profile and user profile..................... 193
  Ad Hoc Conferencing service configuration.......................................... 194
    Configuring Ad hoc audio conferencing service.................................. 194
    Configuring routable services information for Ad Hoc audio conferencing 195
    Assigning Ad Hoc Conferencing service to a domain......................... 196
    Assigning Ad Hoc Conferencing service to a user.............................. 196
  Advanced Screening service configuration.......................................... 197
    Configuring the Advanced Screening service...................................... 197
    Assigning the Advanced Screening service to a user........................... 198
  Allowed Clients service configuration................................................... 198
    Configuring the Allowed Clients service............................................ 199
    Assigning the Allowed Clients service to a domain.............................. 199
    Assigning the Allowed Clients service to a user.................................. 200
  Call Forward Variants service configuration........................................ 200
    Configuring the Call Forward Variants service profile......................... 200
    Assigning the Call Forward Variants service profile to a domain........... 201
    Assigning the Call Forward Variants service profile to a user.............. 202
  Call Grabber service configuration....................................................... 202
    Assigning Call Grabber service to a domain....................................... 203
    Assigning resources for Call Grabber................................................ 203

Adding announcement files to the servicing pool................................... 169
Configuring treatments for service......................................................... 170
User Routing service configuration......................................................... 173
Adding a static route.............................................................................. 174
Assigning the Charge ID to a user......................................................... 174
Vertical Service Code configuration......................................................... 175
  Provisioning Vertical Service Codes...................................................... 176
  Creating a VSC PIN for a subscriber...................................................... 177
Assigning the SIP PBX service to a domain........................................... 177
Assigning the SIP PBX service to a user job aid..................................... 178
Assigning the SIP Line service to a user................................................ 178
Assigning the SIP Line service to a user job aid..................................... 179
Provisioning PSI Distribution for a domain............................................ 179
Contents

Configuring Multiple Attendants service............................................................. 230
Configuring Meet Me Conferencing service...................................................... 230
Configuring routable services information to a Mobility Gateway................... 233
Defining the match criteria for the advanced address book.............................. 233
E911 Options service configuration.................................................................... 234
   Adding an emergency number......................................................................... 234
   Configuring the E911 service......................................................................... 235
   Assigning the E911 system parameter............................................................ 235
   Assigning the Emergency Calling Service..................................................... 236
   Creating or modifying an enterprise ERL....................................................... 237
   Creating or modifying a residential ERL......................................................... 238
   Deleting an ERL............................................................................................ 239
   Capturing ERL additions, deletions, and modifications................................. 240
   Assigning the E911 Options service to a user.............................................. 240
Malicious Call Trace service configuration...................................................... 241
   Adding Malicious Call Trace translation triggers in a domain...................... 241
   Assigning domain data for the Malicious Call Trace service......................... 242
   Assigning Malicious Call Trace service to a user......................................... 243
Mobile Extension service configuration........................................................... 243
MLPP service configuration................................................................................. 243
   MLPP configuration procedures.................................................................... 244
   Creating custom network domains............................................................... 246
   Deleting custom network domains............................................................... 247
   Creating an MLPP namespace...................................................................... 247
   Configuring MLPP feature translation........................................................... 248
   Configuring DSCP marking for the MLPP service........................................ 249
   Creating an MLPP profile............................................................................. 250
   Assigning an MLPP profile to a domain....................................................... 251
   Assigning the MLPP service to a domain...................................................... 252
   Configuring a global diversion destination.................................................. 252
   Configuring MLPP domain data................................................................. 253
   Assigning an MLPP profile to a user............................................................ 254
   Modifying network domain of an existing MLPP namespace....................... 254
Multiple Call Restriction service configuration................................................. 255
   Defining Multiple Call Restriction............................................................... 255
   Assigning Multiple Call Restriction service to a domain............................. 256
Multiple Register service configuration.......................................................... 256
   Configuring the Multiple Register service.................................................. 257
   Assigning the Multiple Register service to a domain................................... 257
   Assigning the Multiple Register service to a user........................................ 258
Music On Hold service configuration............................................................... 258
   Configuring Music On Hold media............................................................. 258
   Music on Hold Media Management............................................................. 259
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Call Logs service configuration</td>
<td>262</td>
</tr>
<tr>
<td>Configuring the Network Call Logs service</td>
<td>263</td>
</tr>
<tr>
<td>Assigning the Network Call Logs service to a domain</td>
<td>263</td>
</tr>
<tr>
<td>Assigning the Network Call Logs service to a user</td>
<td>264</td>
</tr>
<tr>
<td>Network Call Waiting Disable service configuration</td>
<td>264</td>
</tr>
<tr>
<td>Configuring the Network Call Waiting Disable service</td>
<td>264</td>
</tr>
<tr>
<td>Assigning the Network Call Waiting Disable service to a domain</td>
<td>265</td>
</tr>
<tr>
<td>Assigning the Network Call Waiting Disable service to a user</td>
<td>265</td>
</tr>
<tr>
<td>PBX Communicator service configuration</td>
<td>266</td>
</tr>
<tr>
<td>Personal Ringback Tones service configuration</td>
<td>266</td>
</tr>
<tr>
<td>Presence service configuration</td>
<td>266</td>
</tr>
<tr>
<td>Configuring the Presence service</td>
<td>266</td>
</tr>
<tr>
<td>Assigning the Presence service to a domain</td>
<td>267</td>
</tr>
<tr>
<td>Assigning the Presence service to a user</td>
<td>268</td>
</tr>
<tr>
<td>Provisioning Short Dialing Codes</td>
<td>269</td>
</tr>
<tr>
<td>Quality of Service configuration</td>
<td>269</td>
</tr>
<tr>
<td>Configuring the QoS service</td>
<td>270</td>
</tr>
<tr>
<td>Assigning the QoS service to a domain</td>
<td>270</td>
</tr>
<tr>
<td>Assigning the QoS service to a user</td>
<td>271</td>
</tr>
<tr>
<td>Routable services information configuration for Meet Me Audio Conferencing</td>
<td>271</td>
</tr>
<tr>
<td>Configuring access to the logical entity for Meet Me audio conferencing</td>
<td>272</td>
</tr>
<tr>
<td>Creating an alias for Meet Me audio conferencing</td>
<td>272</td>
</tr>
<tr>
<td>Routable services information configuration for the Music on Hold (MOH) feature</td>
<td>273</td>
</tr>
<tr>
<td>Configuring Service Capabilities Interaction Manager</td>
<td>273</td>
</tr>
<tr>
<td>Selective Call Reject service configuration</td>
<td>273</td>
</tr>
<tr>
<td>Configuring the Selective Call Reject service</td>
<td>274</td>
</tr>
<tr>
<td>Assigning the Selective Call Reject service to a domain</td>
<td>274</td>
</tr>
<tr>
<td>Assigning the Selective Call Reject service to a user</td>
<td>275</td>
</tr>
<tr>
<td>Teen Service</td>
<td>275</td>
</tr>
<tr>
<td>TDM Message Waiting Indicator service configuration</td>
<td>276</td>
</tr>
<tr>
<td>Configuring a system profile for the TDM MWI service</td>
<td>276</td>
</tr>
<tr>
<td>Assigning a system profile for the TDM MWI service to a domain</td>
<td>276</td>
</tr>
<tr>
<td>Assigning a system profile for the TDM MWI service to a user</td>
<td>277</td>
</tr>
<tr>
<td>Configuring UCC Short Message Service</td>
<td>277</td>
</tr>
<tr>
<td>Configuring UCC Short Message Service job aid</td>
<td>277</td>
</tr>
<tr>
<td>Uniform Call Distribution service</td>
<td>278</td>
</tr>
<tr>
<td>Routable services information configuration for Unified Communication service</td>
<td>278</td>
</tr>
<tr>
<td>Configuring access to the logical entity for Unified Communications</td>
<td>279</td>
</tr>
<tr>
<td>Creating a message retrieval alias for Unified Communications</td>
<td>279</td>
</tr>
<tr>
<td>Creating an express messaging alias for United Communications</td>
<td>280</td>
</tr>
<tr>
<td>Video service configuration</td>
<td>280</td>
</tr>
<tr>
<td>Configuring the Video service</td>
<td>281</td>
</tr>
<tr>
<td>Assigning the Video service to a domain</td>
<td>281</td>
</tr>
</tbody>
</table>
Contents

Assigning the Video service to a user............................................................ 282
Assigning the Preferred codec to a user....................................................... 282

Voice mail configuration................................................................................. 283
Configuring the voice mail server host......................................................... 283
Adding a SIP-based voice mail server.......................................................... 284
Adding a trunk-based voice mail server......................................................... 285
Adding a line-based voice mail server.......................................................... 286
Adding a prefix-based voice mail server....................................................... 287
Configuring the Voicemail service profile............................................... 288
Assigning the Voicemail service profile to a domain................................. 289
Assigning the Voicemail system profile to a user........................................ 289
Assigning a voice mail server to a user....................................................... 290
Listing, modifying, and deleting a voice mail server.................................. 291

XMPP Gateway service configuration......................................................... 292
Configuring the XMPP Gateway service...................................................... 292
Assigning the XMPP service to a domain.................................................. 293
Assigning the XMPP service to a user......................................................... 293
Configuring the XMPP Incoming Connection policy................................. 294

Chapter 17: Subscriber management procedures........................................ 295
Adding a user to a domain or a subdomain.................................................. 295
Listing and modifying subscribers............................................................... 299
Listing and deleting inactive subscribers..................................................... 302
Changing user password............................................................................. 303
Assigning services to a user........................................................................ 303
Using the Actions tab to modify a user....................................................... 304
Configuring the Personal Agent on behalf of a user................................... 305
Adding aliases and directory numbers for a user........................................ 306
Moving subscribers between domains......................................................... 307

Chapter 18: Avaya Media Server application management procedures........ 310
Finding a Meet Me user by access code...................................................... 310
Finding an active Meet Me conference by access code............................... 311
Finding an active Meet Me conference by domain....................................... 311

Chapter 19: Translations configuration procedures.................................... 312
Telephony route configuration..................................................................... 312
Configuring telephony routes class of service information.......................... 312
Adding a telephony route........................................................................... 313
Listing a telephony route.......................................................................... 315
Adding a route list....................................................................................... 315
Listing, modifying, and deleting a route list................................................ 316
Assigning a number qualifier for a domain................................................ 317
Using the Translation Tool.......................................................................... 317
Assigning pretranslations for a domain....................................................... 318

Chapter 20: Time zone management procedures......................................... 319
Contents

Creating a new time zone.......................................................................................................................... 319
Selecting a time zone................................................................................................................................. 319
  Configuring times zones in the United States.......................................................................................... 320
  Modifying or deleting a time zone............................................................................................................ 321
Chapter 21: Example of Configuring the Presence service........................................................................ 322
Chapter 22: World Wide Numbering and Dial Plan reference................................................................. 325
  Digit format........................................................................................................................................... 325
  Four-digit dialing................................................................................................................................. 327
  Seven-digit dialing............................................................................................................................... 328
  10-digit dialing.................................................................................................................................. 328
  PSTN dialing from within DSN.............................................................................................................. 328
  Class of Service.................................................................................................................................... 329
  Route Code Usage............................................................................................................................... 330
Chapter 1: New in this release

This section details what's new in Avaya Aura® Application Server 5300 Using the Provisioning Client, NN42040-112 for Avaya Aura® Application Server 5300 Release 3.0.

Navigation

• Features on page 16
• Other changes on page 17

Features

For more information about feature-related changes, see the following sections:

• Configuring a new Provisioning Client Admin job aid on page 83
• Adding a subscriber password policy on page 105
• Modifying the Subscriber password policy job aid on page 110
• Branding Media Management on page 128
• Configuring Destination Code Controls service on page 147
• Configuring Destination Code Controls service job aid on page 147
• Configuring system profiles for services job aid on page 184
• Modifying network domain of an existing MLPP namespace on page 254
• XMPP Gateway service configuration on page 292
• Example of Configuring the Presence service on page 322

For information about the new features for Avaya Aura® Application Server 5300, see Avaya Aura® Application Server 5300 Release Delta, NN42040-201.
Document changes since last issue

The following changes have been made to this document since it was issued for Application Server 5300 Release 3.0 in June, 2012:

- Updated Treatment names and causes for VSC on page 171 to update treatment codes for VSC.
- Updated Vertical Service Code configuration on page 175 to provide improved an description of the process to follow when configuring Vertical Service Codes (VSC), including the addition of a work flow diagram.
- Added information about Title (Rank) to Adding a user to a domain or a subdomain job aid on page 296, Adding the Global Address Book Schema job aid on page 139, and Configuring the LDAP schema job aid on page 134.
- Added XMPP Gateway service configuration on page 292.
- Updated configuration steps in the Call Pickup on page 208 section.

Other changes

Revision History

<table>
<thead>
<tr>
<th>Date</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>October 2017</td>
<td>Updated the legal page for Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>April 2017</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 13.</td>
</tr>
<tr>
<td>March 2016</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 12.</td>
</tr>
<tr>
<td>July 2015</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 11.</td>
</tr>
<tr>
<td>December 2014</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 10.</td>
</tr>
<tr>
<td>September 2014</td>
<td>This document is issued to support Avaya Aura® Application Server 5300 Release 3.0 Service Pack 9.</td>
</tr>
<tr>
<td>July 2013</td>
<td>Standard 04.05. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.</td>
</tr>
<tr>
<td>March 2013</td>
<td>Standard 04.04. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. Updated the following sections:</td>
</tr>
<tr>
<td></td>
<td>- Configuring the LDAP schema job aid on page 134</td>
</tr>
<tr>
<td></td>
<td>- Adding a user to a domain or a subdomain job aid on page 296</td>
</tr>
<tr>
<td></td>
<td>- Adding the Global Address Book Schema job aid on page 139</td>
</tr>
</tbody>
</table>

Table continues…
## New in this release

| October 2012 | Standard 04.03. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.  
| | • Removed conceptual information related to Hunting. For conceptual material related to Hunting, see *Avaya Aura® Application Server 5300 Overview* (NN42040–100).  
| | • Added a work flow diagram to *Vertical Service Code configuration* on page 175, and updated *Provisioning Vertical Service Codes* on page 176. |
| June 2012 | Standard 04.02. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0.  
| | Updated various procedures to reflect changes in the User Search portlet. |
| June 2012 | Standard 04.01. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. |
| October 2010 | Standard 02.04. This document is issued to support Avaya Aura® Application Server 5300 Release 3.0. |
| August 2010 | Standard 02.03. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. This document includes technical updates. |
| May 2010 | Standard 02.02. This document is issued to support Avaya Aura® Application Server 5300. |
| April 2010 | Standard 02.01. This document is issued to support Avaya Aura® Application Server 5300 Release 2.0. |
| June 2008 | Standard 01.01. This document is issued to support Nortel Application Server 5300 Release 1.0. |
Chapter 2: Introduction

This document supports the Avaya Aura Provisioning Client user interface. Use the Provisioning Client to perform administration and security tasks.

In this document, the term system refers to Avaya Aura® Application Server 5300.

For information about what features are supported on the system, see Avaya Aura® Application Server 5300 Overview, NN42040-100.

Navigation

- Provisioning Client fundamentals on page 20
- Provisioning Client security on page 25
- Domain management on page 35
- Provisioning for telephony routing and translations on page 65
- Administrative user management procedures on page 78
- Domain management procedures on page 88
- Foreign domain management procedures on page 99
- Password policy procedures on page 105
- Resource management procedures on page 116
- Service nodes configuration on page 118
- System services management procedures on page 124
- Service set procedures on page 180
- User services management procedures on page 182
- Avaya Media Server application management procedures on page 310
- Translations configuration procedures on page 312
- Time zone management procedures on page 319
- Example of Configuring the Presence service on page 322
- World Wide Numbering and Dial Plan reference on page 325
Chapter 3: Provisioning Client fundamentals

This section provides basic information about the Provisioning Client. It describes the administrative and provisioning capabilities of this client. The section provides information about the following topics:

- Provisioning Client overview on page 20
- Software and hardware requirements and recommendations on page 21
- Provisioning Client access on page 22
- Provisioning Client administrative and provisioning tasks on page 22
- Provisioning Client layout on page 23
- Other provisioning mechanisms on page 24

Provisioning Client overview

This chapter provides an introduction to the Provisioning Client. The Provisioning Client is a Web-based graphical user interface that you use to configure access and permissions for the following system components:

- applications
- domains and subdomains (users, devices, telephony routes)
- system (applies to all domains)
- devices
- service nodes
- voice mail servers
- services and service sets
- media portal
- password policy
- applications

Based on the system configuration, subscribers can access the Provisioning Client from anywhere if the URL is publicly accessible, or they can access it only within a particular network if the IP address
Software and hardware requirements and recommendations

Avaya recommends that the capacity of the management PC (the PC at which you run the Provisioning Client) meet the minimum requirements described in the following table.

Table 1: PC requirements for the Provisioning Client

<table>
<thead>
<tr>
<th>Category</th>
<th>Minimum requirement</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Processor</td>
<td>200 MHz Pentium-class or equivalent processor</td>
<td>300 MHz Pentium-class or equivalent processor (or better)</td>
</tr>
<tr>
<td>Free RAM</td>
<td>No additional free RAM required You must meet the minimum memory requirements of your browser. See your browser documentation for more information.</td>
<td>No additional free RAM required You must meet the minimum memory requirements of your browser. See your browser documentation for more information.</td>
</tr>
<tr>
<td>Free hard disk space</td>
<td>No additional hard drive space required Your Web browser performs local caching of Web pages. See your browser documentation for more information about the minimum disk space requirements.</td>
<td>No additional hard drive space required Your Web browser performs local caching of Web pages. See your browser documentation for more information about the minimum disk space requirements.</td>
</tr>
<tr>
<td>Mouse</td>
<td>Optional</td>
<td>Recommended</td>
</tr>
<tr>
<td>Video graphics card</td>
<td>800 x 600 @16bpp [65 536 colors] VGA</td>
<td>1024x768 @16bpp [65 536 colors] VGA or better</td>
</tr>
<tr>
<td>Sound card</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Operating system</td>
<td>Microsoft Windows 7, Microsoft Windows Vista, or Microsoft Windows XP</td>
<td>Microsoft Windows 7, Microsoft Windows Vista, or Microsoft Windows XP</td>
</tr>
<tr>
<td>Network connectivity</td>
<td>56 Kbps modem</td>
<td>10Base-T or other fast network connection, such as Digital Subscriber Line (DSL), Cable, or LAN</td>
</tr>
<tr>
<td>Internet browser</td>
<td>Netscape Communicator 7.0 Microsoft Internet Explorer 6.0</td>
<td>Netscape Communicator 7.1 or better Microsoft Internet Explorer 6.0 or better</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Category</th>
<th>Minimum requirement</th>
<th>Recommended</th>
</tr>
</thead>
<tbody>
<tr>
<td>Java</td>
<td>Not applicable</td>
<td>Not applicable</td>
</tr>
<tr>
<td>Cookies</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
<tr>
<td>Javascript</td>
<td>Enabled</td>
<td>Enabled</td>
</tr>
</tbody>
</table>

## Provisioning Client access

The provisioning options, which appear in the Provisioning Client navigation pane, depend on the level of authority (rights) assigned to the administrator's account.

After a new installation, a single super user role and administrator account exist. The administrator account is associated with the super user role and you cannot change this relationship. You cannot delete the super user role.

For the Provisioning Client, the administrator account is the super user account, which has total control and access to all provisioning rights. The initial password is admin and the super user must change this password during the initial log on.

⚠️ **Important:**

If more than one person knows the administrator (super user) account password, system security is decreased.

The administrator (super user) must configure new roles, new accounts, and assign the new accounts roles. For more information, see [Provisioning Client security](#) on page 25 and [Administrative user management procedures](#) on page 78.

## Provisioning Client administrative and provisioning tasks

With the Provisioning Client you can perform the following administrative and provisioning tasks:

- define administration roles and privileges
- manage (list, add, modify, or delete) users and devices
- define multiple service sets
- create and assigns service profiles and service sets
- assign translation information specific to a domain or subdomain
- provision voice mail servers
- provision 911 emergency notification
Provisioning Client layout

Use the Provisioning Client Home page to access portlets, and search for users. You can open one or more portlets, which appear in the main pane. The following figure shows the Home portlet (Welcome to the Provisioning Client), which always remains open, and is maximized automatically if you minimize any other portlet.

Figure 1: Provisioning Client Home page

Provisioning portlets

The Provisioning Client window contains the provisioning portlets. You can use the provisioning portlets to control and configure access to various Application Server 5300 resources.

After you perform an operation within a portlet, such as submitting a form, or adding, deleting, and modifying data, a status message appears directly under the selected tab in the portlet. The message indicates whether the operation succeeded or failed, and provides an explanation if the operation failed. For an example, see Figure 2: Provisioning Client status message on page 23.

Figure 2: Provisioning Client status message

If a portlet has two levels of data (System, Domain, or User), the portlet provides a Home link. For an example, see Figure 3: Home link on a Provisioning Client portlet on page 23. With this link, you can navigate back to the top level of the portlet.

Figure 3: Home link on a Provisioning Client portlet
If you perform an action that is service-affecting, a Confirmation dialog box appears. To proceed with the action, you must type your administrator password and click Confirm.

![Confirmation dialog](https://example.com/confirmation.png)

**Figure 4: Confirmation dialog**

---

**Other provisioning mechanisms**

In addition to the Provisioning Client, the following mechanisms are used to provision the system.

**Table 2: Provisioning mechanism**

<table>
<thead>
<tr>
<th>Provisioning mechanism</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Provisioning Interface (OPI)</td>
<td>Enables third-party provisioning systems to provision the system. For more information, see Avaya Aura® Application Server 5300 Configuration, NN42040-500 and Avaya Aura® Application Server 5300 Application Programming Interfaces Reference, NN42040-110.</td>
</tr>
<tr>
<td>Lightweight Directory Access Protocol (LDAP)</td>
<td>Allows subscriber data to be synchronized from an existing enterprise directory. If a customer has an existing LDAP directory populated with employees, this allows the customer to synchronize data and make those users available in the system. The synchronization can be set up on a nightly/weekly basis to ensure accuracy. For more information about this functionality, see LDAP synchronization (LDAP Sync) on page 47.</td>
</tr>
</tbody>
</table>
Chapter 4: Provisioning Client security

This section provides an overview of how to administer the Provisioning Client. It covers the following topics:

- **Understanding administration and provisioning** on page 25
- **Understanding provisioning roles and rights** on page 25
- **Provisioning rights and tasks** on page 28
- **Password changes** on page 32
- **Password complexity rules** on page 33

For more information about Provisioning Client user administration, see **Administrative user management procedures** on page 78.

---

**Understanding administration and provisioning**

In the Provisioning Client, a provisioning role is defined as a collection of access rights and privileges that allow an administrator to perform various provisioning tasks. As a System Administrator, you can create any number of provisioning roles, depending on your particular needs. You can add provisioning roles to allow an administrator to perform one or more specific tasks, giving them only a subset of the available rights.

After you log on to the Provisioning Client, a menu bar displays at the top of the Provisioning Client screen. The menu bar provides access to provisioning portlets that you can use to work in the Provisioning Client. The available provisioning portlets, and the types of tasks you can perform as an administrator, are based on the rights assigned to your role.

---

**Understanding provisioning roles and rights**

Administrators can create or define all the necessary provisioning roles to support their system. They can allow or restrict provisioning roles to carry out specific actions.
In the Provisioning Manager, administrators are defined on the system. An administrator has the following capabilities:

- an admin ID
- basic identity information
- a role
- list of allowed domains (root and sub)

A role is a collection of rights. A role contains:

- a name
- data layer rights
- collection of service rights
- Full Domain Access right

A right is a permission, associated either with a data layer or a service and can have the following privileges:

- Read
- Write
- Delete

⚠️ Important:

Having a Delete or Write privilege automatically gives the Read privilege to the administrator.

An administrator can have the following Data Layer rights:

- System Layer Management
  
  With this right, administrators can perform operations for system level data for the services that are assigned to their role.

- Domain Layer Management
  
  With this right, administrators can perform operations for updating domain data for services that are assigned to their role. The operations include adding a subscriber to a domain and removing a subscriber from a domain.

- User Layer Management
  
  With this right, administrators can perform operations for updating user-level data for services that are assigned to their role. The operations include assigning services to users and resetting passwords

⚠️ Important:

The read privilege for all the three rights is available to all administrators by default.

An administrator can also have Full Domain Access right, which gives the administrator access to all domains in the system without the need to individually assign the domains to the administrators. If the administrator’s role contains full domain access right, then the assigned domains list is
overridden. However, Full Domain Access right does not mean that the administrator has access to all domain level data. The administrator still requires the Layer and service rights to have access to specific functions.

Since every function or service in the system is associated with its own right, an administrator also requires the individual Service right. The administrator must have the particular right assigned to him to be able to operate on a specific function or portlet.

---

**Limit access to a domain**

Complementing the rights-based restrictions, administrators can be provisioned against certain domains in order to limit access to within those domains. This prevents an administrator from domain xyz from viewing or modifying details in domain abc, even though they are hosted from the same system. Administrators can then delegate work for subdomains to other administrators without giving them access to data outside that subdomain.

For example, if an administrator assigned to the User Administrator provisioning role has access to suba.xyz (a subdomain of domain xyz), this administrator can add, modify, and delete users in the subdomain, but cannot access the parent domain (domain xyz). This allows for the delegation of tasks on both the rights-level and the domain-level.

Having access to any domain implies having access to all of its descendant subdomains. For example, having access to domain xyz implies having access to suba.xyz. Full domain access will override this domain allocation and allow any administrator assigned with a provisioning role that includes this right to see all domains regardless of what the administrator is provisioned against.

⚠️ **Important:**

Changes to an administrator’s provisioning role take effect on the next login. If you change roles of a logged-in administrator, the changes do not impact the administrator’s existing session.

---

**System administrator provisioning role**

The System Administrator (SA) is the highest level administrator and is the only provisioning role that is preloaded when the Provisioning Client is deployed. The SA has full access and rights to all provisioning features and functions.

The SA can designate someone as an Administrative user from the Add tab of the Admin portlet and grant specific administrator rights to that administrative user from the Add tab of the Admin Role portlet.

Remember that the System Administrator role is the only role that cannot be changed.
Provisioning rights and tasks

Before creating a new provisioning role, an administrator must understand the control associated with each type of provisioning right and the permission each type can grant when the administrator provisions a new role.

Table 3: Provisioning rights

<table>
<thead>
<tr>
<th>Service right name</th>
<th>Service name or function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book Management</td>
<td>Advanced Address Book</td>
</tr>
<tr>
<td>Adhoc Conference Management</td>
<td>Adhoc Conferencing</td>
</tr>
<tr>
<td>Admin</td>
<td>Add, Modify, or Remove administrators</td>
</tr>
<tr>
<td>Advanced Screening Management</td>
<td>Advanced Screening</td>
</tr>
<tr>
<td>Allowed Clients Management</td>
<td>Allowed Clients</td>
</tr>
<tr>
<td>Anonymous Call Rejection Management</td>
<td>Anonymous Call Rejection</td>
</tr>
<tr>
<td>Assistant Console Management</td>
<td>Assistant Console</td>
</tr>
<tr>
<td>Assistant Services Routes Management</td>
<td>Allows an administrator to configure assistant services AS 5300 Personal Agent routes</td>
</tr>
<tr>
<td>Assistant Support Management</td>
<td>Assistant Support</td>
</tr>
<tr>
<td>Banned Subscriber Management</td>
<td>Banned Subscriber</td>
</tr>
<tr>
<td>CPL Service Management</td>
<td>Call Processing Language Setting</td>
</tr>
<tr>
<td>Call Forward Management</td>
<td>Call Forward Variants</td>
</tr>
<tr>
<td>Call Grabber Management</td>
<td>Call Grabber</td>
</tr>
<tr>
<td>Call Park Management</td>
<td>Call Park</td>
</tr>
<tr>
<td>Call Pickup Management</td>
<td>Call Pickup</td>
</tr>
<tr>
<td>Call Return Management</td>
<td>Call Return</td>
</tr>
<tr>
<td>Call Screening Management</td>
<td>Call Type Based Screening</td>
</tr>
<tr>
<td>Call Waiting Disable Management</td>
<td>Call Waiting Disable</td>
</tr>
<tr>
<td>Calling Line ID Restriction Management</td>
<td>Calling Line ID Restriction</td>
</tr>
<tr>
<td>Calling Name Display Management</td>
<td>Calling Name Display</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Service right name</th>
<th>Service name or function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calling Picture Display Management</td>
<td>Calling Picture Display</td>
</tr>
<tr>
<td>Chat Management</td>
<td>IM Chatroom</td>
</tr>
<tr>
<td>Click to call Management</td>
<td>Click to Call</td>
</tr>
<tr>
<td>Client Collab Management</td>
<td>Client Collaboration</td>
</tr>
<tr>
<td>Client Redirect Login Management</td>
<td>Allows an administrator to use Client Redirect Login service for a user.</td>
</tr>
<tr>
<td>Client Types Management</td>
<td>Deprecated</td>
</tr>
<tr>
<td>Colorful Ringback Tones Management</td>
<td>Colorful Ringback Tones (Not supported)</td>
</tr>
<tr>
<td>Converged Desktop Management</td>
<td>Converged Desktop (Not supported)</td>
</tr>
<tr>
<td>Converged Mobility Management</td>
<td>Converged Mobility (Not supported)</td>
</tr>
<tr>
<td>Core Services Session Management</td>
<td>Allows an administrator to configure AS 5300 Session Manager Profile.</td>
</tr>
<tr>
<td>CoS Service Management</td>
<td>Allows an administrator to configure Class of Service.</td>
</tr>
<tr>
<td>Deny All Calls Management</td>
<td>Deny All Calls</td>
</tr>
<tr>
<td>Device Access Restriction Management</td>
<td>Device Access Restrictions</td>
</tr>
<tr>
<td>Device Management</td>
<td>Allows an administrator to manage devices.</td>
</tr>
<tr>
<td>Direct to Gateway Management</td>
<td>Direct to Gateway</td>
</tr>
<tr>
<td>Do Not Disturb Management</td>
<td>Do Not Disturb</td>
</tr>
<tr>
<td>Domain Bulletins Management</td>
<td>Allows an administrator to configure domain bulletins.</td>
</tr>
<tr>
<td>Domain CLI Management</td>
<td>Allows an administrator to configure domain CLI data.</td>
</tr>
<tr>
<td>Domain ISN Management</td>
<td>Allows an administrator to configure domain ISN data.</td>
</tr>
<tr>
<td>Domain Management</td>
<td>Allows an administrator to provision domains and subdomains.</td>
</tr>
<tr>
<td>Domain Profile Management</td>
<td>Allows an administrator to configure domain profiles.</td>
</tr>
<tr>
<td>Domain SOAP Server Management</td>
<td>Allows an administrator to configure SOAP services URL.</td>
</tr>
<tr>
<td>Domain Security Management</td>
<td>Allows an administrator to configure domain security data.</td>
</tr>
<tr>
<td>Domain Service Management</td>
<td>Allows an administrator to provision services for domains.</td>
</tr>
<tr>
<td>Emergency Numbers Management</td>
<td>Allows an administrator to configure emergency numbers.</td>
</tr>
<tr>
<td>Equal Access Management</td>
<td>Equal Access</td>
</tr>
<tr>
<td>Foreign Domain Management</td>
<td>Allows an administrator to configure foreign domains.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Service right name</th>
<th>Service name or function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global Address Book Management</td>
<td>Allows an administrator to configure Global Address Book settings.</td>
</tr>
<tr>
<td>Group Management</td>
<td>Allows an administrator to configure Miscellaneous Groups.</td>
</tr>
<tr>
<td>Hotline Management</td>
<td>Hot Line</td>
</tr>
<tr>
<td>Hunt Group Management</td>
<td>Hunting</td>
</tr>
<tr>
<td>IMS Data Management</td>
<td>Allows an administrator to configure IMS data.</td>
</tr>
<tr>
<td>IP Phone Management</td>
<td>Allows an administrator to manage IP Deskphone devices for users.</td>
</tr>
<tr>
<td>Instant Chat Messaging Management</td>
<td>IM Chatroom</td>
</tr>
<tr>
<td>Instant Messaging Management</td>
<td>Instant Messaging</td>
</tr>
<tr>
<td>Interop Profile Management</td>
<td>Allows an administrator to configure an interop profile.</td>
</tr>
<tr>
<td>Lawful Intercept Management</td>
<td>Allows an administrator to configure Lawful Intercept service.</td>
</tr>
<tr>
<td>(Not supported)</td>
<td>(Not supported)</td>
</tr>
<tr>
<td>LBL Management</td>
<td>Allows an administrator to configure Low Bandwidth Link settings.</td>
</tr>
<tr>
<td>LDAP Management</td>
<td>Allows an administrator to configure LDAP settings.</td>
</tr>
<tr>
<td>Locale Management</td>
<td>Allows an administrator to configure Locales.</td>
</tr>
<tr>
<td>Location Service Management</td>
<td>Allows an administrator to configure Locations.</td>
</tr>
<tr>
<td>MAS Applications Management</td>
<td>Allows an administrator to configure Avaya Media Server application access.</td>
</tr>
<tr>
<td>MLPP Management</td>
<td>Multi-Level Precedence and Preemption</td>
</tr>
<tr>
<td>Malicious Call Trace Management</td>
<td>Malicious Call Trace.</td>
</tr>
<tr>
<td>Match Criteria Management</td>
<td>Allows an administrator to configure match criteria.</td>
</tr>
<tr>
<td>Media Portal Management</td>
<td>Allows an administrator to configure media portal settings.</td>
</tr>
<tr>
<td>MeetMe Management</td>
<td>Meet Me Conferencing</td>
</tr>
<tr>
<td>Mobile Extension Management</td>
<td>Mobile Extension</td>
</tr>
<tr>
<td>Mobility Gateway Management</td>
<td>Mobility</td>
</tr>
<tr>
<td>Mobility Management</td>
<td>Multisite mobility</td>
</tr>
<tr>
<td>Multiple Attendants Management</td>
<td>Multiple Attendants</td>
</tr>
<tr>
<td>Multiple Call Restriction Management</td>
<td>Multiple Call Restriction</td>
</tr>
<tr>
<td>Multiple Login Restriction Management</td>
<td>Multiple Register</td>
</tr>
<tr>
<td>Multiple Site Domain Management</td>
<td>Allows an administrator to manage multisite domain settings.</td>
</tr>
<tr>
<td>Music on Hold Management</td>
<td>Music on Hold</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Service right name</th>
<th>Service name or function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Call Log Management</td>
<td>Network Call Log</td>
</tr>
<tr>
<td>Network Call Waiting Disable Management</td>
<td>Network Call Waiting Disable</td>
</tr>
<tr>
<td>Node Management</td>
<td>Allows an administrator to configure service nodes and logical entities</td>
</tr>
<tr>
<td>PBX Communicator Management</td>
<td>PBX Communicator</td>
</tr>
<tr>
<td>PCC Short Message Management</td>
<td>PCC Short Message</td>
</tr>
<tr>
<td>PCMM Management</td>
<td>Packet Cable Multi Media</td>
</tr>
<tr>
<td>PSI Distribution Data Management</td>
<td>Allows an administrator to configure PSI distribution data.</td>
</tr>
<tr>
<td>Parm Definition Management</td>
<td>Allows an administrator to configure parm definitions. Deprecated.</td>
</tr>
<tr>
<td>Password Policy Management</td>
<td>Allows an administrator to configure password policy.</td>
</tr>
<tr>
<td>Pooled Entity Management</td>
<td>Allows an administrator configure pooled entities. Deprecated.</td>
</tr>
<tr>
<td>Presence Management</td>
<td>Presence.</td>
</tr>
<tr>
<td>Resource Management</td>
<td>Allows an administrator to manage resources that are assigned to domains.</td>
</tr>
<tr>
<td>Ring Tone Management</td>
<td>Allows an administrator to configure ring tones.</td>
</tr>
<tr>
<td>Role Management</td>
<td>Allows an administrator configure roles.</td>
</tr>
<tr>
<td>RoutableService Management</td>
<td>Allows an administrator to configure routable services. Deprecated.</td>
</tr>
<tr>
<td>SCIM Management</td>
<td>Allows an administrator to configure SCIM services.</td>
</tr>
<tr>
<td>SIP Profile Management</td>
<td>Allows an administrator to configure a SIP profile for a domain.</td>
</tr>
<tr>
<td>SIPLines Management</td>
<td>SIP Lines is not supported.</td>
</tr>
<tr>
<td>Selective Call Reject Management</td>
<td>Selective Call Reject</td>
</tr>
<tr>
<td>Service Set Management</td>
<td>Allows an administrator to configure service sets.</td>
</tr>
<tr>
<td>Short Dialing Code Management</td>
<td>Short Dialing Code</td>
</tr>
<tr>
<td>Status Reasons Management</td>
<td>Allows an administrator to configure status reasons.</td>
</tr>
<tr>
<td>System Parameter Management</td>
<td>Allows an administrator to manage system parameters.</td>
</tr>
<tr>
<td>System Service Management</td>
<td>Allows an administrator to configure and manage services at the system level.</td>
</tr>
<tr>
<td>TDM MWI Management</td>
<td>TDM Message Waiting Indicator</td>
</tr>
<tr>
<td>TP Services Management</td>
<td>Allows an administrator to configure third party services</td>
</tr>
<tr>
<td>TR87 Client Control Management</td>
<td>TR87 Client Control</td>
</tr>
<tr>
<td>Telephony Routes</td>
<td>Allows an administrator to configure routelists and telephony routes.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Service right name</th>
<th>Service name or function</th>
</tr>
</thead>
<tbody>
<tr>
<td>Timezone Management</td>
<td>Allows an administrator to configure timezones on the system.</td>
</tr>
<tr>
<td>Treatment Announcements Management</td>
<td>Allows an administrator to configure treatment service.</td>
</tr>
<tr>
<td>UCD Management</td>
<td>Uniform Call Distribution</td>
</tr>
<tr>
<td>UComm Management</td>
<td>Unified Communications</td>
</tr>
<tr>
<td>User Charge Info Management</td>
<td>Allows an administrator to manage Charge IDs for a user.</td>
</tr>
<tr>
<td>User Management</td>
<td>Allows an administrator to add, modify, or remove a user.</td>
</tr>
<tr>
<td>User Personal Data Management</td>
<td>Allows an administrator to manage personal data for a user. Also allows an administrator to log in to a user’s AS 5300 Personal Agent from the Provisioning Client.</td>
</tr>
<tr>
<td>User Picture Management</td>
<td>Allows an administrator to manage the picture for a user.</td>
</tr>
<tr>
<td>User Routes Management</td>
<td>Allows an administrator to manage AS 5300 Personal Agent routes for a user.</td>
</tr>
<tr>
<td>User Service Management</td>
<td>Allows an administrator to enable or disable the list of services for a user.</td>
</tr>
<tr>
<td>User Static Routes Management</td>
<td>Allows an administrator to manage the Static Routes for a user.</td>
</tr>
<tr>
<td>User Timeblock Management</td>
<td>Allows an administrator to manage the Timeblocks for a user.</td>
</tr>
<tr>
<td>Vertical Service Codes Management</td>
<td>Allows an administrator to configure Vertical Service Codes for features.</td>
</tr>
<tr>
<td>Video Management</td>
<td>Video</td>
</tr>
<tr>
<td>Voice Mail Management</td>
<td>Voicemail</td>
</tr>
<tr>
<td>XMPP Management</td>
<td>XMPP Gateway</td>
</tr>
</tbody>
</table>

For more information about configuring new roles for the Provisioning Client and assigning the roles to users to specify admin privileges and level of access, see Configuring a new Provisioning Client role on page 79.

**Password changes**

When an administrator’s password expires, the administrator is forced to change the password to be able to log on to the Provisioning Client. For more information about password policies and the Initial Password Reset option, see Provisioning Client security on page 25.
Password complexity rules

Administrator accounts that provide Operation, Administration and Maintenance (OAM) and Internet Protocol (IP) access to the system through the AS 5300 Element Manager Console and Provisioning Client are subject to password complexity rules. Administrator complexity rules or password policy forces passwords to conform to specific shapes defined by the complexity rules. Additionally, the system also securely stores Administrator passwords.

Figure 5: Password
For more information about password policies for administrators, see Password policy procedures on page 105.
Chapter 5: Domain management

This section provides information about managing domains for Application Server 5300 users. It covers the following topics:

- Introduction to domains on page 36
- Domain naming conventions and restrictions on page 40
- Domain password policy on page 40
- Domain data copy on page 43
- Nodes on page 43
- Gateways on page 43
- Logical Entities on page 44
- Services management on page 45
- Service profile and service set management on page 45
- Resource management on page 46
- LDAP synchronization (LDAP Sync) on page 47
- Hybrid routing on page 53
- SIP clients on page 55
- User management on page 54
- Voice Mail servers provisioning on page 55
- Service nodes configuration on page 56
- Telephony routes configuration on page 57
- Border Control Point 7000 Series provisioning procedures on page 154
- Hotline on page 57
- Malicious Call Trace on page 58
- TDM Message Waiting Indicator on page 59
- Location management on page 59
- Service interactions on page 62

For more information about managing domains, see Domain management procedures on page 88.
Introduction to domains

A domain is used as a control mechanism of users, services, devices, and translations. The Provisioning Client is used to provision a domain. The provisioning of domains allows service providers to define a domain and assign services available for the domain.

You can assign a domain to several Core Service Session Manager profiles. You assign the server home at the user level, by using the Core Services Session Manager profile. The choice of AS 5300 Session Managers, at the user level, is limited only by the list of Core Services Session Manager profiles assigned to the user's domain.

If you have full domain access, you can see all provisioned domains. Otherwise, you will only be able to see the domains and subdomains you are provisioned against. The management rights assigned to a domain administrator dictates what you can do with the domains.

There are several types of domains:

- default domain
- root domain
- subdomain
- foreign domain
- multisite domain

Default domain

The system is preconfigured with a default domain, with services and service profiles assigned to it. This default domain is called Demo. You can delete and recreate the Demo domain at any time.

The following table shows the default services assigned to the domain, what will be in the default service set, and whether a default service profile is also assigned.

ℹ️ Important:

For additional information about service sets and service profiles, see Service profile and service set management on page 45

<table>
<thead>
<tr>
<th>Service</th>
<th>Service Profile Assigned</th>
<th>Service Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc Conferencing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Advanced Address Book</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Advanced Screening</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Allowed Clients</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Anonymous Call Rejection</td>
<td>N/A</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Assistant Console</td>
<td>N/A</td>
<td>No</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Service</th>
<th>Service Profile Assigned</th>
<th>Service Set</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assistant Support</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Call Forward Variants</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Call Grabber</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Call Park</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Call Return</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Call Type Based Screening</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Call Waiting Disable</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Calling Line ID Restriction</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Calling Name Display</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Calling Picture Display</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Click to Call</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Client Collaboration</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Colorful Ringback Tones</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>(Not supported)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Converged Mobility</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Deny All Calls</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Device Access Restrictions</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Do Not Disturb</td>
<td>N/A</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Equal Access</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Hot Line</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>IM Chatroom</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Instant Messaging</td>
<td>N/A</td>
<td>Yes</td>
</tr>
<tr>
<td>Malicious Call Trace</td>
<td>N/A</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Meet Me Conferencing</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Multiple Register</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Music On Hold</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Network Call Logs</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Network Call Waiting Disable</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Packet Cable Multi Media</td>
<td>N/A</td>
<td>No</td>
</tr>
<tr>
<td>Presence</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>QoS</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Selective Call Reject</td>
<td>Yes</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>Short Dialing Code</td>
<td>N/A</td>
<td>Yes - license key</td>
</tr>
<tr>
<td>TDM Message Waiting Indicator</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Unified Communications</td>
<td>Yes</td>
<td>No</td>
</tr>
</tbody>
</table>

*Table continues...*
## Root domain

A root domain is the highest level domain. A service provider can create a root domain for each of their customers. An example of a root domain is avaya.com.

## Subdomain

Use subdomains to divide subscribers within a domain into smaller groups, and thereby to control routing and access to services.

Under each subdomain, you can add additional subdomains, users, devices, and telephony routes. There are no limits to the levels of nesting of subdomains. Each subdomain inherits the parameter values from the root domain.

It is recommended that you set up subdomains based on geographical divisions. For example, using the avaya.com example, you could have avaya.com as the root domain, with subdomains of Richardson and Ottawa. Under each of these subdomains there can be further subdomains, as shown in the following figure.
Foreign domain

When adding a domain, determine whether or not the domain is a foreign domain or not. A foreign domain uses foreign routes, while a local domain uses SIP routing or telephony routes. Foreign domains can be added at any time.

A domain that is not local is considered foreign. Usually, a foreign domain is resolved through Domain Name Server (DNS) and would not need to be provisioned. However, since some deployment scenarios may not involve a DNS, you can datafill routes for a foreign domain.

For example, if the AS 5300 Session Manager that serves avaya.com does not have a DNS, and there is a need for users to be able to make calls to the abc.com domain, then you could add the abc.com domain as a foreign domain and provide a route to the proxy for abc.

Note that you do not control a foreign domain. Therefore you will not be able to provision, for example, users or devices to these domains. However, you can provision routes to a foreign domain.

Multisite domain

Multiple Application Server 5300 sites can share a single domain. Such a domain is called a multisite domain. With the multisite domain, the Application Server 5300 can locate and route messages to a subscriber on a multisite domain in a separate site.
Domain naming conventions and restrictions

When you add a new domain, you must follow the domain naming conventions. Ensure that the domain name is no more than 64 characters in length. It can contain only letters, numbers, and limited symbols and cannot contain specific symbols or characters. The following table lists the restrictions associated with domain names.

### Table 4: Domain name restrictions

<table>
<thead>
<tr>
<th>For a domain name, use</th>
<th>Ranging from</th>
</tr>
</thead>
<tbody>
<tr>
<td>Letters</td>
<td>• a to z</td>
</tr>
<tr>
<td></td>
<td>• A to Z</td>
</tr>
<tr>
<td>Numbers</td>
<td>• 0 to 9</td>
</tr>
<tr>
<td>Symbols</td>
<td>• period (.)</td>
</tr>
<tr>
<td></td>
<td>• hyphen (-)</td>
</tr>
</tbody>
</table>

The following table lists the characters that cannot be used in domain names.

### Table 5: Restricted characters in domain names

<table>
<thead>
<tr>
<th>Restricted characters</th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>'</td>
<td>$</td>
<td>(</td>
<td>)</td>
<td>!</td>
</tr>
<tr>
<td>~</td>
<td>%</td>
<td>_</td>
<td>[</td>
<td>/</td>
</tr>
<tr>
<td>!</td>
<td>^</td>
<td>}</td>
<td>{</td>
<td>?</td>
</tr>
<tr>
<td>@</td>
<td>&amp;</td>
<td>+</td>
<td>&quot;</td>
<td>,</td>
</tr>
<tr>
<td>#</td>
<td>*</td>
<td>=</td>
<td>:</td>
<td>&lt; &gt;</td>
</tr>
</tbody>
</table>

⚠ Important:

Do not use spaces in domain names.

Domain password policy

The password policy defines user password rules in the domain. These rules define the minimum length of a password, the minimum number of digits that a password must contain, the minimum number of characters a password must contain, and whether an initial password reset is required. A single password policy is enforced for all user passwords in the domain. The system enforces the password policies whenever a user creates or changes a password. Domain password policies can

- have a minimum password length between 4 and 32
- have a minimum of 0 to 10 numerical characters
• have a minimum of 0 to 10 non-numerical characters
• contain ASCII characters 0x20 through 0x73 hexadecimal or 32 through 126 decimal. For more information, see an ASCII chart.
• provide a default Password Aging Interval, which becomes the default for all subscribers in the domain

⚠️ Important:

Do not use spaces in the password.

Ensure that the sum of the minimum number of digits and the minimum number of characters is less than or equal to the minimum length of the password.

For more information about Password Policy, see the following sections:

• Provisioning Client security on page 25
• Password policy association with domains on page 41
• Changes to password policy domain associations on page 42
• Subscriber password validation on page 42
• Password policy validation when a subscriber moves between domains on page 42

Password policy association with domains

Password policy controls password length and complexity. A password policy is associated with a domain so that the system can apply the defined controls to the passwords used by the subscribers of that domain.

You must have full domain access to create policies.

The level of administrative privileges assigned to your account controls the list of domains available to you.

A password policy is not enforceable on subscribers until it is associated with a domain. After you associate a password policy with a domain, all subscribers in that domain must conform to that password policy. After you create a password policy, you can either select the policy during the creation of a domain or update a domain and select the policy to use.

These controls enable specification of subscriber password length and complexity for each domain and are defined as part of a password policy. A system can have many password policies defined. There are two reserved password policies defined in the system:

• No Policy is the default policy assigned to new domains as they are added to the system (if you do not specify another password policy). You can modify the default policy.
• Existing supports policy enforcement after a software upgrade to an existing system. The Existing password policy associates a loose password policy to any domain subjected to a software upgrade. The administrator cannot modify the existing policy.
Subscriber passwords are bound by the password policy associated with their domain. This feature provides enforcement of the following:

- a minimum password length that must be between 4 and 32 characters long
- a minimum of 0 to 10 numerical characters that must be present in the password
- a minimum of 0 to 10 non-numerical characters that must be present in the password. The following are valid non-numerical characters:
  - capital and lower case characters A through Z, (specifically ASCII codes: 0x41h through 0x5Ah, and 0x61h through 0x7Ah).
  - special characters .@-^!(),\;:~=+
- whether or not a user will be forced to change their password when they access AS 5300 Personal Agent the first time after an account has been created for them

Changes to password policy domain associations

You can explicitly identify a password policy association when you create a new domain. You can change the password policy of a domain through the domain modification process. If you do not select a password policy for existing domains, the default password policy automatically applies to these domains.

Subscriber password validation

The system validates subscriber passwords for every log on attempt.

When a subscriber attempts to access the Personal Agent, or when an administrator attempts to change subscriber data, the system verifies the subscriber's password for conformance to the current password policy associated with the domain.

Password policy validation when a subscriber moves between domains

If a subscriber is moved from one domain to another domain, the subscriber's password is not validated against the new domain's password policy at the time of the move. The password is validated the next time the subscriber accesses the Personal Agent, or the next time an administrator modifies the subscriber account.

The system prevents subscribers from logging in using passwords that do not conform to the password policy associated with the new domain. Thus, when a subscriber logs on to their Personal Agent with a nonconforming password, the system forces the subscriber to change the password before using Personal Agent.
Important:

When a password policy that is already in use by domains is modified, it is effective only for new subscribers and for existing subscribers who modify their password. The modification does not affect existing subscriber passwords.

Domain data copy

You can simplify the addition of a new domain by copying data from an existing domain. Data that you can copy includes:

- service sets
- service profiles
- routable services

For more information, see Domain management procedures on page 88.

Nodes

A node is a physical element in the network. It can be a gateway, a media service, a SIP PBX, a voice mail service, or any other node.

Gateways

Gateways are integrated into the Location Infrastructure through the association of the location to each gateway as it is provisioned into the system. This association can also be modified after creation (as needed).

Gateways are system resources and so can only be associated with locations defined within the system domain.
Figure 7: Gateway

The Service Node portlet contains the tools required to add, modify, and delete Gateway resources. From the navigation page of the Provisioning Client, select Service Node, Node Management to provision new Gateways into the system and to modify already provisioned Gateways. Both the creation and modification of Gateways provide an opportunity to associate a location with a Gateway.

For more information about adding, listing, or deleting a gateway, see Service nodes configuration on page 118.

Logical Entities

Logical Entities define clusters of servers (gateways and Avaya Media Servers) that are able to provide one or more services. The servers are system resources that provide services to an associated Domain. Logical Entities, as they describe system resources, are integrated into the Location Infrastructure by enabling the association of any system Domain location to the Logical Entity.

A logical entity is also known as a pool of servers (nodes) to which calls are routed for a specific function. This provides load balancing capability that enables calls to be routed to the servers. In the Provisioning Client, and in the procedures in this document, logical entities are sometimes referred to as pools.
For more information about adding, listing, and deleting Logical Entities, see Service nodes configuration on page 118.

### Services management

The administrator defines and assigns services to domains. However, the administrator must have Services provisioning rights to perform these tasks.

To determine which services are required or mutually exclusive for a specific service, see Viewing service dependencies on page 125. For more information about how to configure services, see System services management procedures on page 124 and User services management procedures on page 182.

---

### Service profile and service set management

You can assign services for a domain or subdomain from the Provisioning Client.

After you provision services for a domain, create service profiles and service sets for a domain or subdomain.

- A service profile is any data associated with a service. A system service profile is service data that can be defined at the system level, and a user service profile is service data that can be defined at the user level.
A service set is a group of services available at the domain level that can be assigned to the user. There can be more than one service set at the domain level, which allows assignment of different service sets to different users.

A subscriber must be assigned both a group of services and the service profiles for these services.

The following are general characteristics of the services model:

- A service is assigned to the root domain and is available for use in all subdomains within the domain.
- A service profile assigned to the root domain is available for use in all subdomains within the domain.
- A service must be assigned to the domain in order for the service to be available for all users in the domain.
- A service must be assigned to the user in order for the service to be available to the user.
- If a system profile is mandatory for enabling a service, then the system profile must be assigned to the domain.
- If a system profile is mandatory for enabling a service for a user, then the system profile must be assigned to the user.
- It is possible to assign multiple system profiles to a domain for all the services except E911 service. For E911, only one single system profile can be assigned to the domain.
- If a system profile and a user profile share one parameter, any change or update in that system profile parameter value will not change the respective user profile parameter value.
- Changes made to a service set will not be reflected in any users that have been assigned that service set.

---

**Resource management**

Some services need a license key before an administrator can assign them to a domain. You can assign a license-keyed services to a domain from Resource Management portlet.

A resource is a service and anything that the provisioning manager enforces a count on using the license key. Because services are assigned to users, the number of users having any license-keyed service or non-service can be considered limited and, therefore, the services are considered resources. The following list provides some of the services that are considered assigned resources.

- Advanced Screening
- Call Forward
- Call Return
- Call Type Based Screening
- Deny all Calls
LDAP synchronization (LDAP Sync)

The following sections provide information about Lightweight Directory Access Protocol (LDAP) synchronization.

- LDAP synchronization functionality on page 47
- LDAP sync server configuration on page 49
- Server configuration on page 49
- Schema configuration on page 50
- Sync Filter option on page 52
- User Defaults for LDAP on page 52
- Syncing Scheduler for LDAP on page 52
- Query Test Tool for LDAP on page 53

For more information, see LDAP synchronization procedures on page 132.

LDAP synchronization functionality

The LDAP sync interface propagates subscriber information from an LDAP version 3 server to an Application Server 5300 database. This functionality is offered as part of the Provisioning Manager. The LDAP sync functionality requires that the Application Server 5300 system, particularly the Provisioning Manager, be present or have access to the same network as that of the LDAP sync server.

The feature supports the following functions:

- Addition of new subscribers—the LDAP sync functionality allows creation of new users only if the Relative Distinguished Name (RDN) of the entry in question is not already present on the system for that domain. An example of an RDN is: uid=joeb, ou=Internal, ou=People, o=ABC.
In this example, if the sipuser joeb does not already exist in the system, then this new user can be created.

The following items are known as attributes: uid (user id), ou (organizational unit) and o (organization). See an example of an LDAP sync basic structure: directory information in the following figure. The Distinguished Name (DN) is similar to a file system path in that it defines the directory information tree. However, unlike a file system path that is read left to right, the DN is read from right to left.

Because the RDN must be unique for each user in each domain, any user that was previously added and then moved to a subdomain will still be treated as an existing user. For example, if a user exists in a subdomain, the next synchronization operation would not add that user as a new user in the top-level domain again.

All new users are created in the top-level domain in the Provisioning Client. The top-level entry is the root entry, and each entry contains a DN along with attribute and value pairs. The DN must be unique for a given entry. The following figure is an example of an LDAP sync basic structure.

![LDAP sync structure](image)

**Figure 9: LDAP sync structure**

- Deletion of existing subscribers—the feature does not delete users from the system even if they have been deleted from the LDAP version 3 server. The administrator must manually delete users from the system.

  The status of these users is set to INACTIVE. If a user that has been deleted is subsequently added to the LDAP server again, then the status remains INACTIVE.

- Modification of existing subscribers—if an attribute on the LDAP version 3 server has changed, such as update of a .jpeg photo or number change, then this change is automatically passed to the system during the next synchronization.

Manual or scheduled synchronization of the system with the LDAP server is possible. This functionality can update all user attributes during the synchronization operation, except passwords. Note that passwords can be changed from the Open Provisioning Interface.

Also, note that the system is an LDAP sync client.
It is possible to deploy the LDAP sync functionality with an existing system. In this case, it is possible that the LDAP sync server organization attribute will not match the domain provisioned on the system.

⚠️ Important:
The LDAP sync synchronization functionality is not supported on multisite domains.

### LDAP sync server configuration

LDAP sync server configuration is not supported for subdomains. If a user must be present in a subdomain, the administrator must move that user to a subdomain.

LDAP Synchronization includes the following options:

- **Server Configuration**—configures the primary and secondary LDAP sync servers with which the system communicates.
- **Schema Configuration**—configures schema that the system uses to create users to synchronize with an LDAP version 3 server.
- **User Defaults**—configures the defaults for new users. The defaults include:
  - User Password
  - Class of Service
  - Status Reason
  - Time Zone
  - Locale
  The default values depend on what is already provisioned for the domain.
- **Synchronization Scheduler**—automatically schedules synchronization of the user database with an LDAP version 3 server. The administrator can also schedule an immediate synchronization.
- **Query Test Tool**—verifies that the system is configured correctly to connect to an LDAP version 3 server by allowing the administrator to initiate a query.

### Server configuration

Use the LDAP sync server configuration page to configure:

- an IP address and port of the primary and secondary LDAP sync server with which to communicate
- a user name and password (if rerequired) with which to query the LDAP sync server. Select the LDAP sync server logical name from the list.
- a connection to the LDAP sync server using either a TCP socket or a Secure Socket Layer (SSL) secure socket
Important:
The SSL field is for future use. Selecting SSL causes synchronization failure.

Import the certificate to the JVM through the keytool executable available as part of the Sun JRE

For more information, see Configuring the LDAP server on page 132.

Schema configuration

Schema configuration option enables you to configure the following schema that the system uses from the LDAP sync server for creating new users:

- Distinguished Name Info—A Distinguished Name (DN) is used to distinguish one entry in an LDAP sync database from another as in the following example of an entry whose userid is joeb:

  dn: uid=joeb, ou=Internal,ou=People,o=ABC

  The uid field is part of the RDN for this particular entry. The uid field must be different for every user in the domain. See the following figure that provides LDAP Distinguished name.

Configuring a domain on the system creates the first portion of the DN, o=domain name. The LDAP Distinguished Name o=domain name is present by default. MCP administrators can refine their searches by including other attributes, such as organizational unit (ou). For example, ou=people and ou=external could be included in the dn to further refine the entries in the LDAP sync database that will be used to create users. This limits the synchronization to a portion of the LDAP sync database. The LDAP Distinguished Name field now contains the additional parameters, separated by spaces:

  o=domain name ou=people ou=internal
Figure 10: LDAP Distinguished Name

If no additional parameters are given for the DN, all entries under the o=abc would be used to create new users.

- LDAP sync Server Attribute Mapping (Only the attributes listed in the table that follows can be configured for the system.)

  The Schema Query tool verifies what attributes are available on the LDAP sync server. If necessary the default attributes can be modified to match. If the LDAP sync server does not support the retrieval of its schema, this information should be acquired by the LDAP sync server administrator. The standard attributes are the default. The following is a list of mandatory attributes that must be present in the LDAP sync database to create an user.

Table 6: Mandatory LDAP sync attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td>uid</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
</tr>
</tbody>
</table>

The following is a list of optional LDAP sync Attributes that may be mapped to users, if present in the LDAP sync database.

Table 7: Optional LDAP sync attributes

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Email</td>
<td>mail</td>
</tr>
</tbody>
</table>

*Table continues…*
### Sync Filter option

Sync Filter option enables you to specify which user names, starting with selected characters, are synchronized during a LDAP sync. For more information, see Using the Sync Filter Criteria on page 135.

### User Defaults for LDAP

User Defaults option enables you to select the default User Password, Class of Service, Status Reason, Time Zone, and Locale for any new users that are created.

For more information, see Adding user defaults on page 136.

### Syncing Scheduler for LDAP

There are two ways that an administrator can enable LDAP synchronization:

- Change the top-level domain name on the system to match the organization (o) attribute defined in the LDAP sync database. In this case, all user domain names would differ.

  Furthermore, update of routing and translations to agree with domain names (for example, interdomain routes) might be necessary with this method to deploy the LDAP sync functionality with an existing system.

- Change organization (o) attribute on LDAP sync database to match the domain name configured on the system.

The scheduled time for synchronization is configured in the Provisioning Client. The synchronization process checks every 15 minutes to determine whether it is time to synchronize a domain. In the case of the restart of a Provisioning Manager, a scheduled synchronization job will not run if the
Provisioning Manager comes into service at the same time that a synchronization was originally scheduled.

⚠️ **Caution:**

A restart of the Provisioning Manager interrupts the current web server transactions.

Remember, if a monthly synchronization is scheduled for the 29th (or greater) day of the month, the synchronization will not occur for months that do not contain the number of specified days.

Synchronization will partially fail for a domain with user additions if there are features that are license-keyed and have values unable to accommodate the addition of new users. In this case, the synchronization goes as far as possible until the license limit is reached and then fails after that point. Check the availability of license-keyed features and adjust accordingly to ensure successful synchronization.

When the system synchronizes with an LDAP sync database, the first attribute value of multiple attribute values returned from the LDAP sync database is used.

If a synchronization operation fails, system logs indicate the reason for the failure.

If the Provisioning Manager server fails and the standby Provisioning Manager server starts, then the synchronization will be partially completed. A separate schedule is necessary for a synchronization of a standby Provisioning Manager to occur. The primary and standby Provisioning Managers do not communicate with regards to LDAP synchronization.

For more information, see [Using the LDAP Scheduler](#) on page 137.

---

**Query Test Tool for LDAP**

The LDAP sync Query Test Tool allows the administrator to verify connectivity to a configured LDAP sync database. In order to perform the query, the administrator can enter any node value of a user in the LDAP sync database and click Query LDAP Database.

LDAP-enabled attributes prevent end users from making changes in the Personal Agent, which is a subcomponent of the Provisioning Manager. If a non-mandatory field is left blank, then users can make changes with the Personal Agent.

For more information, see [Using the Query Test Tool](#) on page 140.

---

**Hybrid routing**

With Hybrid routing, Application Server 5300 uses a Lightweight Directory Access Protocol (LDAP) database to allow the Multi-Function Soft Switches (MFSS) to identify a call as either an IP or TDM route, and then to route the call appropriately.

You can use the Provisioning Client to configure hybrid routing and to perform user updates for the LDAP database.
For more information, see Commercial Cost Avoidance and Hybrid Routing configuration on page 141 and Subscriber management procedures on page 295.

User management

This section describes how to manage the users using the Provisioning Client. It covers the following topics:

• Managing user functions on page 54
• Mailbox usage reports on page 54

Converged Desktop services and users are not supported on Application Server 5300.

Managing user functions

After a domain or subdomain is provisioned, perform the following actions:

• adding, viewing, modifying, or deleting users from the domain or subdomain
• adding, viewing, modifying, or deleting Avaya IP Deskphone device properties
• viewing, modifying, or deleting aliases
• provisioning a user’s Meet Me audio conferencing service

For more information, see Subscriber management procedures on page 295.

Converged Desktop

Converged Desktop (CD) is not supported in Application Server 5300

Mailbox usage reports

With the Provisioning Client, you can generate and download reports of mailbox usage for all subscribers in all domains. The system formats the report as a comma delimited file. You can use a spreadsheet program to open and view reports, and to

• create customized reports and graphs
• maintain historical data
SIP clients

Avaya Aura® Application Server 5300 supports only SIP devices. The configuration files for the devices are stored in the sipphone.war folder on the database server. You can place the modified configuration files in the /var/mcp/media/prov_pa_installs/sipphone directory.

The ntappgrp must have access to all files placed in the /var/mcp/media/prov_pa_installs/sipphone directory, including the following files:

- 1140eSIP.cfg
- 1120eSIP.cfg
- 1140e.cfg (During rollback)
- 1120e.cfg (During rollback)
- SIPDefaultConfig.dat
- dialplan.txt
- banner.txt
- secpolicy.txt
- rootca.pem

You can manually edit all of these files, except SIPDefaultConfig.dat, dialplan.txt, and secpolicy.txt, which Avaya provides.

Avaya recommends that you use the Provisioning Client or the Open Provisioning Interface (OPI) to manage the following files:

- SIP<mac>.cfg
- devcert<mac>.p12
- ipctoken<mac>.cfg

The Provisioning Client and OPI store these files in the database, as opposed to placing them in the /var/mcp/media/prov_pa_installs/sipphone directory.

For more information, see SIP client provisioning on page 102.

Voice Mail servers provisioning

With the Provisioning Client, you can provision third-party voice mail server information to

- configure call to route to voice mail
- associate users with a voice mail server
- set up a voice mail server to receive message waiting indicator (MWI) notifications
Important:
The administrator must have provisioning rights to provision the voice mail servers.

Voice mail server types

The following table describes supported voice mail server types.

Table 8: Types of voice mail servers

<table>
<thead>
<tr>
<th>Voice mail server type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SIP-based</td>
<td>This is an IP-based voice mail server that uses the SIP protocol. This server type does not need a PSTN gateway.</td>
</tr>
<tr>
<td>Trunk-based</td>
<td>This is a legacy Public Switched Telephone Network (PSTN)-based voice mail server that uses a Primary Rate Interface (PRI) or Channel Associated Signaling (CAS) gateway. The AS 5300 Session Manager uses SMDI to send call setup information using a Call Detail Message to get Message Waiting Indicator (MWI) information from the voice mail server.</td>
</tr>
<tr>
<td>Line-based</td>
<td>This is a voice mail server with multiple lines, each identified by a 10-digit phone number that goes into the voice mail server. When people leave messages, the individual lines are used in a round-robin manner to connect to the voice mail server to allow someone to leave a message. The AS 5300 Session Manager sends an SMDI message to the voice mail server to help establish the connection to the AS 5300 Session Manager that uses SMDI to obtain Message Waiting Indicator (MWI) information from the voice mail server.</td>
</tr>
<tr>
<td>Prefix-based</td>
<td>This is a voice mail server that uses the prefix of the phone number to send call setup information.</td>
</tr>
</tbody>
</table>

Service nodes configuration

A Service node is defined as any network element in the system that provides a service such as gateways, conference servers, or voice mail servers. An administrator is able to change the IP addresses of a service node in order to accommodate network topology changes and change the IP addresses without reloading or redeploying the software. From the Service node portlet, an administrator can also add logical nodes, which consist of one or more service nodes. A service node contained within a logical node may have additional system- or user-defined parameters, such as a trkgrp, associated with it.

For more information about configuring Service Nodes, see Service nodes configuration on page 118.
Telephony routes configuration

Telephony routing enables customers to configure their dial plans and to set Virtual Private Networks (VPNs). You must have telephony routing and domain management provisioning rights to perform the tasks in this section.

For more information, see Translations configuration procedures on page 312.

Border Control Point 7000 Series provisioning

Application Server 5300 does not support the Border Control Point 7000 series.

Hotline

Each hotline user can be assigned a different Designated Called Party (DCP). The hotline service allows users to make a call to their DCP automatically by picking up the phone. There are three types of hotline users:

- Origination only—User can only place calls to their DCP
- Termination only—User can only receive calls from any other hotline user.
- Both termination and origination—User can place calls to their DCP and receive calls from any other hotline users.

When a hotline user dials a number, Application Server 5300 replaces the number with the user's DCP. According to the hotline user's indicator type, the system adds related tgrp and trunk context parameters.

Hotline services are supported on 1100 series and 1200 series IP Deskphones.

Hotline service is not supported for the Avaya Aura® AS 5300 UC Client. If a hotline user logs into an Avaya Aura® AS 5300 UC Client, the following message will display: "You are being de-registered due to the hotline service being enable in your service profile".

Hotline service can be used by the Audiocodes MP IAD. Audiocodes IAD has its own hotline implementation to automatically dial a provisioned number. When hotline service is provisioned for an IAD subscriber, the application server will change the request URI to dial the DCP instead.

Hotline modes

The Hotline service works in two different modes:

- Service Protection enabled—supported for the SA user type.
• Service Protection not enabled—supported for the SA, SSL, and IMS user types.

Hotline subscribers do not dial any precedence level. For protected hotline subscribers, the system automatically configures the call to the maximum allowed precedence level.

---

**Hotline indicators**

There are two different hotline indicators:

• **Voice**—Users assigned a voice hotline indicator can only connect to other hotline users assigned to a voice indicator.

• **Data**—Users assigned a data hotline indicator can only connect to other hotline users assigned to a data indicator.

Calling party will hear a VCA when attempting to place a call between different hotline indicators, regardless of caller's precedence level.

**Protected parameter**

This parameter enables or disables service protection.

When service protection is enabled:

• Only protected hotline to protected hotline calls are allowed.

• Hold, redirect, transfer and conference are not allowed.

• The AS 5300 Session Manager adds related tgrp and trunk context parameters according to origination hotline user's indicator.

When service protection is disabled:

• There are no restrictions on indicator or hotline types for these users.

• Users have DSCP and Key label values.

• Hold, redirect, transfer and conference are allowed.

---

**Malicious Call Trace**

With the call tracing feature, you can trace nuisance or threatening calls. SA, SSL, and IMS users all have access to this feature.

Administrator can enable automatic tracing when malicious caller is unknown. All incoming or outgoing calls can be traced and malicious caller can also be found from logs.

There are two types of call tracing:

• Terminating call tracing—All incoming calls to a specified directory number (DN) are enabled and can be traced, even if the nuisance calling number is unknown.
• Outgoing call tracing—Outgoing nuisance calls to a specified DN suspected of originating from a given system are traced.

Outgoing call tracing and Terminating call tracing provisions remain intact after system re-initialization.

# TDM Message Waiting Indicator

The Voicemail service supports Time Division Multiplexing (TDM) voice mail servers. TDM Message Waiting Indicator (TDM MWI) provides voice mail notification to TDM subscribers.

The Avaya Media Server provides the voice mail functionality and stores voice mail messages for retrieval. The system uses Simplified Message Desk Interface (SMDI) protocol to transmit TDM MWI notification messages.

For more information about how to provision TDM subscribers, see the following sections:

- Adding a user to a domain or a subdomain on page 295
- Adding a service set on page 180
- TDM Message Waiting Indicator service configuration on page 276

For information about how to configure the SMDI server, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*.

# Location management

This section describes how to manage the location of the users. The section covers the following topics:

- Create a domain default location on page 59
- Add, modify, or delete a location on page 60
- Associate a user with a location on page 60
- Assign a default location for an Avaya IP Deskphone on page 61
- Foreign domains location on page 62

# Create a domain default location

Whenever a domain is created (including the system domain that is created by the system administrator), it automatically creates a default location (called other). Since other is the only location present at the moment of a domain's creation, it is used as the initial default location for the domain.
Remember, locations are provisioned in the root domain.

There is an other location for every domain. While the name other is ambiguous, each other location is unique (qualified by the domain name). The other location cannot be deleted. After initial creation, you can create a multi-layered location hierarchy for a domain.

Use the following procedures to modify default locations:

- Modifying the default location of a domain on page 149
- Modifying the default location of a subdomain on page 150

Add, modify, or delete a location

Locations are defined within a domain. Locations are labeled using a location name that is used to identify the location within the domain. A particular domain cannot contain duplicate location names. However, a location name can be reused across domains, but this does not infer any association because a location name by itself only has meaning within a domain. Thus, all locations provisioned in the system are unique and are fully qualified by their domain and location name.

An example of this is the default location (other) that is created automatically whenever a domain is created. Every domain has a default location of other and each instance of other is unique.

Locations are provisioned at the parent domain level of the system. Locations can be constructed in a tree-like structure that represents the geography of the service area. The location tree hierarchy makes for a more logical representation of location and provides an intuitive structure for navigation (especially for users using the access clients).

Use the following procedures to add, modify, and delete a location:

- Adding a location on page 150
- Modifying a location on page 151
- Deleting a location on page 152

Associate a user with a location

Users are integrated into the location infrastructure through the location field when they are provisioned into the system as shown in the following figure.

Comments on this document? infodev@avaya.com
Assign a default location for an Avaya IP Deskphone

Avaya IP Deskphone devices can have a default location associated with them. This default location is at the top of the list of locations offered to the first user to register for service on this client. This prominent positioning is a cue to the user that this location is the best location association for this client.

Figure 11: Associating users with locations

Figure 12: Default location
Foreign domains location

Foreign Domains do not have a visible association with the Location Infrastructure, but they are integrated into the Location Infrastructure internally through the automatic creation of the default other location for each Foreign Domain.

The foreign domain other location is limited in that it cannot be provisioned as an ERL. Consequently, emergency calls from foreign domains are not supported by this feature.

For non-emergency calls, a single unique location is all you need to enable foreign domains to benefit from the Location Infrastructure.

Figure 13: Foreign domains locations

For more information, see Foreign domain management procedures on page 99.

Service interactions

This section describes the interaction restrictions and dependencies between subscriber services. It covers the following topics:

- Interactions when assigning multiple services on page 62

Interactions when assigning multiple services

The following table describes the interactions that occur when multiple services are assigned to a subscriber.
### Table 9: Service interactions

<table>
<thead>
<tr>
<th>This service</th>
<th>Interacts with this service</th>
<th>In this way</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voicemail</td>
<td>Advanced Screening</td>
<td>When you assign the voice mail service and do not assign the Advanced Screening service, then only the default route is available for the subscriber. The default route tries the subscriber's registered clients for five rings and then transfers to voice mail.</td>
</tr>
</tbody>
</table>
| Device Access Restrictions |                             | When the Voicemail service and the Device Access Restrictions service are assigned to a service set and the Restriction Access parameter is configured to Restricted Access, then the subscriber is not able to call voice mail using the IP Deskphone by going off hook and pressing VMail.  
Device Access Restrictions and CS 2000 SIP Line services are mutually exclusive. |
| CS2000 SIP Line services |                             | Voicemail and CS 2000 SIP Line services are mutually exclusive.                                                                                                                                 |
| Presence              | Advanced Addressbook        | When you assign the Presence service and the Advanced Addressbook service to a service set and the Addressbook service parameter Maximum Number of Addressbook Entries Allowed is less than the Presence service parameter Maximum size of client friend list, then the number of friends that a subscriber may have is limited to the Addressbook service parameter Maximum Number of Addressbook Entries Allowed.  
Note that the maximum value is 750; however, administrators should consult traffic and capacity guidelines when defining the service parameters for Advanced Addressbook. |
| Device Access Restrictions |                             | When you assign the Presence service and the Device Access Restrictions service to a service set and set the Restriction Access parameter to Restricted Access, then the subscriber will not be able to access presence on the IP Deskphone.  
When you assign the Presence service to a service set but do not assign the Addressbook service to the service set, then the number of friends that a subscriber may have is limited to 10 or the Presence service parameter Maximum size of client friend list (whichever is less). |
| XMPP Gateway          |                             | The Extensible Messaging and Presence Protocol (XMPP) Gateway allows subscribers to send and receive presence status to and from external XMPP users or remote Application Server 5300 users. |

*Table continues…*
<table>
<thead>
<tr>
<th>This service</th>
<th>Interacts with this service</th>
<th>In this way</th>
</tr>
</thead>
<tbody>
<tr>
<td>Advanced Screening</td>
<td>Voicemail</td>
<td>When you assign the Advanced Screening service to a service set but do not assign the Voicemail service to the service set, then the Personal Agent Route Wizard does not let anyone create a route that terminates a call to voice mail (through the voice mail service).</td>
</tr>
<tr>
<td>Hotline</td>
<td>CS2000 SIP Line services</td>
<td>Hotline and CS 2000 SIP Line services are mutually exclusive.</td>
</tr>
<tr>
<td>IM Chatroom</td>
<td>Instant Messaging</td>
<td></td>
</tr>
<tr>
<td>Assistant Support</td>
<td>Advanced Screening</td>
<td>This requires Call Park and Presence (presence-based routing).</td>
</tr>
<tr>
<td>Assistant Console</td>
<td>Advanced Screening</td>
<td>Requires Advanced Screening, Call Park, Presence (presence-based routing).</td>
</tr>
<tr>
<td></td>
<td>CallPark</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Presence</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Presence Based Routing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CS 2000 SIP Line</td>
<td>Mutually exclusive - CS 2000 SIP Line</td>
</tr>
<tr>
<td>Call Park</td>
<td>Calling Line ID</td>
<td>Mutually exclusive:</td>
</tr>
<tr>
<td></td>
<td>Call Waiting Disable</td>
<td>• Calling Line ID Restriction</td>
</tr>
<tr>
<td>CS 2000 SIP Line</td>
<td>PCClientSet Control</td>
<td>• Call Waiting Disable</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• CS 2000 SIP Line</td>
</tr>
<tr>
<td>Wireless Gateway</td>
<td>Application Server 5300 does not support the Wireless Gateway.</td>
<td>Application Server 5300 does not support the Wireless Gateway.</td>
</tr>
</tbody>
</table>
Chapter 6: Provisioning for telephony routing and translations

This section provides a basic understanding of how to provision telephony style translations interworking with traditional circuit-switched network routing.

• Telephony routing concepts on page 65
• Configuring translation for one system on page 67
• Configuring translation for two systems on page 68
• Telephony routing terminology on page 71
• Sample dial plan for telephony routes on page 74
• Configuring Interop Profile on page 77

Telephony routing concepts

The basic function of any communications equipment is routing, and SIP-based systems add requirements to routing when compared to traditional circuit-switched network-based routing. Routing in the VoIP networks adds the complexity of integrating with the traditional circuit-switched networks and domain-based VoIP and SIP networks.

Subdomains

The concept of subdomains allows the domain administrator to group users into smaller routing groups. For example, Avaya can have a single domain supporting a Richardson subdomain and an Ottawa subdomain. Users within Avaya are assigned to subdomains, but can be reached by using only the top domain. The concept of SIP subdomains is similar to the e-mail domains used within an enterprise.

⚠️ Important:

Subscribers do not have to be aware of subdomains. Subdomains are used only to group subscribers for partitioning telephony translations.

The following figure shows an example of the subdomain concept.
Class of Service

Class of Service (COS) screens restrict users from accessing certain telephony routes within a domain and subdomain. The following restrictions are imposed on the use of COS:

- COS values are assigned to routes as well as domains, subdomains, and subscribers. Access to routes is restricted by comparing the COS value assigned to the route with the COS value assigned to the subscriber, or the default for the domain/subdomain if the call was not subscriber-originated. Only routes with equal or lower COS values will be selected.
- A domain, subdomain, or subscriber has access to the routes if the assigned COS permits access to the routes.

The domain-based COS value is used to determine the telephony routes for incoming sessions from gateways or other SIP networks. In these scenarios the Uniform Resource Identifier (URI) domain does not host the originator. Therefore, for security purposes, the URI domain's COS is applied to screen the call.

- If the From header and Request URI do not have the same domain, then the domain specified in the Request URI is used to determine the telephony routes.
- If the From and Request URI domains are the same and the originator is an MCP subscriber, then the originator's COS determines the telephony routes. If the originator does not have an assigned COS, then the COS for the originator's subdomain is used. If the subdomain COS is not found, go up the domain tree until you find a COS value set on a parent domain. If the COS value set is not found, then the call is rejected.
• The same COS values can be assigned to a domain, subdomain, and a subscriber.

**AS 5300 Session Manager routing stages**

The following figure shows the relationship between the telephony routing stages provided by the AS 5300 Session Manager. If the COS value of the subscriber and subdomain route do not match, then the parent and subsequent subdomains are checked for routes that permit access.

![Telephony routing stages diagram](diagram)

**Figure 15: Telephony routing stages**

---

**Configuring translation for one system**

**About this task**

The Equal Access (EA) Bridge domain routes SIP-to-SIP local calls between EA and non-EA domains. EA Bridge domain translation is defined with one telephony route, which adds an EA prefix in front of a DN number and then searches aliases at EA Domain.

The system domain routes inbound PSTN calls to the parent domain of EA and non-EA subscribers. System domain translation must be defined with two telephony routes, in the following order:

1. routes to non-EA domain
2. routes to EA Bridge domain
At non-EA Domains, user aliases contain 10-digit user DN numbers. Non-EA Domain translations must contain multiple telephony routes, in the following order:

1. routes to EA Bridge domain
2. routes to PSTN

Users who use local carriers for long-distance calls must be assigned to an EA Domain. EA Domain translation must contain multiple telephony routes, in the following order:

1. telephony route, which adds an EA prefix in front of a DN number and then searches aliases at EA Domain
2. telephony route, which routes calls to a system domain

Configuring translation for two systems

About this task

The system domain routes inbound PSTN calls to the parent domain of EA and non-EA subscribers. System domain translations must be defined with three telephony routes, in the following order:

1. routes to a non-EA Domain of the primary system
2. routes to a non-EA Domain at the secondary system
3. routes calls to the EA Bridge domain

EA Bridge domain translation must be defined with two telephony routes, in the following order:

1. adds an EA prefix in front of a DN number and then searches aliases at EA Domain of the primary system
2. adds an EA prefix in front of a DN number and then searches aliases at EA Domain of the secondary system

Non-EA Domain user aliases contain 10-digit user DN numbers. Non-EA Domain translations must contain multiple telephony routes, in the following order:

1. routes to a non-EA domain of the secondary system
2. routes to an EA Bridge domain
3. routes to PSTN

Users who use local carriers for long-distance calls must be assigned to an EA Domain. EA Domain translation must contain multiple telephony routes, in the following order:

1. private telephony route, which adds an EA prefix in front of a DN number and then searches aliases at an EA Domain
2. routes calls to a system domain

The following figure shows inbound routing translation, outbound routing translation to a non-EA domain, and outbound routing translation to an EA domain between two systems.
Figure 16: Inbound routing

MCS user routes via PRIs
Provisioning for telephony routing and translations

Figure 17: Outbound non-EA routing

MCS user routes via PRIs

Comments on this document? infodev@avaya.com
Route lists on page 71
Routes on page 73

Route lists

Route lists consist of specific telephony routes for a local domain or subdomain. The following additional options can be applied to routes in the route list:

- allow all incoming sessions from other domains
- block all incoming sessions from other domains
- redirect all incoming session from other domains
- allow all incoming sessions from other subdomains
- block all incoming sessions from other subdomains
• redirect all incoming session from other subdomains

**Example of telephony route redirection between domains**

The following figure shows an example of a telephony redirect imposed by a route list in the xyz.com domain when a session originates from the abc.com domain.

![Telephony route redirection between domains](image)

Figure 19: Telephony route redirection between domains

**Example of telephony route redirection between subdomains**

The following figure shows an example of a telephony redirect between two subdomains. In this scenario the originating subscriber's subdomain is checked when a route list in the subdomain otta.abc.com sets the subdomain redirect option.
Figure 20: Telephony route redirection between subdomains

Routes

Telephony routes provide the actual dial plan route calls. It includes routes for a private digit dial plan, routes to gateways, and telephony style routing between SIP domains and subdomains. The three types of telephony routes available are (in the order preference of route selection)

- Private
- SIP
- Gateway

Private telephony routes

Private telephony routes are used for abbreviated telephony-style digit dial plans. For example, private dial plans apply abbreviated dial plan rules to locate subscriber aliases. Private routes can be set up for a 5-digit dial plan between selected subscribers in a domain.

SIP routes

SIP routes have two functions: first, SIP routes cause translations to be carried out in a different domain; second, they look for subscriber aliases in a different domain.
Gateway routes

Gateway routes terminate to physical protocol gateways.

Sample dial plan for telephony routes

This section provides a sample dial plan for provisioning the following telephony routes:

- private telephony route for using five-digit translations between subscribers
- SIP telephony route for using PSTN-style number plan to call between different domains
- gateway route to make local (PSTN) calls using 9+ prefix

Provisioning domains, subscribers, and COS

Before implementing the dial plan, provision a list of domains, subscribers, and COS for the following domains in the example:

- abc.com—includes the rich.abc.com and otta.abc.com subdomains
- xyz.com

The following figure shows the domains and subscribers in the sample dial plan.

Figure 21: Domains and subscribers in the dial plan

The domain abc.com defines the following three types of COS:

- lobby_dial_plan (lowest COS)
• local_dial_plan
• company_dial_plan (highest COS)

A subscriber that has company_dial_plan COS will also have access to routes defined for lobby_dial_plan and local_dial_plan. The domain xyz.com defines a COS, all_dial_plans, that is available to all subscribers in this domain.

⚠️ Important:

The assumption here is that each subscriber is assigned a 10-digit alias in all the domains.

---

### Example dial plan assignments

The following table provides an example list of subscribers, subscriber aliases, and COS assignments in the domains.

<table>
<thead>
<tr>
<th>Subscriber</th>
<th>Alias</th>
<th>Domain</th>
<th>Subdomain</th>
<th>COS</th>
</tr>
</thead>
<tbody>
<tr>
<td>lobby</td>
<td>9726850000</td>
<td>abc.com</td>
<td>rich.abc.com</td>
<td>lobby_dial_plan</td>
</tr>
<tr>
<td>paul</td>
<td>9726851000</td>
<td>abc.com</td>
<td>rich.abc.com</td>
<td>local_dial_plan</td>
</tr>
<tr>
<td>john</td>
<td>9726852000</td>
<td>abc.com</td>
<td>otta.abc.com</td>
<td>company_dial_plan</td>
</tr>
<tr>
<td>fred</td>
<td>2146842000</td>
<td>xyz.com</td>
<td></td>
<td>all_dial_plans</td>
</tr>
</tbody>
</table>

---

### Dial plan description

The dial plan for the two parent domains (abc.com and xyz.com) uses the various digit ranges as described in the following table.

<table>
<thead>
<tr>
<th>Route name</th>
<th>Description</th>
<th>From</th>
<th>To</th>
<th>Number of digits</th>
<th>Domain</th>
<th>Subdomain</th>
<th>Type of route</th>
</tr>
</thead>
<tbody>
<tr>
<td>5_digit_plan</td>
<td>5+4 digits to reach subscribers in rich.abc.com</td>
<td>5</td>
<td>5</td>
<td>5</td>
<td>abc.com</td>
<td>rich.abc.com</td>
<td>Private</td>
</tr>
<tr>
<td>pstn_route</td>
<td>9+10 digits to reach a PSTN subscriber. Strip the 9 before reaching the subscriber.</td>
<td>9</td>
<td>9</td>
<td>11</td>
<td>abc.com</td>
<td></td>
<td>Gateway</td>
</tr>
</tbody>
</table>

Table continues…
The following provides further description of the dial plans:

- The 5+4-digit dial plan allows the subscribers in subdomain rich.abc.com to reach other subscribers in the same subdomain using only a five-digit dial plan (for example, 5+1000). Because the five-digit dial plan is only required in the subdomain, it is assigned as a private route.
- The 9+10-digit dial plan is used to access the SIP PRI Gateway to terminate calls to a PSTN network; so this is assigned a gateway route.
- The 6+7-digit dial plan is used for communicating between two parent domains; therefore, this digit range is assigned to SIP routes.

### Associating COS and the route

The COS and routes described earlier are tied together to provide the user restrictions in the following table. This table shows that the lobby_dial_plan COS has access only to the 5+4-digit dialing, therefore, restricting phones in a lobby to five-digit dialing only. The company_dial_plan, having the highest COS, has access to all three routes.

#### Table 12: User restrictions

<table>
<thead>
<tr>
<th>COS</th>
<th>Routes</th>
</tr>
</thead>
<tbody>
<tr>
<td>lobby_dial_plan</td>
<td>5+4 digits to reach subscribers in rich.abc.com</td>
</tr>
<tr>
<td>local_dial_plan</td>
<td>5+4 digits to reach subscribers in rich.abc.com 9+10 digits to reach a PSTN subscriber. Strip the 9 before reaching the subscriber.</td>
</tr>
<tr>
<td>company_dial_plan</td>
<td>5+4 digits to reach subscribers in rich.abc.com 9+10 digits to reach a PSTN subscriber. Strip the 9 before reaching the subscriber. 6+7 digits to reach xyz.com from abc.com</td>
</tr>
<tr>
<td>all_dial_plans</td>
<td>6+7 digits to reach abc.com from xyz.com</td>
</tr>
</tbody>
</table>
Configuring Interop Profile

About this task
Use this procedure to configure Interop Profile.

Procedure
1. From the Provisioning Client menu bar, select Translations > Interop Profile.
2. In the Interop Profile portlet, type an interop profile name in the Name field.
3. Click Save.
Chapter 7: Administrative user management procedures

About this task
To control access to the Provisioning Client, create administrative roles and users, and then assign roles to the users. Each administrative user requires a password to log on to the Provisioning Client. For more information about security for the Provisioning Client, including password rules, see Avaya Aura® Application Server 5300 Security, NN42040-601.

- Starting the Provisioning Client on page 79
- Configuring a new Provisioning Client role on page 79
- Configuring Provisioning Client roles on page 80
- Changing the password for the Provisioning Client admin account on page 81
- Modifying a Provisioning Client role on page 81
- Deleting a Provisioning Client role on page 82
- Configuring a new Provisioning Client Admin on page 83
- Listing Provisioning Client users on page 84
- Deleting a Provisioning Client user on page 84
- Listing and deleting inactive Admin accounts on page 85
- Resetting an administrator password on page 85
- Recovering a session after it times out on page 86
- Using the online help on page 86
- Exiting the Provisioning Client on page 87

Note:
Application Server 5300 Release 3.0 introduces new rights to Provisioning Client Administrator accounts and passwords. When your system is upgraded to Release 3.0, any custom roles created in previous releases of Application Server 5300 have these new rights configured to default values. You must configure the new rights manually for custom roles.
Starting the Provisioning Client

About this task
You access the Provisioning Client by using the Web browser on a PC. Perform this procedure to start and log on to the Provisioning Client.

Procedure

1. On the PC, start any supported Web browser.
2. In the Address bar of the Web browser, enter the Uniform Resource Locator (URL) for the Provisioning Client.
   
The URL must be similar to: http://<Provisioning Manager IP>:8443/prov
   
   **Important:**
   
   If unencrypted access is disabled, you must use https://<Provisioning Manager IP>:8443/prov
3. If a security alert appears, proceed only if you trust the site security certificate.
4. Read the security warning and select the check box to acknowledge that you have read and understood the message.
5. Click Confirm.
6. On the Provisioning Client log on page, in the User Name box, type your user name.
7. In the Password box, type your password.
8. Click Login.
9. Read the security warning and select the check box to acknowledge that you have read and understood the message.
10. Click Confirm.

Configuring a new Provisioning Client role

Use this procedure to configure new roles for the Provisioning Client and assign the roles to users to specify administrator privileges and level of access.

Before you begin

- You have administration management rights.
- You are a secadmin.

The secadmin role has complete access.
**Procedure**

1. From the Provisioning Client menu bar, select **Admin > Role** to access the Admin Role portlet.

2. On the **Add** tab, in the **Role Name** box, type a name for the new role.

3. In the **Role description** box, type a brief description of the role.

4. Under the **Select All** option, check the **Read**, **Write**, or **Delete** boxes if you want the administrator to have a specific privilege or check all boxes to provide all privileges.

5. Under the **Data Layer Management** option, check the **Write** and **Delete** boxes if you want the administrator to have one or both privileges on the **System**, **Domain**, and **User** level.

6. Select the necessary **Read**, **Write**, and **Delete** check boxes to configure access for each Admin privilege.

7. Click **Save**.

---

### Copying Provisioning Client roles

**About this task**

Use this procedure to copy the data in an existing role to be used in the creation of a new role.

**Procedure**

1. From the Provisioning Client menu bar, select **Admin > Role** to access the Admin Role portlet.

2. In the list of roles, locate the role to be copied and click **Copy**.

3. On the **Copy** tab, in the **New Role Name** field, type a name for the new role.

4. In the **Role description** field, type a brief description of the role.

5. Under the **Select All** option, check the **Read**, **Write**, or **Delete** boxes if you want the administrator to have a specific privilege or check all boxes to provide all privileges.

6. Under the **Data Layer Management** option, check the **Write** and **Delete** boxes if you want the administrator to have one or both privileges on the **System**, **Domain**, and **User** level.

7. Select the necessary **Read**, **Write**, and **Delete** check boxes to configure access for each Admin privilege.

8. Click **Save**.
Changing the password for the Provisioning Client admin account

Use this procedure to change the administrator password. For security reasons, change the default password.

Importantly:

Changes to administrator passwords take effect immediately. If an administrator is logged in and the administrator's password is changed, the administrator must enter the new password to continue working.

Before you begin

• You have the administration management right.
• You have the secadmin role.

Procedure

1. From the Provisioning Client menu bar, select Admin > Change Admin Password.
2. In the Admin portlet, select the Password tab.
3. Type the New Password, Confirm Password, and Current Password values.
4. Click Save.

Your new password activates upon your next login.

Changing the administrator password job aid

About this task

The following job aid describes the parameters that appear on the Password tab of the Admin portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New password</td>
<td>Type a new password.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the new password again.</td>
</tr>
<tr>
<td>Current password</td>
<td>Type your current password.</td>
</tr>
</tbody>
</table>

Modifying a Provisioning Client role

You can modify roles for the Provisioning Client to specify admin privileges and level of access.

Before you begin

• You are a secadmin.
The secadmin role has complete access.

**Procedure**

1. From the Provisioning Client menu bar, select **Admin > Role** to access the Admin Role portlet.
2. On the **List** tab, in the **Role Name** column, click the name of the role to be modified.
3. In the **Role Description** box, type a brief description of the role.
4. Under the **Data Layer Management** option, check the **Write** and **Delete** boxes if you want the administrator to have one or both privileges on the **System**, **Domain**, and **User** level.
5. Select the necessary **Read**, **Write**, and **Delete** check boxes to configure access for each Admin privilege.
6. Click **Save**.

---

**Modifying a Provisioning Client role job aid**

**About this task**

For more information about the administrative privileges listed on the **Add a New Role** page, see the following sections:

- [Understanding provisioning roles and rights](#) on page 25
- [Provisioning rights and tasks](#) on page 28

---

**Deleting a Provisioning Client role**

You can delete a Provisioning Client role that is no longer in use.

**Before you begin**

- You are a secadmin.

   The secadmin role has complete access.

**Procedure**

1. From the Provisioning Client menu bar, select **Admin > Role**.
2. In the Admin Role portlet, click the **List** tab.
3. In the table, click **Delete** for the role that you want to delete.
4. Type the SA password in the confirmation window to delete the admin role and click **Confirm**.
Configuring a new Provisioning Client Admin

Use this procedure to configure new Admin users for the Provisioning Client. Assign each new Admin user a role so they can perform the administrative functions associated with that role.

Before you begin

- You have the administration management right.
- You are a secadmin.
  The secadmin role has complete access.

Procedure

1. From the Provisioning Client menu bar, select **Admin > Add** to access the Admin portlet.
2. On the Add tab, select **Enable account**.
3. On the Add tab, configure parameters as required.
4. Click **Save**.

Configuring a new Provisioning Client Admin job aid

About this task

The following job aid describes the parameters that appear on the **Add** tab of the Admin portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>This parameter contains the Admin account user name (maximum 64 characters).</td>
</tr>
<tr>
<td>First Name</td>
<td>This parameter contains the user's first name (maximum 30 characters).</td>
</tr>
<tr>
<td>Last Name</td>
<td>This parameter contains the user's last name (maximum 30 characters).</td>
</tr>
<tr>
<td>Password</td>
<td>This parameter contains the password for the user account.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>This parameter must match the Password parameter.</td>
</tr>
<tr>
<td>Disable password aging</td>
<td>Select this check box to disable password aging.</td>
</tr>
<tr>
<td>Enforce password change</td>
<td>Select this check box to enforce password change during the first log on.</td>
</tr>
<tr>
<td>Enable account</td>
<td>Select this check box to enable the account. The administrator account is not accessible unless you enable this option.</td>
</tr>
<tr>
<td>Disable account inactivity period</td>
<td>This parameter defines whether the account is disabled after the period of inactivity defined in the Account Inactivity Period (days) Log On Rule.</td>
</tr>
</tbody>
</table>

If Disable account inactivity period is set to yes, the account is never disabled due to inactivity. If Disable account inactivity period is set to no, the Account Inactivity Period (days) Log On Rule causes the system to automatically disable the account after the configured number of days.
<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>By default, Disable account inactivity period is set to yes for the default Admin.</td>
<td></td>
</tr>
<tr>
<td><strong>Caution:</strong></td>
<td>If you configure all Admin accounts to be disabled after a period of inactivity, there is a risk of permanently locking all administrators out of the system.</td>
</tr>
<tr>
<td>Maximum Password Life (days)</td>
<td>The value you enter in this field overrides the system Password Policy for Maximum Password Life. Leave blank to use the system value. This parameter defines the maximum number of days before the user's password expires. The range of values allowed is 0–180 days. For a password that never expires, enter 0 (zero). Default value: 90</td>
</tr>
<tr>
<td>Email</td>
<td>This parameter contains the user's e-mail address (if available).</td>
</tr>
<tr>
<td>Business Phone</td>
<td>This parameter contains the user's business telephone number (if available).</td>
</tr>
<tr>
<td>Home Phone</td>
<td>This parameter contains the user's home phone number (if available).</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>This parameter contains the user's cell phone number (if available).</td>
</tr>
<tr>
<td>Pager</td>
<td>This parameter contains the user's pager number (if available).</td>
</tr>
<tr>
<td>Time Zone</td>
<td>This parameter (select from the list) contains the user's time zone.</td>
</tr>
<tr>
<td>Locale</td>
<td>This parameter (select from the list) contains the user's preferred language.</td>
</tr>
</tbody>
</table>

**Listing Provisioning Client users**

**About this task**

Use this procedure to search for administrator user accounts for the Provisioning Client.

**Procedure**

1. From the Provisioning Client menu bar, select **Admin > List** to access the Admin portlet.
2. To see a list of administrator user accounts, select the **List** tab.

**Deleting a Provisioning Client user**

**About this task**

Use this procedure to remove Provisioning Client user accounts that are no longer required.
Listing and deleting inactive Admin accounts

About this task
Use this procedure to list and delete inactive Admin accounts.

Procedure
1. From the Provisioning Client menu bar, select Admin > List to access the Admin portlet.
2. Select the Advanced Search tab.
3. In the Inactive time in days box, type a value (Days since last log on. Enter 0 to list all accounts).
4. Click Search.
5. To delete an unwanted Admin user:
   a. Select the List tab.
   b. Click Delete for the Admin account that you want to delete.
   c. On the confirmation dialog, type your administrator password, and click Confirm.

Resetting an administrator password

Use this procedure to reset another administrator's password.

Before you begin
• You have the administration management right.
• To reset the password for the admin account, you must have the secadmin role.

Procedure
1. From the Provisioning Client menu bar, select Admin > List to access the Admin portlet.
2. On the List tab, click Reset for the administrator whose password you want to reset.
3. Configure the New password and Confirm password parameters and select the Enforce password change check box.
4. Click Save.
Resetting the administrator password job aid

The following job aid describes the parameters listed in the Admin portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New password</td>
<td>Type a new password.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the new password again.</td>
</tr>
<tr>
<td>Enforce password change</td>
<td>Select the check box to enforce password change immediately.</td>
</tr>
</tbody>
</table>

Recovering a session after it times out

About this task

If the Provisioning Client is inactive for a period of time, the session expires (times out). Consequently, if you try to use the Provisioning Client, the Provisioning Client Login page appears. Perform this procedure to restart a Provisioning Client session.

Procedure

1. On the Pre-log on banner page, select the check box to acknowledge that you have read and understood the message.
2. Click Confirm.
3. On the Provisioning Client Login page, in the User Name box, type your user name.
4. In the Password box, type your password.
5. Click Login.
6. On the Post-log on banner page, select the check box to acknowledge that you have read and understood the message.
7. Click Confirm.

Using the online help

About this task

Online help provides the following features:

- help pages that contain forward and backward navigation icons
- procedures that help you use the Provisioning Client
- a Table of Contents with hypertext links
- an Index with hypertext links
Perform this procedures to obtain help with the Provisioning Client.

Procedure
To view the online task-based help system, on any Provisioning Client portlett, click the help icon ?.

Exiting the Provisioning Client

About this task
Use the following procedure to exit the Provisioning Client and end the session.

Procedure
On the Provisioning Client heading, above the menu bar, click Logout.
Chapter 8: Domain management procedures

About this task
Use the procedures in this section to manage the domain settings of the Application Server 5300 users.

- Creating the default Demo domain on page 88
- Configuring a multisite domain on page 89
- Configuring a root domain with defaults on page 91
- Configuring a subdomain on page 92
- Copying services and profiles to a new domain on page 93
- Copying service sets to a new domain on page 93
- Copying routable services to a new domain on page 94
- Modifying an existing domain on page 94
- Defining the default Personal Agent URL properties on page 95
- Deleting a local domain or subdomain on page 96
- Configuring domain locales on page 96
- Adding a network identifier to a domain on page 97
- Using the Single to Multi-site Migration Tool on page 97

Creating the default Demo domain

About this task
You can create a default domain, with services and service profiles already assigned to it. You can delete and recreate this domain at any time. Use this procedure to create or recreate the default Demo domain.

Procedure

1. From the Provisioning Client menu bar, select Domain > Quick Start Demo to access the Domain portlet.
2. On the **Quick Start Demo** tab, configure the parameters for the domain and then click **Save**.

### Configuring the default Demo domain job aid

**About this task**

This job aid describes the parameters that appear on the **Quick Start Demo** tab of the Domain portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>Type the name of the root domain you want to create, using the following format:</td>
</tr>
<tr>
<td></td>
<td>domainname.com</td>
</tr>
<tr>
<td></td>
<td>An example of a root domain is avaya.com.</td>
</tr>
<tr>
<td><strong>Add 5 users and assign resources</strong></td>
<td>Select this option to create five users and to assign to them the default standalone service set. In addition license key resources for the five users and the services contained in the service set are assigned to the domain.</td>
</tr>
<tr>
<td></td>
<td>To reclaim these resources for use in another domain, you can delete the domain, or delete the users and then unassign the resources from the domain.</td>
</tr>
<tr>
<td><strong>User password</strong></td>
<td>The password for the five user accounts.</td>
</tr>
<tr>
<td><strong>Confirm user password</strong></td>
<td>Confirm the password for the five user accounts.</td>
</tr>
</tbody>
</table>

### Configuring a multisite domain

Use this procedure to configure a root domain as multisite, for hybrid routing or Commercial Cost Avoidance. After you configure a multisite domain, the domain enforces the LDAP push mechanism with the customer LDAP server.

**Before you begin**

- The appropriate NKRS key must be applied to the system in order for the administrator to configure a domain as multisite.
- Domain characteristics must be common among the sites and all of the users of the multisite domain.
- A root domain must have an SLR server (LDAP server) and SLR schema (LDAP schema) associated with it before it can be set as multisite.
Important:

This operation is service-affecting. After you configure the domain as multisite, the system considers the LDAP server to be the primary database. You cannot add or delete users if the LDAP server is unreachable. You cannot delete or update users unless they are defined in the LDAP server.

Important:

You can configure only root-level domains as multisite. Associated domains then become multisite. You cannot remove the multisite designation for a domain after you configure it.

Important:

Uniqueness of all subscribers (subscriber names, alias) must be maintained in a multisite domain because duplicate subscribers are not permitted within a multisite domain.

Procedure

1. On the Provisioning Client Domain portlet, on the List tab, select the domain.
2. Select the Multisite tab.
3. Select the Multisite check box and click Save.

Important:

Before you confirm the action, read the text in the confirmation dialog. The configuration of a multisite domain is service-affecting.

4. In the confirmation dialog, type your administrator password, and click Confirm.

Subscriber Lookup and Routing

With the Subscriber Lookup and Routing (SLR) feature, Application Server 5300 sites can share a single domain, which is called a multisite. This feature allows locating and routing messages to a subscriber on a multisite domain in a separate site. This function is performed through a query to the Lightweight Directory Access Protocol (LDAP) server. All provisioning details of sites in a multisite are stored both in the Database and LDAP.

This feature also allows Subscriber Mobility between the Application Server 5300 sites in a multisite domain. A user can gain access to their account from a client homed in another site. This feature does not require that the user change the proxy information, but rather the user enters the user name and authentication information, and the system determines the location for that subscriber. Each subscriber (whether in single site or multisite domain) is associated directly with a home AS 5300 Session Manager as opposed to his domain being associated to the Server home.
Configuring a root domain with defaults

About this task

Use this procedure to create a root domain with default services, service profiles, and service sets assigned to the domain. A root domain is the highest level domain by which you organize users, services, devices, and translations.

⚠️ Important:

This is the recommended method of adding a domain. Advanced users can select the Add Without Defaults (Advanced) tab to add a domain without default services, service profiles and service sets.

Procedure

1. From the Provisioning Client menu bar, select Domain > Add Root Domain > With Defaults (Recommended) to access the Domain Details portlet.
2. On the Add With Defaults (Recommended) tab, configure the Name, Password policy, Realm, and Time zone parameters.
3. Click Save.

Configuring a root domain job aid

About this task

This job aid describes the parameters that appear on the Add tab of the Domain portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the root domain you want to create by using the following format:</td>
</tr>
<tr>
<td></td>
<td>domainname.com</td>
</tr>
<tr>
<td></td>
<td>An example of a root domain is avaya.com.</td>
</tr>
<tr>
<td>Password Policy</td>
<td>The subscriber password complexity rules for the domain. Select from the list. Subscriber password complexity rules can be defined to enforce such things as the minimum length of a password, the minimum number of digits that a password must contain, and the minimum number of characters a password must contain. The relationship between these three password complexity controls is such that the sum of the minimum number of digits and the minimum number of characters must be less than or equal to the minimum length of the password.</td>
</tr>
<tr>
<td>Realm (for a domain)</td>
<td>The domain for subscribers when they are being authenticated. Subscribers can register in multiple domains. When users enter a password during authentication, they need to know the domain so that they can enter the appropriate password. Range: up to 120 characters Default: Realm</td>
</tr>
</tbody>
</table>
### Configuring a subdomain

**About this task**
Use this procedure to create subdomains to organize users, services, devices, and translation into smaller groups within a domain.

**Procedure**
1. From the Provisioning Client menu bar, select **Domain > Add Sub-domain**.
2. On the **Add Sub-domain** tab, configure the **Parent domain**, **Name**, and **Time zone** parameters.
3. *(Optional)* To have the subdomain inherit data from the parent domain, select the **Copy parent domain data** check box.
4. Click **Save**.

### Configuring a subdomain job aid

**About this task**
This job aid describes the parameters that appear on the **Add** tab of the Domain portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parent domain</td>
<td>The name of the domain for which you want to configure a subdomain.</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the subdomain you want to create by using the following format:</td>
</tr>
<tr>
<td></td>
<td><a href="mailto:subdomainname@domain.com">subdomainname@domain.com</a></td>
</tr>
<tr>
<td></td>
<td>For example, if the root domain name is avaya.com, the subdomain name can</td>
</tr>
<tr>
<td></td>
<td>be <a href="mailto:ottawa@avaya.com">ottawa@avaya.com</a>.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone of the user.</td>
</tr>
<tr>
<td>Common Names</td>
<td>The common names of the subdomain. When <strong>SIP TLS Identity Checking</strong></td>
</tr>
<tr>
<td></td>
<td>is enabled, the common names in this field are compared against the</td>
</tr>
<tr>
<td></td>
<td>common name in the X.509 client certificate for the SIP TLS connections.</td>
</tr>
</tbody>
</table>

*Table continues…*
### Parameters and Description

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy parent domain data</td>
<td>If selected, the subdomain inherits the following data from the parent domain:</td>
</tr>
<tr>
<td></td>
<td>• Domain SOAP Server data</td>
</tr>
<tr>
<td></td>
<td>• Unified Communications service domain data</td>
</tr>
<tr>
<td></td>
<td>• Unified Communications service routable service data</td>
</tr>
<tr>
<td></td>
<td>• Meet Me service domain data</td>
</tr>
<tr>
<td></td>
<td>• Meet Me service conference pool data</td>
</tr>
<tr>
<td></td>
<td>• Colorful Ringback Tones service pool data</td>
</tr>
<tr>
<td></td>
<td>(Colorful Ringback Tones is not supported)</td>
</tr>
<tr>
<td>Up to five common names can be configured for a subdomain.</td>
<td></td>
</tr>
</tbody>
</table>

---

### Copying services and profiles to a new domain

**About this task**

Use this procedure to copy services and profiles from an existing domain to a new domain.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > Copy** to access the Domain Copy portlet.
2. On the **Services & Profiles** tab, select a domain, from which services are to be copied, in the **Select domain** pull-down and click `>>`.
3. Select a target domain in the **Target domain** pull-down. Select services in the **Available Services** list to be copied to the target domain and click **Copy**.
4. Click **Save**.

---

### Copying service sets to a new domain

**About this task**

Use this procedure to copy service sets from an existing domain to a new domain.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > Copy** to access the Domain Copy portlet.
2. On the **Service Sets** tab, select a domain, from which service sets are to be copied, in the **Select domain** pull-down and click `>>`. 
3. Select a target domain in the **Target domain** pull-down and click **>>**.
4. Select service sets in the **Available Service Set** list to be copied to the target domain and click **Copy**.
5. Click **Save**.

---

**Copying routable services to a new domain**

**About this task**

Use this procedure to copy routable services from an existing domain to a new domain.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > Copy** to access the Domain Copy portlet.
2. On the **Routable Services** tab, select a domain, from which the routable services are to be copied, in the **Select domain** pull-down and click **>>**.
3. Select a target domain in the **Target domain** pull-down.
4. Select services in the **Available Services** list to be copied to the target domain and click **Copy**.
5. Click **Save**.

---

**Modifying an existing domain**

**About this task**

Use this procedure to modify an existing domain.

**Procedure**

1. On the **List** tab in the **Domain** portlet, select the domain you want to modify.
2. On the **Details** tab, modify the parameters as required.
3. Click **Save**.

---

**Modifying an existing domain job aid**

**About this task**

This job aid describes the parameters for modifying a domain that appear on the **Details** tab of the Domain Details page.
### Defining the default Personal Agent URL properties

**About this task**

Use this procedure to define the default Personal Agent URL properties.

**Procedure**

1. On the **List** tab in the **Domain** portlet, select the domain for which you want to define the default Personal Agent URL properties.
2. On the **Domain Details** portlet, select the **Personal Agent** tab.
3. Configure the **DNS Domain Name**, **HTTP port**, **HTTPS port** parameters.
4. Click **Save**.

---

**Defining the default Personal Agent URL properties job aid**

This job aid describes the parameters for modifying a domain that appear on the **Personal Agent** tab of the **Domain Details** page.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DNS Domain Name</strong></td>
<td>This is the host name of the machine that hosts the Provisioning Manager. The Avaya Aura® AS 5300 UC Client uses it to retrieve data</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td></td>
<td>required through the Provisioning Manager. Note that the Domain URL has to be a DNS-resolvable hostname and not an IP address.</td>
</tr>
<tr>
<td>HTTP Port</td>
<td>This is the port information tagged onto the Domain URL information and which is sent to the Avaya Aura® AS 5300 UC Client, which uses the information to retrieve data from the Provisioning Manager in a nonsecure or HTTP mode.</td>
</tr>
<tr>
<td>HTTPS port</td>
<td>This is the port information tagged onto the Domain URL information and which is sent to the Avaya Aura® AS 5300 UC Client, which uses the information to retrieve data from the Provisioning Manager in a secure or HTTPS mode using Secure Socket Layer (SSL).</td>
</tr>
</tbody>
</table>

**Deleting a local domain or subdomain**

**About this task**

Use this procedure to delete a local domain.

**Important:**

If you delete a domain, you delete everything it contains (including service sets and subscribers assigned within).

**Procedure**

1. In the Domain portlet, select the **Action** tab.
2. Select the domain you want to delete from the list.
3. Click **Delete**.
4. In the confirmation window, type your administrator password and click **Confirm**.

**Configuring domain locales**

**About this task**

Use this procedure to configure domain locales.

A domain locale is a list of permitted locales (languages specific to country and region, for example, Chinese, Traditional Chinese, and French) allowed in a domain. With domain locales, you can limit the language choices for users in a domain. For instance, a US company can limit the locales to English and Spanish. A Canadian company can limit the locales to English and French. An Asian company may only have Traditional Chinese and Japanese.

**Procedure**

1. On the **List** tab in the Domain portlet, click the domain you want to modify.
2. Select the **Locale** tab.
3. Select the corresponding check box for each locale that you want to permit.
4. Click **Save**.
5. Select a default locale from the **Default domain locale** list.
6. Click **Save**.

---

**Adding a network identifier to a domain**

**About this task**

Use this procedure to add a network identifier for a domain.

A network identifier gives the operators the ability and flexibility to charge for the access and services they offer to the users. The network identifier is associated for each domain and must be the same for a domain tree. A network identifier can be the same across domains.

**Procedure**

1. From the Provisioning Client menu bar, select **Translations > Network ID**.
2. On the **Domain Data** tab, type the name of the domain to which you want to add a network identifier, and then click `>>`.
3. In the Network Identifier area, type an identifier in the **Network ID** field.
   - The network identifier can be up to 64 characters long.
4. Click **Save** to save the identifier.

---

**Using the Single to Multi-site Migration Tool**

Use this procedure to generate LDAP Data Interchange Format (LDIF) file(s) to perform the following operations:

- Add routing information for all subscribers belonging to a multisite domain.
- Delete routing information for all subscribers belonging to a multisite domain.
- Update routing information for subscribers on a per-multisite domain basis when you modify a Session Manager alias.
- Update Master LSC and Serving SS CCA IDs for all subscribers belonging to a multisite domain.

**Procedure**

1. Log on to the Provisioning Client.
2. Click **Tools, Single to Multi-site Migration Tool**.

3. Follow the on-screen instructions to download the Single to Multi-site Migration Tool zip file.

4. Extract the zip file to a local folder, and open the ReadMe.txt file that is included in the zip file.

5. Follow the instructions in the ReadMe.txt to launch the tool, and optionally add, delete, or update routing information, or update server IDs for all subscribers in a multisite domain.
Chapter 9: Foreign domain management procedures

About this task
Use the procedures in this section to manage foreign domains.

- Adding a foreign domain on page 99
- Listing or modifying a foreign domain on page 100
- Deleting a foreign domain on page 101

Adding a foreign domain

Use this procedure to add a foreign domain.

Before you begin
- You can access the Provisioning Client.
- You know the IP address of the remote foreign destination.

Procedure
1. From the Provisioning Client menu bar, select Domain > Foreign Domain to access the Foreign Domain portlet.
2. On the Add tab, configure the Name, SIP proxy name, SIP URI params, Foreign destination, and Domain aliases parameters.
3. Click Save.

Adding a foreign domain job aid

About this task
This job aid describes the parameters that appear on the Add tab in the Foreign Domain portlet.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type the name of the Foreign Domain. The name of the foreign domain must match the name of the domain hosted by the external SIP proxy.</td>
</tr>
<tr>
<td>SIP proxy name</td>
<td>A foreign domain proxy can be defined by either using an external SIP proxy provisioned in element manager or by specifying an IP address. A fully-qualified domain name (FQDN) can be used instead of the IP Address. Select either External Domain or Address Name.</td>
</tr>
<tr>
<td></td>
<td>If External Domain is selected, the domain URL entered in the address field must be a DNS-resolvable external domain name or hostname. If Address Name is selected, an address should be selected from the drop-down menu in the address box. The address name is the Long Name of the external SIP proxy, defined through the AS 5300 Element Manager Console.</td>
</tr>
<tr>
<td>SIP URI params</td>
<td>URI parameters include:</td>
</tr>
<tr>
<td></td>
<td>• authenticated This parameter allows all incoming request messages from a foreign domain defined with an FQDN to be accepted without an authentication challenge. The resolved IP addresses are added to the SESM authentication table. A DNS server with an entry matching the FQDN must be set up on all of the SESMs on which the Foreign Domain will be used.</td>
</tr>
<tr>
<td></td>
<td>• trusted This allows all outgoing messages going to this domain to be handled as going to a “trusted” domain.</td>
</tr>
<tr>
<td></td>
<td>• nt_info=proxy This parameter should be added when the Foreign Domain SIP Proxy represents an Application Server 5300 system. This parameter is used to tell the foreign server that the call has been forwarded by another Application Server 5300 system.</td>
</tr>
<tr>
<td>Foreign Destination</td>
<td>Clicking the ADD button adds a SIP proxy route with its corresponding SIP URI parameters in the Foreign Destination field. Clicking the REMOVE button removes the entries in this field.</td>
</tr>
<tr>
<td>Domain Aliases</td>
<td>Select one or more aliases associated with informational elements that are configured as the General type. The alias is used as an alias for the foreign domain.</td>
</tr>
</tbody>
</table>
Procedure

1. From the Provisioning Client menu bar, select **Domain > Foreign Domain** to access the Foreign Domain portlet.
   
   The **List** tab on the Foreign Domain portlet shows a list of existing foreign domains.

2. Click the link of the foreign domain you want to modify.

3. On the domain details page, configure **Name, SIP proxy name, SIP URI params, Foreign destination**, and **Domain aliases** fields.

4. Click **Save**.

---

Deleting a foreign domain

About this task

Use this procedure to delete a foreign domain.

Procedure

1. From the Provisioning Client menu bar, select **Domain > Foreign Domain** to access the Foreign Domain portlet.

2. In the Foreign Domain portlet, click the **List** tab.

3. Click the **Delete** link next to the foreign domain that you want to delete.

4. In the confirmation dialog, type your administrator password and click **Confirm**.

   **Important:**

   After you delete a foreign domain, subscribers can no longer route requests to that domain.
Chapter 10: SIP client provisioning

About this task
Use the procedures from this chapter to manage SIP devices.

- Adding a SIP device on page 102
- Adding multiple SIP devices on page 102
- Modifying a SIP device on page 103
- Deleting a SIP device on page 103

Adding a SIP device

About this task
Use this procedure to add a new SIP device to the system.

Procedure
1. From the Provisioning Client menu bar, select Clients > SIP Clients > Domain SIP Clients to access the SIP Client Device portlet.
2. In the Domain Devices tab, from the Domain list, select a domain, and then click >>.
3. In the MAC address box, type the MAC address for the new SIP device and click Save.

Adding multiple SIP devices

About this task
Use this procedure to add multiple new SIP devices to the system in bulk.

Procedure
1. From the Provisioning Client menu bar, select Clients > SIP Clients > SIP Clients Search to access the SIP Client Device portlet.
2. In the Domain Devices tab, from the Domain list, select a domain, and then click >>.
3. Click Bulk import.
4. On the Bulk Import tab, click Browse.
5. Navigate to and select the bulk import file and click Open.
6. Click Save.

---

### Modifying a SIP device

**About this task**
Modify a SIP device to add or remove users. You can use this procedure to delete a SIP device, or to regenerate the configuration files for the device.

**Procedure**
1. From the Provisioning Client menu bar, select **Clients > SIP Clients > Domain SIP Clients** to access the SIP Client Device portlet.
2. On the **Domain Devices** tab, from the **Domain** list, select a domain and click >>.
3. From the table, select the corresponding MAC address for the device that you want to modify.
4. On the **Modify Device** tab, in the **Add users** box, type a user name in the user@domain format and click Add.
5. Use the **First**, **Up**, **Down**, and **Last** buttons to change the order of users assigned to the device.
6. (Optional) To remove a user assigned to the device, click Remove.
7. (Optional) To remove all users assigned to the device, click Remove All.
8. To save your changes, click Save.
9. (Optional) To delete the device, on the **Modify Device** tab, click Delete.
10. (Optional) To regenerate configuration files for the device, on the **Modify Device** tab, click Delete.

---

### Deleting a SIP device

**About this task**
Delete a SIP device (and all related configuration files) that is no longer in use on the system.

**Procedure**
1. From the Provisioning Client menu bar, select **Clients > SIP Clients > Domain SIP Clients** to access the SIP Client Device portlet.
2. In the **Domain Devices** tab, from the **Domain** list, select a domain, and then click `>>`
3. From the **Device label** table column, select the check box of a device you want to delete.
4. Click **Delete**.
Chapter 11: Password policy procedures

About this task
Use the procedures in this section for password policies.

Use the Password Policy portlet to control the password policies on the system. A password policy defines the minimum length, minimum number of characters, minimum number of digits, and other password restrictions. For brief descriptions about subscriber password policy, see Password policy association with domains on page 41.

• Adding a subscriber password policy on page 105
• Assigning a subscriber password policy to a domain on page 109
• Listing, modifying, or deleting a subscriber password policy on page 110
• Modifying per-user password policies on page 114
• Subscriber Audit on page 115

Provider Managed Clients (PMC) password policy is not supported.

Adding a subscriber password policy
Use this procedure to add a subscriber password policy.

Before you begin
• You have full access to the domain.
• Password policies to be deleted are not associated with domains.

Procedure
1. From the Provisioning Client menu bar, select Services > Privacy/Security > Subscriber Password Policy to access the Password Policy portlet.
2. On the Add Subscriber Password Policy tab, configure the password policy parameters.
3. Click Save.
Adding a subscriber password policy job aid

About this task

The following job aid describes the parameters that appear on the Add Password Policy tab in the Password Policy portlet.

Tip:

For increased security, require subscribers to include digits, uppercase characters, and lowercase characters in their passwords.

Subscriber password policy parameters

About this task

The following table describes the subscriber password policies.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password policy name</td>
<td>Enter a password based on the policy rules (case sensitive, and from 1 to 30 characters in length).</td>
</tr>
<tr>
<td>Minimum length of password</td>
<td>This rule defines the minimum length of the password. In the range of 4–32. Default is 4. The following restriction applies: The Minimum Length of the Password value must be equal to or greater than the sum of Minimum Number of Digits, Minimum Number of Lowercase Characters, Minimum Number of Uppercase Characters, and Minimum Number of Special Characters.</td>
</tr>
<tr>
<td>Minimum number of digits in password</td>
<td>This rule defines the minimum number of digits in the password. In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of lowercase characters in password</td>
<td>This rule defines the minimum number of lowercase characters in the password. In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of uppercase characters in password</td>
<td>This rule defines the minimum number of uppercase characters in the password. In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of special characters in password</td>
<td>This rule defines the minimum number of special characters in the password. Valid special characters are . @ - _ &amp; ^ ? ! ( ) , / : ; ~ = +</td>
</tr>
</tbody>
</table>

Caution:

The system supports passwords up to a maximum of 511 characters. However, some phone clients limit the maximum length of passwords. Verify the capabilities of your phone before creating a long password.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum number of consecutive same character in password</td>
<td>This rule defines the maximum number of times a character can repeat consecutively in a password. When this value is configured to 0, checking for consecutive characters is disabled. In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of characters different from previous password</td>
<td>This rule defines the minimum number of characters in the password that must be different from the previous password. When this value is configured to 0, checking for the number of characters different from previous password is disabled. In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Password history</td>
<td>This rule defines the number of passwords the system stores in the subscriber's password history. The system rejects the reuse of passwords if they are found in the subscriber's history. When this value is configured to 0, users can reuse their current password. When this value is configured to 0, the Minimum number of characters different from previous password value must also be 0. In the range of 0 to 24. Default is 1.</td>
</tr>
<tr>
<td>User ID or reversed User ID permitted in password</td>
<td>This rule defines whether the user ID or reversed user ID is permitted in the password Default is enabled.</td>
</tr>
<tr>
<td>Check for dictionary words in password</td>
<td>This rule indicates whether or not the system performs dictionary word checking in passwords. When this rule is enabled, administrators are prevented from using passwords that are derived from dictionary words. When this rule enabled, the Minimum Length of Password field must be configured to 6 or greater. Default is disabled.</td>
</tr>
</tbody>
</table>

**Note:**

The system uses the Linux cracklib library to ensure that the password is not based on a dictionary word. This library manipulates the new password in various ways to determine if the new password is derived from a dictionary word, or based on the patterns from a standard keyboard.

The following examples do not consider other password policy setting, such as minimum number of special chars:

- aSdfqH1 is an invalid password --- the password is based on a dictionary word (keyboard pattern).
### Parameter Description

- **element123** is an invalid password --- the password is based on a dictionary word “element”.
- **12*Elements** is an invalid password --- the password is based on a dictionary word “element”.
- **element1234** is a valid password --- the password is not considered to be derived from word “element,” because the difference is more than 4 characters.
- **TwentyElements** is a valid password --- the password is not considered to be derived from word “element” or “Twenty” because the difference from each word is more than 4 characters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Initial password reset</strong></td>
<td>This rule forces a user to change the password when they access Personal Agent for the first time after the account is created. Select TRUE or FALSE. Default: TRUE</td>
</tr>
<tr>
<td><strong>Maximum failed login allowed</strong></td>
<td>This rule defines the number of failed authorization attempts allowed before a subscriber is locked out. Authorization attempts refer to the number of client requests processed by AS 5300 Session Manager. A lower value results in increased security; however it must be balanced against the Lockout Duration. A value of 3 gives sufficient leeway if the Lockout Duration value is hundreds of seconds. Enter a value in the range: 1–10. Default: 1</td>
</tr>
<tr>
<td><strong>Lockout duration in seconds</strong></td>
<td>This rule defines the number of seconds that subscribers are locked out after they exceed the maximum failed login attempts threshold. A value of 0 disables subscriber lockout. For increased security, use a higher value. However, longer lockout durations can also increase support calls from subscribers who find themselves unable to authenticate using the correct password. For example, a value of 900 seconds (15 minutes) provides a relatively long lockout duration, while a value of 3 seconds provides a lockout duration just long enough for a user to retype a password. Enter a value in the range: 0–3600. Default: 0</td>
</tr>
<tr>
<td><strong>Maximum password life in days</strong></td>
<td>This rule defines the number of days for which a subscriber's password is valid. Subscribers with an expired password can log on only to change their password. You can override this rule for individual subscribers. A value of 0 causes passwords never to expire.</td>
</tr>
</tbody>
</table>
### Assigning a subscriber password policy to a domain

Use this procedure to assign a subscriber password policy to a domain.

**Before you begin**

- You have full access to the domain.
- At least one password policy exists.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > List** to access the Domain panel.
2. On the **Details** tab, configure the **password policy name**.
3. Click **Save**.

---

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Minimum password life in hours     | This rule defines the minimum age a password must have before the user can change the password.  
A value of 0 disables this option, allowing users to change their password immediately.  
Enter a value in the range: 0-480. Default: 0 |
| Expiry notification in days        | This rule defines the number of days in advance that the system notifies users whose password is soon to expire.  
The value you enter for Expiry notification cannot be greater than the value for Maximum Password Life.  
A value of 0 disables notification.  
Enter a value in the range: 0-30. Default: 0 |
| Account Inactivity Period in days  | This rule defines the maximum number of consecutive days an subscriber account can be inactive before the system automatically disables the account.  
A value of 0 disables this option, so subscriber accounts are never disabled due to inactivity.  
Enter a value in the range: 0-180. Default: 0 |

---

**Note:**  
To disable Maximum password life in days for all subscribers, you must disable the feature in each Password Policy, and you must clear the Maximum Password Life override value, on a per-user basis, for any subscriber that has an override value configured.
Listing, modifying, or deleting a subscriber password policy

Use this procedure to list, modify, or delete a subscriber password policy.

⚠️ Important:

If you try to delete a password policy that is associated with a domain, an error message appears. You must assign a different password policy to the domains.

Before you begin

• You have full access to the domain.
• Password policies to be deleted are not associated with domains.

Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Subscriber Password Policy to access the Password Policy portlet.

2. On the Add Subscriber Password Policy tab, select the name of the password policy in the Name table column.

3. Configure the password policy parameters as required.

4. Click Save.

5. To delete a policy, in the Name table column, click the Delete link of a policy.

6. Enter a valid administrator's password in the confirmation window to delete the policy, and click Confirm.

Modifying the Subscriber password policy job aid

About this task

This job aid describes the parameters that appear on the Add Password Policy tab of the policy name you selected for modification.

For increased security, require subscribers to include digits, uppercase characters, and lowercase characters in their passwords.

Subscriber password policy parameters

About this task

The following table describes the subscriber password policies.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password policy name</td>
<td>Enter a password based on the policy rules (case sensitive, and from 1 to 30 characters in length).</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum length of password</td>
<td>This rule defines the minimum length of the password.</td>
</tr>
<tr>
<td></td>
<td>In the range of 4–32. Default is 4.</td>
</tr>
<tr>
<td></td>
<td>The following restriction applies:</td>
</tr>
<tr>
<td></td>
<td>• The Minimum Length of the Password value must be equal to or greater than the sum of Minimum Number of Digits, Minimum Number of Lowercase Characters, Minimum Number of Uppercase Characters, and Minimum Number of Special Characters.</td>
</tr>
<tr>
<td><strong>Caution:</strong></td>
<td>The system supports passwords up to a maximum of 511 characters. However, some phone clients limit the maximum length of passwords. Verify the capabilities of your phone before creating a long password.</td>
</tr>
<tr>
<td>Minimum number of digits in password</td>
<td>This rule defines the minimum number of digits in the password.</td>
</tr>
<tr>
<td></td>
<td>In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of lowercase characters in password</td>
<td>This rule defines the minimum number of lowercase characters in the password.</td>
</tr>
<tr>
<td></td>
<td>In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of uppercase characters in password</td>
<td>This rule defines the minimum number of uppercase characters in the password.</td>
</tr>
<tr>
<td></td>
<td>In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of special characters in password</td>
<td>This rule defines the minimum number of special characters in the password. Valid special characters are @ _ &amp; ^ ? ! ( ) , / \ ; : ~ = +</td>
</tr>
<tr>
<td></td>
<td>In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Maximum number of consecutive same character in password</td>
<td>This rule defines the maximum number of times a character can repeat consecutively in a password.</td>
</tr>
<tr>
<td></td>
<td>When this value is configured to 0, checking for consecutive characters is disabled.</td>
</tr>
<tr>
<td></td>
<td>In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Minimum number of characters different from previous password</td>
<td>This rule defines the minimum number of characters in the password that must be different from the previous password.</td>
</tr>
<tr>
<td></td>
<td>When this value is configured to 0, checking for the number of characters different from previous password is disabled.</td>
</tr>
<tr>
<td></td>
<td>In the range of 0 to 10. Default is 0.</td>
</tr>
<tr>
<td>Password history</td>
<td>This rule defines the number of passwords the system stores in the subscriber's password history. The system rejects the reuse of passwords if they are found in the subscriber's history.</td>
</tr>
<tr>
<td></td>
<td>When this value is configured to 0, users can reuse their current password.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Description</td>
<td>When this value is configured to 0, the Minimum number of characters different from previous password value must also be 0. In the range of 0 to 24. Default is 1.</td>
</tr>
<tr>
<td>User ID or reversed User ID permitted in password</td>
<td>This rule defines whether the user ID or reversed user ID is permitted in the password.</td>
</tr>
<tr>
<td></td>
<td>Default is enabled.</td>
</tr>
<tr>
<td>Check for dictionary words in password</td>
<td>This rule indicates whether or not the system performs dictionary word checking in passwords. When this rule is enabled, administrators are prevented from using passwords that are derived from dictionary words.</td>
</tr>
<tr>
<td></td>
<td>When this rule enabled, the Minimum Length of Password field must be configured to 6 or greater.</td>
</tr>
<tr>
<td></td>
<td>Default is disabled.</td>
</tr>
<tr>
<td>Note:</td>
<td>The system uses the Linux cracklib library to ensure that the password is not based on a dictionary word. This library manipulates the new password in various ways to determine if the new password is derived from a dictionary word, or based on the patterns from a standard keyboard.</td>
</tr>
<tr>
<td></td>
<td>The following examples do not consider other password policy setting, such as minimum number of special chars:</td>
</tr>
<tr>
<td></td>
<td>• aSdFgH1 is an invalid password --- the password is based on a dictionary word (keyboard pattern).</td>
</tr>
<tr>
<td></td>
<td>• element123 is an invalid password --- the password is based on a dictionary word “element”.</td>
</tr>
<tr>
<td></td>
<td>• 12*Elements is an invalid password --- the password is based on a dictionary word “element”.</td>
</tr>
<tr>
<td></td>
<td>• element1234 is a valid password --- the password is not considered to be derived from word “element,” because the difference is more than 4 characters.</td>
</tr>
<tr>
<td></td>
<td>• TwentyElements is a valid password --- the password is not considered to be derived from word “element” or “Twenty” because the difference from each word is more than 4 characters.</td>
</tr>
<tr>
<td>Initial password reset</td>
<td>This rule forces a user to change the password when they access Personal Agent for the first time after the account is created. Select TRUE or FALSE. Default: TRUE</td>
</tr>
<tr>
<td>Maximum failed login allowed</td>
<td>This rule defines the number of failed authorization attempts allowed before a subscriber is locked out. Authorization attempts refer to the number of client requests processed by AS 5300 Session Manager. A lower value results in increased security; however it must be balanced</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td>against the Lockout Duration. A value of 3 gives sufficient leeway if the Lockout Duration value is hundreds of seconds. Enter a value in the range: 1–10. Default: 1</td>
</tr>
<tr>
<td></td>
<td>Note: The AS 5300 Session Manager processes only the messages included in the Authorized Methods list (available in AS 5300 Element Manager Console).</td>
</tr>
<tr>
<td>Lockout duration in seconds</td>
<td>This rule defines the number of seconds that subscribers are locked out after they exceed the maximum failed login attempts threshold. A value of 0 disables subscriber lockout. For increased security, use a higher value. However, longer lockout durations can also increase support calls from subscribers who find themselves unable to authenticate using the correct password. For example, a value of 900 seconds (15 minutes) provides a relatively long lockout duration, while a value of 3 seconds provides a lockout duration just long enough for a user to retype a password. Enter a value in the range: 0–3600. Default: 0</td>
</tr>
<tr>
<td>Maximum password life in days</td>
<td>This rule defines the number of days for which a subscriber's password is valid. Subscribers with an expired password can log on only to change their password. You can override this rule for individual subscribers. A value of 0 causes passwords never to expire. Enter a value in the range: 0-180. Default: 0</td>
</tr>
<tr>
<td></td>
<td>Note: To disable Maximum password life in days for all subscribers, you must disable the feature in each Password Policy, and you must clear the Maximum Password Life override value, on a per-user basis, for any subscriber that has an override value configured.</td>
</tr>
<tr>
<td>Minimum password life in hours</td>
<td>This rule defines the minimum age a password must have before the user can change the password. A value of 0 disables this option, allowing users to change their password immediately. Enter a value in the range: 0-480. Default: 0</td>
</tr>
<tr>
<td>Expiry notification in days</td>
<td>This rule defines the number of days in advance that the system notifies users whose password is soon to expire. The value you enter for Expiry notification cannot be greater than the value for Maximum Password Life. A value of 0 disables notification. Enter a value in the range: 0-30. Default: 0</td>
</tr>
</tbody>
</table>
### Account Inactivity Period in days

This rule defines the maximum number of consecutive days an subscriber account can be inactive before the system automatically disables the account. A value of 0 disables this option, so subscriber accounts are never disabled due to inactivity. Enter a value in the range: 0-180. Default: 0.

### Modifying per-user password policies

#### About this task

Use this procedure to modify per-user subscriber password policies, which override policy policies.

#### Procedure

1. From the Provisioning Client menu bar, select **User > Search > Advanced Search**.
2. Select a domain, and click **Search**.
3. Click the name of the subscriber to modify.
4. Click the **Password Policy** tab.
5. Enter appropriate values to override password policies.
6. Click **Save**.

### Modifying per-user password policies job aid

#### About this task

This job aid describes the override parameters that appear on the **Password Policy** tab of the subscriber you selected for modification.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum Password Life</td>
<td>This field overrides, for the selected subscriber, the per-domain Maximum password life in days rule. Enter the number of days for which the subscriber's password is valid. A value of 0 turns off the per-user option, causing the system to apply the per-domain value to the selected subscriber. Enter a value in the range: 0-180. Default: 0</td>
</tr>
</tbody>
</table>
Subscriber Audit

About this task

Subscriber Audit is a configurable daily task that runs on each Provisioning Client and monitors subscriber accounts.

Table 13: Values monitored by Subscriber Audit

<table>
<thead>
<tr>
<th>Audit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Password Expiry Audit</td>
<td>This audit monitors the password expiry period of each subscriber account, based on the configured Maximum Password Life. The audit notifies subscribers whose password is due to expire, and forces a password change the next time the subscriber logs in.</td>
</tr>
<tr>
<td>Disable Inactivity Account</td>
<td>This audit monitors the account activity record for each subscriber, and disables any account that has no activity during Account Inactivity Period.</td>
</tr>
</tbody>
</table>

If your system has more than one Provisioning Client, enable Subscriber Password Expiry Audit on only one Provisioning Client.

Enabling or disabling Password Expiry Audit

About this task

Use this procedure to enable or disable Subscriber Audit (Password Expiry Audit).

Procedure

1. Use one of the following methods to access the AS 5300 Element Manager Console: if MCP FIPS is enabled: run `fips-mgmtconsole.bat`, if MCP FIPS is not enabled: run `https://<EM Console IP>:12121`
2. Log in as a user with administrator privilege.
3. Next to Network Elements, click +.
4. Next to Provisioning Managers, click +.
5. Next to `<prov name>`, click +.
6. Click Configuration Parameters.
7. In the Parm Group menu at the top of the Configuration Parameters window, select SubscriberAudit.
8. To enable Password Expiry Audit, configure EnableAudit to true, or to disable Password Expiry Audit, configure EnableAudit to false.
9. View the PROV log file, which is stored in `/var/mcp/oss/seclog/EM/security/MCP/`, and verify that it contains the following statement: `PROV1_0 SPISEC 654 INFO MAR16 16:38:10:445 MCP_15.1.0.0Password Expiry Audit <activated/deactivated>`.
Chapter 12: Resource management procedures

About this task
Use the procedures in this section to manage the available resources on a system.

- Listing system resources on page 116
- Assigning resources to a domain on page 116
- Viewing user count on page 117

Listing system resources

About this task
Use this procedure to view the number of units of resources allocated to a domain and the current number of existing and remaining units in the domain that can be added with the services.

Procedure
1. From the Provisioning Client menu bar, select Services > Resources to access the Resource Management portlet.
2. On the System Resources tab, click the name of the service in the Resource name table column to view the resource allocation for each service for a domain.

Assigning resources to a domain

About this task
Use this procedure to assign resources to a domain.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Resources to access the Resource Management portlet.
2. On the Domain resources tab, from the Select domain list, select an existing domain and click >>.
3. In the **Assign** column of each service, assign the required number of units of the resources.

⚠️ **Important:**

The service can be tagged as a resource; that is, there is a limit on the number of units of the service that can be assigned to the domain.

4. Click **Save**.

The units requested are validated against the remaining units for that resource in the system. The system saves the allocations if the validation passes.

---

**Viewing user count**

**About this task**

Use this procedure to view the License Key User Count of the system and the division of this resource among different domains.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > Domain Steps > Assign Resources**.

2. From the **Select domain** list, select an existing domain and click `>>`. 
Chapter 13: Service nodes configuration

About this task
Use the procedures in this section to configure the Service Nodes.

- Adding a node on page 118
- Listing nodes on page 120
- Assigning a domain to a node on page 120
- Adding a logical entity on page 120
- Listing, modifying, deleting a logical entity on page 122
- Assigning a node or a logical entity to a domain or subdomain on page 122

Adding a node

About this task
A Service node is defined as any network element in the system that provides a service such as gateways, conference servers, or voice mail servers. An administrator is able to change the IP addresses of a service node in order to accommodate network topology changes and change the IP addresses without reloading or redeploying the software. From the Service node portlet, an administrator can also add logical nodes, which consist of one or more service nodes. A service node contained within a logical node may have additional system- or user-defined parameters, such as a trkgrp, associated with it.

Use this procedure to add a physical node, such as a gateway or an Avaya Media Server and assign it the necessary attributes, such as its location and node type.

Procedure

1. From the Provisioning Client menu bar, select Translations > Service Node to access the Service Node portlet.
2. On the Node tab, configure the parameters as required.
3. Click Save.
Adding a node job aid

About this task

This job aid describes the parameters that appear on the **Node** tab in the Service Node portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Node Name       | Add the name of the node you want to add, such as the Audio Codes gateway, or the Avaya Media Server.  
|                 | **Important:** Ensure that a node is 1 through 40 characters long. It can only contain letters, numbers, and specific symbols.  
|                 | • Letters a to z, A to Z  
|                 | • Numbers 0 to 9  
|                 | • Symbols: underscore (_)                                                                                                                                 |
| Node Address    | Select either the Address Name or External Domain. These fields are mutually exclusive and cannot be selected simultaneously.  
|                 | **Address Name**: From the list, select one of the elements on the AS 5300 Element Manager: an Audio Codes gateway, a media server, or an Informational Element of type General or Gateway or Pooled Media resource.  
|                 | **External Domain**: Select this parameter if an IP address is unavailable.  
|                 | The External Domain address is used during an upgrade. If the host field on the gateway or the route on the logical entity cannot be parsed properly, the entire route is entered in this field, enabling all calls to work, and a log is generated for all these types. Any data available in this field is not validated and cannot be RE-IPed. |
| Node Type       | Select the node type from the list. For example, select the PRI gateway.                                                                                                                                 |
| Location        | Select the location of the node from the list.                                                                                                                                 |
| Is Trusted      | Select the check box if the node is trusted.                                                                                                                                 |
| Behind 1-to1 NAT| Select the check box if the Behind 1-to-1 NAT is available.                                                                                                                                 |
| Enhanced IM     | Select the check box if enhanced IM is available.                                                                                                                                 |
| Dual CLI        | Dual Calling Line ID (Dual CLI) is not supported.                                                                                                                                 |
Listing nodes

About this task
List nodes to view all the nodes provisioned on the system.

Procedure
1. From the Provisioning Client menu bar, select Translations > Service Node to access the Service Node portlet.
2. In the Node tab, scroll down to view the list of nodes and details for each node.

Assigning a domain to a node

About this task
Use this procedure to assign a domain to a node, such as a gateway or an Avaya Media Server.

Procedure
1. From the Provisioning Client menu bar, select Translations > Service Node to access the Service Node portlet.
2. On the Node tab, scroll down to view the list of nodes and details of each node.
3. Select the Domains link of the node name from the table.
4. Select the domain you want to associate with the node from the Available Domains list.
5. Click Save.
6. If you want to remove the domain you just added, select it from the Assigned Domains box and click Remove.
7. If you want to remove a domain already listed in the Assigned Domains box, then select the domain from the box and click Remove.
8. Click Save.

Adding a logical entity

About this task
Use this procedure to add a logical entity and to associate parameters with a specific physical node.

Procedure
1. From the Provisioning Client menu bar, select Translations > Logical Entity to access the Service Node portlet.
2. Configure the **Entity Name** > **Routable Services** > **Selection Algorithm**, parameters.

3. In the **Add route(s) to logical entity** section, configure the **Name**, **Node**, **Parms**, and **Weight (0-10)** parameters.

4. Click **Save** to add the new or modified logical entity.

### Adding a logical entity job aid

**About this task**

This job aid lists the parameters that you use to configure a new logical entity. The job aid also lists the weight-guidelines.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Entity Name</td>
<td>Type a name for the logical entity.</td>
</tr>
<tr>
<td>Routable Services</td>
<td>From the list, select the appropriate type as determined by the type of logical entity being added.</td>
</tr>
<tr>
<td>Selection Algorithm</td>
<td>From the list, select Sequential or Weighted Average. Assign one or more routes and associated weights to the entity.</td>
</tr>
<tr>
<td>Name</td>
<td>Name the route in this field.</td>
</tr>
<tr>
<td>Node</td>
<td>Select the appropriate node from the list.</td>
</tr>
<tr>
<td>Parms</td>
<td>Select the appropriate element from the list:</td>
</tr>
<tr>
<td></td>
<td>• Trunk Group—This parameter associates a node with a trunk group.</td>
</tr>
<tr>
<td></td>
<td>• Facility Domain—This is the domain associated with the outgoing requested URL.</td>
</tr>
<tr>
<td></td>
<td>• User—The field is used in conjunction with SIP and PSTN-type gateways. The only option currently available in the list is phone. The phone is added to requested URL in the outgoing SIP INVITE.</td>
</tr>
<tr>
<td></td>
<td>• Locale—Select the language of the device. Populate the field to add a locale to the outgoing SIP message.</td>
</tr>
<tr>
<td>Weight (0-10)</td>
<td>Type a value between 0 and 10 for the route weight.</td>
</tr>
</tbody>
</table>

The following guidelines apply for the Weight field:

- Routes with a zero weight are disabled.
- At least one route must be defined before the logical entity can be added.
- The total weight of all routes can be zero.
- The percentage of the total weight for each route is calculated automatically.
- Weight field has no meaning when Sequential Selection Algorithm is selected.
Listing, modifying, deleting a logical entity

About this task
Use this procedure to list, modify, or delete a logical entity.

From the Logical Entity tab on the Service Node portlet you can modify or delete information for existing logical entities provisioned in the system.

Procedure
1. From the Provisioning Client menu bar, select Translations > Logical Entity to access the Service Node portlet.
2. Scroll down to view the table that shows a list of logical entities.
3. To modify a logical entity, click the link for the logical entity in the Name table column.
4. On the Modify Logical Entity tab, change the parameters information and values.
5. Click Modify to save your changes.
6. To assign or remove domains to a logical entity, from the Logical Entity tab, click the Assign/Remove link for the logical entity in the Domains table column.
7. On the Available domains page, from the Assign Domain list, select the domain that you want to assign.
8. Click Add.
9. From the Assigned Domains list, select a domain and click Remove to remove the domain.
10. Click Save.
11. To delete a logical entity, from the Logical Entity tab, click the Delete link for the logical entity in the Delete table column.
12. In the confirmation dialog, type your administrator password and click Confirm.

Assigning a node or a logical entity to a domain or subdomain

About this task
Use this procedure to assign a node or logical entity to a subdomain at the root domain level.

Procedure
1. From the Provisioning Client menu bar, select Translations > Service Node to access the Service Node portlet.
2. On the List nodes from domain tab, select a domain in the Select domain pull-down and then click >>
3. In the list of nodes that appears, locate the node to which you want to assign a domain, and then click the corresponding link under the **Domains** column of the row.

4. In the **Available domains** list, select a domain that you want to assign to the node you selected in the previous step.

5. Click **Add**.
Chapter 14: System services management procedures

About this task
Use the procedures in this section to manage system services.

- Viewing service dependencies on page 125
- Banned User service configuration on page 125
- Branding announcements configuration on page 126
- Configuring access to branding routable services information on page 127
- Assigning branding files on page 128
- Configuring the Call Processing Language service on page 129
- Configuring a profile for a domain on page 130
- Configuring PPND for a domain on page 131
- Enabling the Global Address Book for a domain on page 132
- LDAP synchronization procedures on page 132
- Commercial Cost Avoidance and Hybrid Routing configuration on page 141
- Configuring Destination Code Controls service on page 147
- Location management procedures on page 149
- Border Control Point 7000 Series provisioning procedures on page 154
- Miscellaneous Groups service configuration on page 154
- Provider Managed Clients service configuration on page 154
- Ring Tone service configuration on page 154
- Security service configuration on page 158
- Status Reasons service configuration on page 160
- Configuring TR87 Client Control on page 161
- Treatments service configuration on page 165
- User Routing service configuration on page 173
- Vertical Service Code service configuration on page 175
- Assigning the SIP PBX service to a domain on page 177
Assigning the SIP Line service to a user on page 178

Provisioning PSI Distribution for a domain on page 179

---

**Viewing service dependencies**

**About this task**

Use this procedure to view required and mutually exclusive services for a specific service.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Assign Services** to access the User Services portlet.

2. Select the **Services Assignment** tab.

3. From the Select domain list, select a domain, and click `>>`.

4. Click **View service dependencies**.

   The User Services portlet shows you the services required for a specific service and the services that are mutually exclusive with a specific service.

---

**Banned User service configuration**

**About this task**

Use the procedures in this section to configure the Banned User service.

- **Banning users** on page 125
- **Viewing a list of banned users** on page 126

---

**Banning users**

**About this task**

You can ban an individual user or a group of users in a domain from using the Presence service. The ban affects all subdomains under the domain.

**Procedure**

1. From the Provisioning Client menu bar, select **User > Banned User** to access the Banned User Service portlet.

2. On the **Banned users** tab, from the **Select domain** list, select the domain and click `>>`.

3. Configure the **Party (user@domain)** and **Description** parameters.
4. Click **Save**.

**Banning users job aid**

This job aid describes the parameters for the **Banned users** tab in the Banned users Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Party (user@domain)      | To ban an individual user, use the following format:  
\[
\text{<username>@<domain_name.com>}.  
\]
To ban a group of users in a domain, use the following wildcard format:  
\[
\text{<*>@<domain_name.com>}.  
\]
| Description              | Enter a reason for banning the user or group of users to the domain list.                                                                 |

**Viewing a list of banned users**

**About this task**

Use this procedure to view a list of users banned from viewing the online status of a single user or a group of users in a domain. You can delete users from the list.

**Procedure**

1. From the Provisioning Client menu bar, select **User > Banned User** to access the Banned User Service portlet.

2. On the **Banned users** tab, from the **Select domain** list, select the domain and click `>>`.

3. To delete a user or a group of users from the ban list, click the **Delete** link next to the party to ban.

4. Enter a valid administrator's password in the confirmation window to delete the user or group of users.

**Branding announcements configuration**

**About this task**

Configure branding announcements to play the following two types of audio files to callers:
Table 14: Announcements service

<table>
<thead>
<tr>
<th>Announcement type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>treatment/cause</td>
<td>Informs the caller of the status of their call. These announcements tell the calling parties why their calls cannot be completed immediately. For example, the announcement might inform the caller that all circuits are busy.</td>
</tr>
<tr>
<td>branding</td>
<td>Identifies company or product names for commercial purposes.</td>
</tr>
</tbody>
</table>

⚠️ Important:

Avaya does not supply any default audio files with the Announcements service software. The system administrator must obtain and provision the audio files.

- Configuring access to branding routable services information on page 127
- Assigning branding files on page 128

---

Configuring access to branding routable services information

About this task

Use this procedure to configure branding routable services information for the Announcement logical entity (also called a pool).

With branding announcements, you can play marketing messages (to identify company or product names) to people who use your network. A branding announcement plays before the call routes to the called number. Branding announcements consist of one or more audio messages that you can chain together and for which you can specify a playback order. Additionally, you can configure these messages to loop.

Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Branding.
2. In the Branding Service portlet, select the Create Files tab.
3. From the Select domain list, select a Domain and click >>.
4. From the Select pool list, select a pool to which you want to assign branding files and click >>.
5. In the File field, enter the name of a branding file.
6. From the Locale list, select a locale and click Save.
7. Repeat steps 5 and 6 for each additional branding file.
Assigning branding files

About this task
Use this procedure to assign branding files in the domain where access to the Announcements service is needed.

Procedure
1. From the Provisioning Client menu bar, select Services > Announcements > Branding.
2. In the Branding Service portlet, select the Create Files tab.
3. In the Branding Service portlet, select the Assign Files tab.
4. From the Select domain list, select a domain and click >>.
5. From the Select pool list, select a pool to which you want to assign branding files and click >>.
6. From the Available files list, select a file that you want to use and click Copy.
7. In the Select repeat (times played) field, select the number of times for the system to replay the file.
8. Repeat 6 on page 128 and 7 on page 128 for each additional branding file you want to include.
9. Click Save.

Branding Media Management

About this task
Use the procedures in this section to manage Branding media.

- Adding media files for Branding on page 128
- Managing media files for Branding on page 129

Adding media files for Branding

About this task
Use this procedure to add media files for Branding.

Procedure
1. From the Provisioning Client menu bar, select Services > Announcements > Branding to access the Branding portlet.
2. In the Select domain list, select a domain in which to add the file and click >>.
3. In the Select pool list, select a pool in which to add the file and click >>.
4. Click Browse and select the file to add.
5. In the **Name** field, type the name for the new media file.
6. In the **Locale** list, select a locale in which to add the file.
7. Click **Save**.

**Adding media files for Branding job aid**

**About this task**

The following job aid describes the parameters for adding media files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a descriptive name for the new media file.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select a locale for the new media file.</td>
</tr>
</tbody>
</table>

**Managing media files for Branding**

**About this task**

Use this procedure to download or delete Branding media files.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Announcements > Branding** to access the Branding portlet.
2. *(Optional)* To delete a file, click **Delete** next to the file name. Enter your password and click **Confirm**.
3. *(Optional)* To delete all files, click **Remove All**. Enter your password, and click **Confirm**.
4. *(Optional)* To download a file, click **Download** next to the file name. Click **Browse** to select an application with which to open the file, **OR** click **OK** to save the file to your local PC.

---

**Creating, reviewing, and deleting domain bulletins**

IP Client Manager (IPCM) is not supported in Application Server 5300.

---

**Configuring the Call Processing Language service**

Use this procedure to configure the Call Processing Language (CPL) service.

**Before you begin**

- You have Services provisioninging rights.
### Procedure

1. From the Provisioning Client menu bar, select **Services > Call Routing > Call Processing Language** to access the CPL Service portlet.
2. Configure the parameters on the **System Data** tab.
3. Click **Save**.

---

#### Configuring the Call Processing Language service job aid

**About this task**

This job aid describes the parameters for the **System data** tab in the CPL portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default route rings</td>
<td>Enter a value for how many times the phone rings for the default route.</td>
</tr>
<tr>
<td>Default route converged no VM rings</td>
<td>Not used in Avaya Aura® Application Server 5300.</td>
</tr>
<tr>
<td>Default route no VM rings</td>
<td>Enter a value for how many times the phone rings for the default route for a user has no voice mail.</td>
</tr>
<tr>
<td>Route ring cycle time</td>
<td>Enter a value in this check box.</td>
</tr>
</tbody>
</table>

---

#### Configuring a profile for a domain

**About this task**

Use this procedure to configure a profile for a domain.

**Procedure**

1. From the Provisioning Client menu bar, select **Translations > Domain Profile** to access the Domain Profile Service portlet.
2. On the **Assign** tab, from the **Select domain** list, select the domain for which you want to configure a profile.
3. Click **>>**.
4. From the **Profile** list, select a profile for the domain.

For a SIP to PSTN call, the subdomain profile name is sent to the gateway when the telephony route defined on this subdomain is used. Likewise, the root profile name is sent to the gateway when the telephony route defined on this root domain is used. For example, when a SIP user of a subdomain calls a PSTN using the prefix of the telephony route defined on the root domain, the profile name of the root domain is sent on the gateway. However, if the subdomain and root domain reside on different AS 5300 Session Managers, the call fails.
To avoid this scenario, ensure that the subdomain has its own profile name and telephony route and also check the prefix through the translation tool.

For the VRDN configuration, the profile name must be the same as the profile name in Table TELEPROF in the CS 2000. CS 2000 NGSS is not supported.

5. Click **Save**.

---

### Configuring PPND for a domain

**About this task**

Use this procedure to configure Public/Private Name and Number Display (PPND) for a domain. Dual CLI is not supported.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Domain CLI** to access the DomainCLI Service portlet.

2. On the **Domain Service Data** tab, from the **Select domain** list, select the domain for which you want to configure PPND.

3. Click **>>**.

4. Configure the parameters on the **Domain Service Data** tab.

5. Click **Save**.

---

### Configuring PPND for a domain

**About this task**

Use this procedure to configure Public/Private Name and Number Display (PPND) for a domain. Dual CLI is not supported.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Domain CLI** to access the DomainCLI Service portlet.

2. On the **Domain Service Data** tab, from the **Select domain** list, select the domain for which you want to configure PPND.

3. Click **>>**.

4. Configure the parameters on the **Domain Service Data** tab.

5. Click **Save**.
Enabling the Global Address Book for a domain

About this task
Use this procedure to enable the Global Address Book for a domain.

Procedure
1. From the Provisioning Client menu bar, select Services > Client Interface > Global Address Book to access the Global Address Book Service portlet.
2. On the Domain Service Data tab, from the Select domain list, select the domain for which you want to configure CLI services, and then click >>.
3. Select the Global address book enabled check box to enable this service.
4. Click Save.

LDAP synchronization procedures

About this task
Use the procedures in this section to synchronize the Lightweight Directory Access Protocol (LDAP) directory.

- Configuring the LDAP server on page 132
- Configuring the LDAP schema on page 134
- Adding the Global Address Book Schema on page 138
- Using the Sync Filter Criteria on page 135
- Adding user defaults on page 136
- Using the LDAP Scheduler on page 137
- Configuring directories for a domain on page 139
- Using the Query Test Tool on page 140

Configuring the LDAP server

About this task
Use this procedure to configure the system to communicate with an Lightweight Directory Access Protocol (LDAP) server.

Procedure
1. From the Provisioning Client menu bar, select System > LDAP to access the LDAP Service portlet.
2. On the **Server** tab, from the **Select domain** list, select the domain for which you want to configure a server.

3. Click `>>`.

4. Click **Modify Server Details**.

5. Configure the parameters on the **Server Details** tab.

6. Click **Save**.

### Configuring the LDAP server job aid

#### About this task

This job aid describes the parameters for the **Server** tab of the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary server address</td>
<td>From the list, select the port of primary LDAP server to communicate with.</td>
</tr>
<tr>
<td>Primary server require server login</td>
<td>Check this box if you want to require login to the server.</td>
</tr>
<tr>
<td>Primary server user name</td>
<td>Enter the user name used to connect to LDAP server. Ensure that the LDAP server user name cannot be more than 128 characters.</td>
</tr>
<tr>
<td>Primary server password</td>
<td>Enter a password of the LDAP server, if necessary, for querying the server. Select the LDAP server logical name from the list.</td>
</tr>
<tr>
<td>Use Secure Connection</td>
<td>Check this box if you want to use secure connection. Connect to LDAP server with a secure socket through Secure Socket Layer (SSL) or through a normal TCP socket. The certificate must be imported to the JVM through the keytool executable available as part of the Sun JRE.</td>
</tr>
<tr>
<td>Secondary server address</td>
<td>From the list, select the port of secondary LDAP server to communicate with.</td>
</tr>
<tr>
<td>Secondary server require server login</td>
<td>Check this box if you want to require login to the server.</td>
</tr>
<tr>
<td>Secondary server user name</td>
<td>Enter the user name used to connect to LDAP server. Ensure that the LDAP server user name cannot be more than 128 characters.</td>
</tr>
<tr>
<td>Secondary server password</td>
<td>Enter a password of the LDAP server, if necessary, for querying the server. Select the LDAP server logical name from the list.</td>
</tr>
<tr>
<td>Secondary server use secure connection</td>
<td>Check this box if you want to use secure connection. Connect to LDAP server with a secure socket through Secure Socket Layer (SSL) or through a normal TCP socket. The certificate must be imported to the JVM through the keytool executable available as part of the Sun JRE.</td>
</tr>
</tbody>
</table>
Configuring the LDAP schema

About this task
Use this procedure to configure the schema that the system uses from the LDAP server for creating new subscribers.

Procedure
1. From the Provisioning Client menu bar, select System > LDAP to access the LDAP Service portlet.
2. On the Sync Schema tab, from the Select domain list, select the domain.
3. Click >>.
4. Configure the parameters on the Sync Schema tab.
5. Click Save.

Configuring the LDAP schema job aid

About this task
This job aid describes the parameters for the Sync Schema tab of the LDAP Service portlet.

You can store numbers in the LDAP database in the international GSM format (+ <country_code> <number>), for example, +331444441234. The system automatically removes the ‘+’ from the following fields, eliminating the need for administrator interaction:

• Business Phone
• Home Phone
• Cell Phone
• Pager
• Fax

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Mandatory / Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Distinguished Name</td>
<td>DN</td>
<td>Mandatory</td>
<td>A DN is used to distinguish one entry in an LDAP database from another as in the following example of an entry whose userid is joeb: dn: uid=joeb, ou=Internal, ou=People, o=ABC</td>
</tr>
<tr>
<td>User name</td>
<td>uid</td>
<td>Mandatory</td>
<td>The uid field is part of the RDN for this particular entry. The uid field must be unique for every subscriber in the domain.</td>
</tr>
<tr>
<td>First Name OR</td>
<td>givenName</td>
<td>Mandatory</td>
<td>The first name of the subscriber. OR</td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Mandatory / Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title and First Name</td>
<td></td>
<td>Optional</td>
<td>Optionally, enter rank givenName, to describe the title (or rank) plus the first name of the subscriber.</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Mandatory</td>
<td>The last name of the subscriber.</td>
</tr>
<tr>
<td>Email</td>
<td>mail</td>
<td>Optional</td>
<td>The e-mail address of the subscriber.</td>
</tr>
<tr>
<td>Business Phone</td>
<td>telephoneNum</td>
<td>Optional</td>
<td>The work phone number of the subscriber.</td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Optional</td>
<td>The home phone number of the subscriber.</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>mobile</td>
<td>Optional</td>
<td>The cell phone number of the subscriber.</td>
</tr>
<tr>
<td>Pager</td>
<td>pager</td>
<td>Optional</td>
<td>The pager number of the subscriber.</td>
</tr>
<tr>
<td>Fax</td>
<td>facsimileTelephoneNumber</td>
<td>Optional</td>
<td>The fax number of the subscriber.</td>
</tr>
<tr>
<td>Jpeg Photo</td>
<td>JpegPhoto</td>
<td>Optional</td>
<td>The photograph of the subscriber.</td>
</tr>
<tr>
<td>MCP User</td>
<td>LDAP schema name used for the user</td>
<td>Optional</td>
<td>The LDAP schema name used for the subscriber.</td>
</tr>
</tbody>
</table>

Selecting attributes as shown in the table prevents the subscriber from modifying these fields through the Avaya Aura® Application Server 5300 Personal Agent. This is necessary because otherwise a subscriber could modify a jpegPhoto through the Avaya Aura® Application Server 5300 Personal Agent, and then, during the next synchronization operation, the jpegPhoto would be overwritten with whatever jpegPhoto was present in the LDAP database.

If you leave any of the non-mandatory fields blank, then during an LDAP synchronization operation, the blank attributes are not synchronized, and the subscriber is subsequently allowed to modify those particular fields through the Avaya Aura® Application Server 5300 Personal Agent.

---

## Using the Sync Filter Criteria

### About this task

Use this procedure to specify which user names starting with selected characters should be synchronized during an LDAP sync.

### Procedure

1. From the Provisioning Client menu bar, select **System > LDAP** to access the LDAP Service portlet.
2. On the **Sync Filter** tab, from the **Select domain** list, select the domain.
3. Click >>.
4. Configure the parameters on the **Sync Filter** tab.
5. Select **Save**.

⚠️ **Important:**

If you select one or more parameters, you add only the user names that start with the selected parameters to the system. If you leave the filters blank, LDAP synchronization occurs for all user names that start with any supported character.

**Using the Sync Filter Criteria job aid**

This job aid describes the parameters for the **Sync Filter** tab of the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Any Number</td>
<td>Select the Any Number check box. The numbers are from 0 through 9.</td>
</tr>
<tr>
<td>Any Alpha Character</td>
<td>Select the Any Alpha Character check box. The alpha character are from A through Z.</td>
</tr>
<tr>
<td>Special Character(s)</td>
<td>Select the Special Character check box.</td>
</tr>
<tr>
<td></td>
<td>The special characters list can be a list of numbers and/or alpha characters previously specified or a hyphen (-), comma (,), underscore (_), and period (.).</td>
</tr>
<tr>
<td></td>
<td>Note that a &quot;,&quot; (comma) must be used between selected characters</td>
</tr>
<tr>
<td></td>
<td>The following example shows the user names that an administrator selects, separating the numbers and characters with commas:</td>
</tr>
<tr>
<td></td>
<td>“f”, “g”, “1”, “a”, “u”, “e”, “s”</td>
</tr>
</tbody>
</table>

---

**Adding user defaults**

**About this task**

Use this procedure to add user defaults for a new user.

**Procedure**

1. From the Provisioning Client menu bar, select **System > LDAP** to access the LDAP Service portlet.
2. On the **Sync User Defaults** tab, from the **Select domain** list, select the domain.
3. Click >>.
4. Configure the parameters on the **Sync User Defaults** tab.
5. Click **Save**.
Adding user defaults job aid

About this task

This job aid describes the parameters for the Sync User Defaults tab in the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default User Password</td>
<td>Type the default password. Password should be 4-20 characters in length and should have minimum 4 digits and minimum 0 characters in it. The valid characters are A-Z, a-z, and !, &amp; , (, ) , ' , , - , ., ,, ?, @, ^ and _ . Password initial reset is not required. The password should match the default domain password policy if the policy was changed after the synchronization was scheduled. That particular synchronization operation will not be affected until another synchronization is scheduled or web was restarted. In such case, the password policy should match that of domain password.</td>
</tr>
<tr>
<td>Default Class of Service</td>
<td>Select the default class of service from the list.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select the language from the list.</td>
</tr>
<tr>
<td>Time Zone</td>
<td>Select the time zone from the list.</td>
</tr>
<tr>
<td>Service set</td>
<td>Select the default service set from the list.</td>
</tr>
<tr>
<td>Status</td>
<td>Select Active or Inactive from the list.</td>
</tr>
</tbody>
</table>

Using the LDAP Scheduler

Use the LDAP scheduler to configure when automatic synchronization of an LDAP database with the system will occur. The administrator can schedule queries on a monthly, weekly, daily, or immediate basis.

Before you begin

• Ensure to schedule LDAP synchronization during the off-peak hours to preserve system resources and bandwidth.

Procedure

1. From the Provisioning Client menu bar, select System > LDAP to access the LDAP Service portlet.
2. On the Sync Scheduler tab, from the Select domain list, select the domain.
3. Click >>.
4. In the Scheduler configuration box, select Enable scheduler, and then select the appropriate check boxes in the Time and Frequency sections to create the synchronization schedule.
If the scheduler is enabled, you may see the current status when you access the scheduler for the first time.

5. Click to select the **Save** check box to run the scheduler at a later time.

6. Select **Sync Now** check box to start the synchronization process immediately.

<table>
<thead>
<tr>
<th>If</th>
<th>Then</th>
</tr>
</thead>
</table>
| the administrator chooses to begin the synchronization process immediately or at a later time | the following warning message appears:  
  • The synchronization operation could impact system performance.  
  • Avaya recommends that the synchronization be scheduled during off-peak hours. |
| the administrator runs the synchronization process and it fails                  | system logs indicate one or more of the following failure reasons:  
  • LDAP Server Connection Failure—During the LDAP synchronization operation, the Primary and Secondary servers were unreachable.  
  • Maximum User Limit Reached—During the LDAP synchronization operation, the maximum number of users allowed to be provisioned was reached. |

After a synchronization is complete, the system enforces the same password rules for the new user accounts as it does for user accounts added directly from the Provisioning Client.

**Important:**

The administrator also can turn on or off the synchronization operation for a given domain. The synchronization schedule is based on the time configuration of the server that hosts the Provisioning Manager. If the server time is incorrect, the synchronization runs at the incorrect time.

---

**Adding the Global Address Book Schema**

**About this task**

Use this procedure to add the Global Address Book (GAB) Schema.

**Procedure**

1. From the Provisioning Client menu bar, select **System > LDAP** to access the LDAP Service portlet.
2. On the **GAB Schema** tab, from the **Select domain** list, select the domain.
3. Click **>>**.
4. On the **GAB Schema** tab, configure the parameters as required.
5. Click **Save**.
Adding the Global Address Book Schema job aid

About this task

This job aid describes the parameters for the GAB Schema tab in the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP Distinguished Name</td>
<td>DN</td>
<td>Mandatory</td>
<td>A DN is used to distinguish one entry in an LDAP database from another as in the following example of an entry whose userid is joeb: dn: uid=joeb, ou=Internal,ou=People,o=ABC</td>
</tr>
<tr>
<td>User name</td>
<td>uid</td>
<td>Mandatory</td>
<td>The uid field is part of the RDN for this particular entry. The uid field must be different for every user in the domain.</td>
</tr>
<tr>
<td>First Name OR Title and First Name</td>
<td>givenName</td>
<td>Mandatory</td>
<td>The first name of the subscriber. OR Optionally, enter rank givenName, to describe the title (or rank) plus the first name of the subscriber.</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Mandatory</td>
<td>The last name of the user.</td>
</tr>
<tr>
<td>Email</td>
<td>mail</td>
<td>Optional</td>
<td>The e-mail address of the user.</td>
</tr>
<tr>
<td>Business Phone</td>
<td>telephoneNumber</td>
<td>Optional</td>
<td>The work phone number of the user.</td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Optional</td>
<td>The home phone number of the user.</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>mobile</td>
<td>Optional</td>
<td>The cell phone number of the user.</td>
</tr>
<tr>
<td>Pager</td>
<td>pager</td>
<td>Optional</td>
<td>The pager number of the user.</td>
</tr>
<tr>
<td>Fax</td>
<td>facsimileTelephoneNumber</td>
<td>Optional</td>
<td>The fax number of the user.</td>
</tr>
<tr>
<td>Jpeg Photo</td>
<td>JpegPhoto</td>
<td>Optional</td>
<td>The photograph of the user.</td>
</tr>
</tbody>
</table>

Note:
Data from the LDAP scheme overrides data from the local database.

Configuring directories for a domain

About this task

Use this procedure to configure directories for a domain

Procedure

1. From the Provisioning Client menu bar, select System > LDAP to access the LDAP Service portlet.
2. On the **GAB Directory Services** tab, from the **Select domain** list, select the domain.
3. Click `>>`.
4. On the **GAB Directory Services** tab, configure the parameters as required.
5. Click **Save**.

### Configuring directories for a domain job aid

#### About this task

This job aid describes the parameters for the **GAB Directory Services** tab in the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory response timeout</td>
<td>Type a maximum of 5 digit value in this field. This value is the timeout value in milliseconds for the search directory. The default value is 3000 milliseconds.</td>
</tr>
<tr>
<td>Enable Local Global Address Book</td>
<td>Check the box to enable the local global address book.</td>
</tr>
<tr>
<td>Enable External Directory</td>
<td>Check the box to enable the external directory.</td>
</tr>
</tbody>
</table>

### Using the Query Test Tool

Use the Query Test Tool to query the LDAP database for a user to verify connectivity to a configured LDAP database for LDAP Sync.

#### Before you begin

- Ensure that the LDAP Server Configuration sheet is already configured before you use this tool.

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>This tool is not used for the SLR multisite LDAP database.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>It is recommended that a search be performed on the LDAP attributes of Global Address Book. Refer to the <strong>GAB Schema</strong> tab in the LDAP Service portlet.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Due to the Open LDAP Server limitation on schema definition of the attribute facsimileTelephoneNumber, EQUALITY or SUBSTRING search on facsimileTelephoneNumber is not supported.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Important:</th>
</tr>
</thead>
<tbody>
<tr>
<td>The search records obtained depend on the schema definition of the LDAP attribute. If the EQUALITY is caseExactIA5Match and no SUBSTRING definition, the search should be performed by using the exact string or by <code>*</code> (asterisk).</td>
</tr>
</tbody>
</table>
Procedure

1. From the Provisioning Client menu bar, select System > LDAP to access the LDAP Service portlet.
2. On the Query Test Tool tab, from the Select domain list, select the domain.
3. Click >>.
4. On the Query Test Tool tab, configure the search parameters as required.
5. Click Search.

Using the Query Test Tool job aid

This job aid describes the parameters for the Query Test Tool tab in the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LDAP attribute to search on</td>
<td>Enter the name of the LDAP Database Attribute. The name can be up to 120 characters in length.</td>
</tr>
<tr>
<td>Attribute search string</td>
<td>Enter the value of the LDAP Database Attribute. The value can be up to 120 characters in length.</td>
</tr>
</tbody>
</table>

Commercial Cost Avoidance and Hybrid Routing configuration

About this task

Use the procedures in this section to configure the following features:

- Hybrid routing—so that the Avaya Aura® Application Server 5300 can identify IP and TDM routes, and then route them appropriately
- Commercial Cost Avoidance—so that users can dial a public number and have the call routed across the private network if the public number maps to a private one.

- Configuring the SLR LDAP server on page 141
- Configuring LDAP operation timeouts on page 142
- Configuring the SLR LDAP schema on page 143
- Configuring a multisite domain on page 89
- Configuring CCA feature translations on page 145

Configuring the SLR LDAP server

About this task

Configure the Subscriber Lookup and Routing (SLR) Lightweight Directory Access Protocol (LDAP) server to specify the LDAP server for a root domain.
Procedure
1. From the Provisioning Client menu bar, select **System > LDAP** to access the LDAP Service portlet.
2. On the **SLR Server** tab, from the **Select domain** list, select the domain for which you want to configure a server.
3. Click `>>`.
4. Click **Modify Server Details**.
5. Configure the parameters on the **Server Details** tab.
6. Click **Save**.

Configuring the SLR LDAP server job aid

**About this task**

This job aid describes the parameters for the **SLR Server** tab of the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing server address</td>
<td>From the list, select the SLR LDAP server.</td>
</tr>
<tr>
<td>Require server login</td>
<td>Select this box to require log on to the server. If you select this option, you must specify values for the Server username and the Server password parameters.</td>
</tr>
<tr>
<td>Server user name</td>
<td>Enter the user name used to connect to LDAP server. Ensure that the LDAP server user name cannot be more than 128 characters.</td>
</tr>
<tr>
<td>Server password</td>
<td>Enter a password of the LDAP server, if necessary, for querying the server. Select the LDAP server logical name from the list.</td>
</tr>
<tr>
<td>Use Secure Connection</td>
<td>Check this box if you want to use a secure connection. Connect to LDAP server with a secure socket through Secure Socket Layer (SSL) or through a normal TCP socket. The certificate must be imported to the JVM through the keytool executable available as part of the Sun JRE.</td>
</tr>
</tbody>
</table>

Configuring LDAP operation timeouts

**About this task**

Configure the LDAP Read response and Write response timeouts to specify the time in milliseconds for clients to wait for a response from the LDAP server. After the configured time elapses without response from the LDAP server, LDAP operations fail.

**Procedure**
1. From the Provisioning Client menu bar, select **System > LDAP** to access the LDAP Service portlet.
2. On the **SLR Configuration** tab, from the **Select domain** list, select the domain for which you want to configure a server.

3. Click `>`.

4. Configure the **Read response timeout** and the **Write response timeout**.

5. Click **Save**.

### Configuring LDAP operation timeouts job aid

**About this task**

This job aid describes the parameters for the LDAP operation timeouts.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read response timeout</td>
<td>The length of time (in milliseconds) for a client to wait for a response from the LDAP server, for a read operation.</td>
</tr>
<tr>
<td>Write response timeout</td>
<td>The length of time (in milliseconds) for a client to wait for a response from the LDAP server, for a write operation.</td>
</tr>
</tbody>
</table>

### Configuring the SLR LDAP schema

**About this task**

Configure the SLR LDAP schema for the Subscriber Location and Routing (SLR), Commercial Cost Avoidance (CCA), and hybrid routing features, which all use the same LDAP database and schema.

**Procedure**

1. From the Provisioning Client menu bar, select **System > LDAP** to access the LDAP Service portlet.
2. On the **SLR Schema** tab, from the **Select domain** list, select the domain.
3. Click `>`.
4. Configure the parameters.
5. Click **Save**.

### Configuring the SLR LDAP schema job aid

**About this task**

This job aid describes the parameters for the **SLR Schema** tab of the LDAP Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RTS DB support</td>
<td>Unchecked</td>
<td>Optional</td>
<td>If you select this check box the user will be saved to the LDAP database as</td>
</tr>
<tr>
<td>Parameter</td>
<td>Default value</td>
<td>Mandatory or Optional</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>---------------</td>
<td>-----------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>homed in root domain,</td>
<td></td>
<td></td>
<td>otherwise the user will be saved as homed in sub-domain.</td>
</tr>
<tr>
<td>Note:</td>
<td></td>
<td></td>
<td>You need to select this check box if you are using either CCA or hybrid routing.</td>
</tr>
<tr>
<td>LDAP Distinguished Name</td>
<td>DN</td>
<td>Mandatory</td>
<td>The name of the schema attribute in the LDAP database, which holds the distinguished name or DN of the entry. A DN distinguishes one entry in an LDAP database from another as in the following example of an entry where the userid is joeb: dn: uid=joeb, ou=Internal,ou=People,o=ABC For CCA and hybrid routing, this maps to DN.</td>
</tr>
<tr>
<td>User name</td>
<td>uid</td>
<td>Mandatory</td>
<td>The name of the schema attribute in the LDAP database, which holds the Application Server 5300 SIP username. This parameter must be different for every user in the domain. For CCA and hybrid routing, this maps to uid.</td>
</tr>
<tr>
<td>First Name</td>
<td>givenName</td>
<td>Mandatory</td>
<td>The name of the schema attribute in the LDAP database, which holds the first name of the user. Although required, CCA and hybrid routing, do not use this parameter.</td>
</tr>
<tr>
<td>Last Name</td>
<td>sn</td>
<td>Mandatory</td>
<td>The name of the schema attribute in the LDAP database, which holds the last name of the user. Although required, CCA and hybrid routing, do not use this parameter.</td>
</tr>
<tr>
<td>Email</td>
<td>mail</td>
<td>Optional</td>
<td>The e-mail address of the user.</td>
</tr>
<tr>
<td>Business Phone</td>
<td>telephoneNumber</td>
<td>Optional</td>
<td>The work phone number of the user.</td>
</tr>
<tr>
<td>Home Phone</td>
<td>homePhone</td>
<td>Optional</td>
<td>The home phone number of the user.</td>
</tr>
<tr>
<td>Cell Phone</td>
<td>mobile</td>
<td>Optional</td>
<td>The cell phone number of the user.</td>
</tr>
<tr>
<td>Pager</td>
<td>pager</td>
<td>Optional</td>
<td>The pager number of the user.</td>
</tr>
<tr>
<td>Fax</td>
<td>facsimileTelephone Number</td>
<td>Optional</td>
<td>The fax number of the user.</td>
</tr>
<tr>
<td>Sip User name</td>
<td>sipUsername</td>
<td>Optional</td>
<td>The name of the field in LDAP database, which maps to sipUsername For CCA and hybrid routing, this maps to sipUsername.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default value</th>
<th>Mandatory or Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sip Alias</td>
<td>sipAlias</td>
<td>Optional</td>
<td>The name of the schema attribute in the LDAP database, which holds the fully qualified public number for the user. For CCA and hybrid routing, this maps to sipAlias.</td>
</tr>
<tr>
<td>Sip Directory number</td>
<td>dirNumber</td>
<td>Optional</td>
<td>The name of the schema attribute in the LDAP database, which holds the private number for the user. For CCA and hybrid routing, this maps to dirNumber.</td>
</tr>
<tr>
<td>SESM home</td>
<td>serverHome</td>
<td>Optional</td>
<td>The home AS 5300 Session Manager.</td>
</tr>
<tr>
<td>IsMobile</td>
<td>IsMobile</td>
<td>Optional</td>
<td></td>
</tr>
<tr>
<td>Sip Subscriber Type</td>
<td>subscriber Type</td>
<td>Optional</td>
<td>The name of the field in LDAP database, which maps to the CCA ID of Master LSC. For CCA and hybrid routing, this maps to LSCCCAID.</td>
</tr>
<tr>
<td>LSCCCAID</td>
<td>LSCCCAID</td>
<td>Optional</td>
<td>The name of the field in LDAP database, which maps to the CCA ID of Master LSC. For CCA and hybrid routing, this maps to LSCCCAID.</td>
</tr>
<tr>
<td>SCCAID</td>
<td>SCCAID</td>
<td>Optional</td>
<td>The name of the field in LDAP database, which maps to the CCA ID of the SS that serves the Master LSC. For CCA and hybrid routing, this maps to SCCAID.</td>
</tr>
</tbody>
</table>

### Configuring CCA feature translations

Configure CCA feature translations to:

- distinguish CCA calls from regular calls. If the number matches the To, From, Min, or Max Digits parameter values from CCA feature translation, the call is a CCA call.
- provide a unique fully qualified international public number (even if the dialed digits are a local or national number) to use to search the LDAP database.

⚠️ **Important:**

If you configure two or more translations in the same domain with identical To, From, Min, or Max Digits parameter values, the system uses the last translation added. Avaya does not recommend this configuration.

### Before you begin

- You have Commercial Cost Avoidance provisioning rights.

  If you do not have delete privileges, the Delete link does not appear for configured translations. If you do not have write privileges, the Save button does not appear on the Feature Translation tab.
Procedure

1. From the Provisioning Client menu bar, select Services > Call Routing > Commercial Cost Avoidance to access the Commercial Cost Avoidance Service portlet.

2. On the Feature Translation tab, from the Select domain list, select the domain.

3. Click >>.

4. Configure the parameters.

5. Click Save.

Configuring CCA feature translations job aid

About this task

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory / Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Enter a meaningful name that specifies the translation record in the Name field. The name must be 1 to 32 characters in length.</td>
</tr>
<tr>
<td>From digits</td>
<td>Mandatory</td>
<td>Enter a value that matches the To digits parameter.</td>
</tr>
<tr>
<td>To digits</td>
<td>Mandatory</td>
<td>Enter a value that matches the From digits parameter.</td>
</tr>
<tr>
<td>Min digits</td>
<td>Mandatory</td>
<td>Enter the minimum number of digits for a number.</td>
</tr>
<tr>
<td>Max digits</td>
<td>Mandatory</td>
<td>Enter the maximum number of digits for a number.</td>
</tr>
<tr>
<td>Remove digits</td>
<td>Optional</td>
<td>Enter the number of prefix digits to remove.</td>
</tr>
<tr>
<td>Query Prefix</td>
<td>Optional</td>
<td>Enter the VSC prefix. The prefix must be 2 to 32 digits in length.</td>
</tr>
</tbody>
</table>

The following figure provides an example of feature translation configuration.

<table>
<thead>
<tr>
<th>Name</th>
<th>From digits</th>
<th>To digits</th>
<th>Min digits</th>
<th>Max digits</th>
<th>Remove digits</th>
<th>Query Prefix</th>
<th>Delete</th>
</tr>
</thead>
<tbody>
<tr>
<td>long_distance</td>
<td>99</td>
<td>98</td>
<td>13</td>
<td>13</td>
<td>2</td>
<td></td>
<td>Delete</td>
</tr>
<tr>
<td>international</td>
<td>99011</td>
<td>90011</td>
<td>16</td>
<td>16</td>
<td>6</td>
<td></td>
<td>Delete</td>
</tr>
<tr>
<td>7digits_local</td>
<td>99</td>
<td>99</td>
<td>12</td>
<td>12</td>
<td>2</td>
<td>7</td>
<td>Delete</td>
</tr>
<tr>
<td>7digits_local</td>
<td>99</td>
<td>99</td>
<td>12</td>
<td>12</td>
<td>2</td>
<td>1718</td>
<td>Delete</td>
</tr>
</tbody>
</table>

Figure 22: Feature translations example

The following points apply to Figure 22: Feature translations example on page 146.

- The example shows the correct CCA feature translations configuration for a number with a Country Code of 1 and a City Code of 718.
- If a subscriber dials the CCA code + local number (i.e. 991234567), the “7digits_local” translation applies. The CCA service removes “99” and adds “1718” (Prefix) to the number. This results in “17181234567” (which is the fully qualified international number of the terminating party). This is the number that will be used to query the LDAP.
- If a subscriber dials the CCA code + national number (i.e. 997181234567), the “10digits_local” translation applies. The CCA service removes “99” and adds “1”. This also results in “17181234567”.

System services management procedures
• If a subscriber dials the CCA code + international (US) number (i.e. 9817181234567), the “long_distance” translation applies. The CCA service removes “98” and does not add any digits. Again, this results in “17181234567”.

• If a subscriber dials the CCA prefix + international (not US) number (i.e. 9801117181234567), the “international” translation applies. The CCA service removes “98011” and does not add any digits resulting in “17181234567”.

• If no LDAP entry for the public number exists, or if the CCA routed call fails to complete, the system reroutes the call using the dialed digits—with or without the CCA code (depending on the value entered for “Remove digits”).

Configuring Destination Code Controls service

Use this procedure to configure Destination Code Controls (DCC) service. DCC is a manual protective control that restricts calls to specific areas or destinations that have been temporarily designated as difficult or impossible to reach. DCC is applied at the LSC or the MFSS to limit the number of calls to the specific destination.

This procedure allows you to specify the percentage of calls that need to be blocked temporarily for the destinations designated as ‘difficult to reach’.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Restrictions > Destination Code Controls to access Destination Code Controls service portlet

2. On the DCC prefixes tab, select a domain from Select domain list and click >>

3. Specify Name, From digits, To digits, Min digits and Max digits for DCC prefix.

4. In the Percent of blocked calls field, specify the percentage of incoming calls that are to be rejected by the core.

5. Select the Enable check box to enable the DCC entry.

   Note:
   You can also enable/disable the DCC entries by selecting or clearing the corresponding Enabled fields in the DCC prefixes table.

6. Click Save to save the changes for the current DCC entry.

7. Click Activate to activate/de-activate the modified DCC entries in the DCC prefixes table.

Configuring Destination Code Controls service job aid

The North American numbering format ‘NPA-NXX-XXXX’, is summarized in the following table:
### Component List

<table>
<thead>
<tr>
<th>NPA</th>
<th>Numbering Plan Area Code</th>
<th>[2-9] for the first digit, and [0-9] for the second and third digits</th>
</tr>
</thead>
<tbody>
<tr>
<td>NXX</td>
<td>Central Office (exchange) code</td>
<td>[2-9] for the first digit, and [0-9] for the second and third digits</td>
</tr>
<tr>
<td>XXXXX</td>
<td>Subscriber Number</td>
<td>0–9 for all four digits</td>
</tr>
</tbody>
</table>

Use the DCC prefixes tab of the DCC service portlet to configure an entire Numbering Plan Area (NPA) or a group of specific NNX codes within an NPA. You can also configure a single NNX or NNX-D, a hundred group within an NNX.

This job aid describes the parameters for the DCC prefixes tab in DCC portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Mandatory/Optional</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Mandatory</td>
<td>Specify a meaningful name to identify the DCC record. The name must be 1 to 32 characters in length.</td>
</tr>
<tr>
<td>From digits</td>
<td>Mandatory</td>
<td>Specify the starting digits for DCC prefix. This parameter must have the same number of digits as the To digits parameter.</td>
</tr>
<tr>
<td>To digits</td>
<td>Mandatory</td>
<td>Specify the ending digits for DCC prefix. This parameter must have the same number of digits as the From digits parameter.</td>
</tr>
<tr>
<td>Min digits</td>
<td>Mandatory</td>
<td>Type the minimum number of digits for a number.</td>
</tr>
<tr>
<td>Max digits</td>
<td>Mandatory</td>
<td>Type the maximum number of digits for a number.</td>
</tr>
<tr>
<td>Percent of blocked calls</td>
<td>Mandatory</td>
<td>Specify the percentage of incoming calls which are to be rejected by core. Value ranges from 0 to 100 (default value is 0).</td>
</tr>
<tr>
<td>Enabled</td>
<td>Mandatory</td>
<td>Check this box to turn on the DCC entry and uncheck this box to turn it off (this is disabled by default ). If any one of the configured DCC entry is enabled, an alarm is raised.</td>
</tr>
</tbody>
</table>

**Example**

To configure DCC entries to block 20 percent of the calls between the following two DN numbers:
- 234–235– 5678
- 237–351– 4567

You can configure the DCC entries for this as given below:
## Location management procedures

Use the procedures in this section to configure and manage the location of users.

**Navigation**

- [Modifying the default location of a domain](#) on page 149
- [Modifying the default location of a subdomain](#) on page 150
- [Adding a location](#) on page 150
- [Modifying a location](#) on page 151
- [Deleting a location](#) on page 152
- [Viewing and deleting deprecated locations](#) on page 152
- [Associating a user with a location](#) on page 153

### Modifying the default location of a domain

**About this task**

Use this procedure to modify the current default location for a domain.

The Domain Locations field specifies a default location that is used to process calls (should no other location information be available to guide the call).

You can modify the default location for a domain to be any of the locations defined in that domain's location hierarchy.

**Procedure**

1. From the Provisioning Client menu bar, select **System > Location** to access the Location Service portlet.
2. On the **Domain Data** tab, from the **Select domain** list, select the domain and click `>>`.
3. Select an alternate location from the **Location** list.
4. Click **Save**.
Modifying the default location of a domain job aid

About this task

Keep in mind that, when a location is deleted, the location is not immediately removed from the Database Manager. Instead, a timestamp of the current time plus two days is written to the Location Database Table DEPRECATED field. A process is run once every 24 hours to remove location and ERL database entries that have expired DEPRECATED field values. A job is added to the nightly database cleanup activities to remove deprecated locations, Emergency Response Locations (ERLs), and Automatic Number Identifiers (ANIs).

The DEPRECATED fields in the database tables contain timestamps of when the locations, ERLs and ANIs are no longer valid. If the value in the DEPRECATED field is before the current date/time, the location or ERL, is permanently deleted from the database table.

Modifying the default location of a subdomain

About this task

Use this procedure to modify the current default location for a subdomain.

When a new subdomain is created, the subdomain inherits the current location associated with the root domain by default. However, you can change this default location association to be any of the defined locations for the domain that appear in the Domain Locations list.

Procedure

1. From the Provisioning Client menu bar, select System > Location to access the Location Service portlet.
2. On the Domain Data tab, from the Select domain list, select the subdomain, and click >>.
3. Select a location from the Location list to modify the current default domain location.
4. Click Save.

Adding a location

About this task

Use this procedure to add a location.

Procedure

1. From the Provisioning Client menu bar, select System > Location to access the Location Service portlet.
2. On the Location tab, from the Select domain list, select the domain, and click >>.
3. Click Add Location to create a new location.
4. Configure the parameters on the Add Location tab.
5. Click Save.
Adding a location job aid

About this task
This job aid describes the parameters for the Add Location tab of the Location Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Name</td>
<td>This is the location name, a brief description of the location you are adding. This field cannot be null. Maximum length = 30 characters.</td>
</tr>
<tr>
<td>Location Description</td>
<td>This is the Master Street Address Guide (MSAG) address for the location you are creating. This field is required if you are defining the location as an ERL. If you are not defining the location as an ERL, you can leave this value blank or enter a longer description or address. Maximum length = 150 characters.</td>
</tr>
<tr>
<td>ASAC Location Profile</td>
<td>This is the list of configured ASAC Budget to Remote Locations in the EM console.</td>
</tr>
</tbody>
</table>

Note:
ASAC Location Profile must be applied only to top-level (root) locations. Top-level locations that have ASAC Location Profile assigned to them cannot have child locations.

Modifying a location

About this task
Use this procedure to modify a location.

Procedure
1. From the Provisioning Client menu bar, select System > Location to access the Location Service portlet.
2. On the Location tab, from the Select domain list, select the domain and click >>.
3. Select the link of the location you want to modify.
4. On the Modify Location tab, configure the parameters as required.
5. Click Save.

Modifying a location job aid

About this task
This job aid describes the parameters for the Modify Location tab in the Location Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Name</td>
<td>This is the location name, a brief description of the location you are adding. This field cannot be null. Maximum length = 30 characters.</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location Description</td>
<td>This is the Master Street Address Guide (MSAG) address for the location you are creating. This field is required if you are defining the location as an ERL. If you are not defining the location as an ERL, you can leave this value blank or enter a longer description or address. Maximum length = 150 characters.</td>
</tr>
</tbody>
</table>
| ASAC Location Profile    | This is the list of configured ASAC Budget to Remote Locations in the EM console.  

**Note:**  
ASAC Location Profile must be applied only to top-level (root) locations. Top-level locations that have ASAC Location Profile assigned to them cannot have child locations. |

---

**Deleting a location**

**About this task**

Use this procedure to delete a location.

**Procedure**

1. From the Provisioning Client menu bar, select **System > Location** to access the Location Service portlet.
2. On the **Location** tab, from the **Select domain** list, select the domain and click `>>`.
3. Click the trashcan icon to the right of the domain or subdomain location that you want to delete.
4. In the confirmation dialog, type your administrator password.
5. Click **Confirm**.

---

**Viewing and deleting deprecated locations**

**About this task**

Use this procedure to view deprecated locations.

When a location is deleted, the location is not immediately removed from the Database Manager. Instead, a timestamp of the current time plus two days is written to the DEPRECATED field in the Location database table. A process is run once every 24 hours to remove the location and ERL database entries that have expired DEPRECATED field values.

**Procedure**

1. From the Provisioning Client menu bar, select **System > Location** to access the Location Service portlet.
2. On the **Location** tab, from the **Select domain** list, select the domain and click `>>`.

3. Click **List Deprecated Locations**.

4. Click **Delete**.

5. In the confirmation dialog, type your administrator password.

6. Click **Confirm** to delete the deprecated locations.

---

**Associating a user with a location**

**About this task**

Use this procedure to associate a user with a location.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Routing > User Routing** to access the User Routing Service portlet.

2. On the **Charge ID** tab, in the **Select User** box, type a user name in the user@domain format.

3. Click `>>`.

4. In the **Public Charge ID** box, type a dialable directory number (DN).

5. **(Optional)** In the **Private Charge ID** box, type a dialable public or private directory number (DN).

6. Click **Save**.

---

**Associating a user with a location job aid**

The following table describes the parameters that you configure to associate a user with a location.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Charge ID</td>
<td>A directory number (DN)—a 10-digit national dial plan number, to associate with the user. The E911 operator uses this number as the callback number should the operator ever have to reestablish the call. The Public Charge ID only applies to residential E911 and therefore is not a required field for Enterprise E911. The public charge ID typically consists of a public or private directory number. Your charge ID may contain other numbers that are not directory numbers. They can be account numbers, your lucky number, any number the administrator wants to put in there to identify the user for accounting purposes.</td>
</tr>
<tr>
<td>Private Charge ID</td>
<td>A dialable public or private directory number (DN)—a 10-digit national dial plan number, to associate with the user. The charge ID can consist of other numbers, such as account numbers to identify the user for accounting purposes.</td>
</tr>
</tbody>
</table>
Border Control Point 7000 Series provisioning procedures

About this task
Avaya Aura® Application Server 5300 does not support the Border Control Point 7000 Series.

Miscellaneous Groups service configuration

About this task
Application Server 5300 does not support the Miscellaneous Groups service.

Provider Managed Clients service configuration

About this task
Application Server 5300 does not support Provider Managed Clients (PMC) service.

Ring Tone service configuration

About this task
Use the procedures in this section to configure the Ring Tone service.

- Creating ring tones on page 154
- Listing, modifying, or deleting ring tones on page 155
- Configuring ring tone profiles on page 156
- Listing, modifying, and deleting ring tone profiles on page 156
- Assigning ring tone profiles to a domain on page 157

Creating ring tones

About this task
Use this procedure to create ring tones

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > Ringtone to access the Ring Tone Service portlet.
2. On the **Create Ring Tone** tab, configure the parameters as required.
3. Click **Save**.

### Creating ring tones job aid

**About this task**

This job aid describes the parameters for the **Create Ring Tone** tab in the Ring Tone Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the ring tone you want to create.</td>
</tr>
<tr>
<td>Ring tone URL</td>
<td>Type an IP address of the ring tone location.</td>
</tr>
</tbody>
</table>

### Listing, modifying, or deleting ring tones

**About this task**

Use this procedure to list, modify, or delete ring tones.

**Procedure**

1. From the Provisioning Client menu bar, select **Service > Call Termination > Ringtone** to access the Ring Tone Service portlet.
2. To modify a ring tone profile, select the ring tone link in the **Name** table column.
3. On the **Modify Ring Tone** tab, modify the parameters.
4. Click **Save**.
5. To delete a ring tone profile, click **Delete** for ring tone profile.

An upgrade installation creates a default ring tone profile with Avaya standard ring tones.

### Modifying ring tone job aid

**About this task**

This job aid describes the parameters for the **Modify Ring Tone** tab in the Ring Tone Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the ring tone profile.</td>
</tr>
<tr>
<td>Ring tone URL</td>
<td>Type an IP address of the ring tone location.</td>
</tr>
</tbody>
</table>
Configuring ring tone profiles

About this task
Use this procedure to configure ring tone profiles. You can associate a profile with a specific set of ring tones.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Ringtone to access the Ring Tone Service portlet.
2. In the Ring Tone Service portlet, select the System Profile tab.
3. In the Profile Name box, type the name of the profile.
4. From the Available Ring Tones list, select the ring tone.
5. Click Copy.
6. Click Save.

Configuring ring tone profiles job aid

About this task
This job aid describes the buttons that appear on the System Profile tab in the Ring Tone Service portlet.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Click Copy to copy a specific ring tone from the Available Ring Tones box.</td>
</tr>
<tr>
<td>Copy all</td>
<td>Click Copy All to copy all ring tones from the Available Ring Tones box.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click Remove to remove a specific ring tone from the Selected Ring Tones box.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Click Remove All to remove all ring tones from the Selected Ring Tones box.</td>
</tr>
<tr>
<td>Save</td>
<td>Click Save to save the ring tone or ring tones you selected for a profile.</td>
</tr>
</tbody>
</table>

Listing, modifying, and deleting ring tone profiles

About this task
Use this procedure to list, modify, and delete ring tone profiles.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Ringtone to access the Ring Tone Service portlet.
2. In the Ring Tone Service portlet, select the System Profile tab.
3. To modify a ring tone profile, select the ring tone link in the **Profile Name** table column.

4. From the **Available Ring Tones** list, select one or more ring tone profiles.

5. Click **Copy** to place the ring tone profiles in the **Selected Ring Tones** list.

6. To remove ring tone profiles, select one or more ring tone profiles from the **Selected Ring Tones** list, and click **Remove**.

7. Click **Save**.

8. To delete a ring tone profile, click **Delete** for the ring tone profile.

An upgrade installation creates a default ring tone profile with Avaya standard ring tones.

---

**Assigning ring tone profiles to a domain**

**About this task**

Use this procedure to assign ring tone profiles to a domain.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Termination > Ringtone** to access the Ring Tone Service portlet.

2. In the Ring Tone Service portlet, select the **System Profile** tab.

3. To assign or remove ring tone profiles from a domain, click **Assign/Remove** from the **Domain** table column.

4. Select one or more domains from the **Available Domains** list.

5. Click **Copy** to place the domains in the **Selected Domains** list.

6. To remove domains, select one or more domains from the **Selected Domains** list, and click **Remove**.

7. Click **Save**.

**Assigning profiles to a domain job aid**

This job aid describes the buttons that appear on the **System Profile** tab in the Ring Tone Service portlet.

<table>
<thead>
<tr>
<th>Button</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Copy</td>
<td>Click <strong>Copy</strong> to copy a specific profile from the <strong>Available Domains</strong> box.</td>
</tr>
<tr>
<td>Copy all</td>
<td>Click <strong>Copy all</strong> to copy all profiles from the <strong>Available Domains</strong> box.</td>
</tr>
<tr>
<td>Remove</td>
<td>Click <strong>Remove</strong> to remove a specific profile from the <strong>Selected Domains</strong> box.</td>
</tr>
<tr>
<td>Remove All</td>
<td>Click <strong>Remove All</strong> to remove all profiles from the <strong>Available Domains</strong> box.</td>
</tr>
</tbody>
</table>
Security service configuration

About this task

Use the procedures in this section to configure the Security service.

- Configuring the Media Security Profile for a domain on page 158
- Configuring Signaling Security for a domain on page 159

Configuring the Media Security Profile for a domain

Use this procedure to configure the Media Security Profile that the AS 5300 Session Manager uses to enforce a particular level of media security for a domain.

⚠ Important:

Systems that do not use TLS and SRTP use UDP and RTP. The Audiocodes Mediant 3000 does not support best effort RTP/SRTP (mixed-mode). The configuration for all endpoints must be either secure or nonsecure for media.

Before you begin

- You have Domain Security Management privileges.

Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Security to access the Security Service portlet.
2. On the Media Security tab, select a domain where you want to provision media security in the Select domain list.
3. Select a profile from the Media Security Profile list.
   - Best Effort—supports both RTP and SRTP media in the domain
   - Security Enforced—supports only SRTP media in the domain
   - Security Disabled—supports only RTP media in the domain
4. (Optional) Click Reset to Defaults to repopulate the window with Best Effort Media Security configuration values.
5. Click Save to save the Media Security configuration parameters. A message appears indicating that the Media Security configuration is saved successfully.

Variable Definitions

<table>
<thead>
<tr>
<th>Variable</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;Domain_name&gt;</td>
<td>This value is the name of the domain for which you want to configure security.</td>
</tr>
</tbody>
</table>
Configuring the Media Security Profile for a domain job aid

About this task

The AS 5300 Session Manager enforces the Media Security Profile for all offers and answers, for the domain.

This job aid lists the media security profiles and describes how the AS 5300 Session Manager handles requests for each profile.

<table>
<thead>
<tr>
<th>Media Security Profile</th>
<th>Request with secure media in SDP (RTP/SAVP)</th>
<th>Request with unsecure media in SDP (RTP/AVP)</th>
<th>Request with both secure and unsecure media in SDP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Security Enforced</td>
<td>Continue</td>
<td>Reject with 415</td>
<td>Configure the port to 0 for the unsecure SDP and continue</td>
</tr>
<tr>
<td>Best Effort</td>
<td>Continue</td>
<td>Continue</td>
<td>Continue</td>
</tr>
<tr>
<td>Security Disabled</td>
<td>Reject with 415</td>
<td>Continue</td>
<td>Configure the port to 0 for the secure SDP and continue</td>
</tr>
</tbody>
</table>

Configuring Signaling Security for a domain

About this task

Use this procedure to provision Signaling security data for the domain. Signaling security enforces the type of signaling that is allowed in a domain.

Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Security to access the Security Service portlet.
2. In the Security Service portlet, select the Signaling Security tab.
3. In the Select domain field, select a domain where you want to provision media security, and click >>.
4. In the Signaling Security Profile field, select a profile.
   - Best Effort—signaling in the domain can be of type TLS, TCP, or UDP, with preference for TLS
   - Security Enforced—only TLS signaling will be allowed in the domain
5. To enable the SIP TLS Identity Checking feature, select the SIP-TLS Identity Check option.
6. Click Restore to Default to repopulate the window with Best Effort Signaling Security configuration values.
7. Click Save to save the Signaling Security configuration parameters.
Status Reasons service configuration

About this task
Use the procedures in this section to configure the Status Reasons service.

- Configuring domain status reasons on page 160
- Viewing a status reason on page 161
- Deleting a status reason on page 161

Configuring domain status reasons

About this task
When a user is inactive, the user cannot register to the AS 5300 Session Manager. Therefore, the user cannot use any of the services provided by the AS 5300 Session Manager, including making calls. You can define a reason for an inactive user’s status and assign it to individual users.

Procedure

1. From the Provisioning Client menu bar, select System > Status Reason to access the Status Reasons Service portlet.
2. On the StatusReason tab, from the Select domain list, select the domain and click >>.
3. On the StatusReason tab, configure the parameters as required.
4. Click Save.

Adding a status reason job aid

About this task
This job aid describes the parameters for the StatusReason tab in the Status Reasons Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Options include ACTIVE and INACTIVE.</td>
</tr>
<tr>
<td>Name</td>
<td>Type a name to identify the status reason.</td>
</tr>
<tr>
<td>Description</td>
<td>Type a description for the inactive status. For example, if the user is on vacation, the reason can be: On vacation for two weeks</td>
</tr>
<tr>
<td>URL</td>
<td>Type a Web page address. The Web page displays the status reason description to explain the called user’s inactive status.</td>
</tr>
</tbody>
</table>
Viewing a status reason

About this task
Use this procedure to view the reasons for an inactive user status.

When a user is inactive, the user cannot register to the AS 5300 Session Manager. This means that the user cannot use any of the services provided by the AS 5300 Session Manager, including making calls or subscribing to other users’ presence.

Procedure
1. From the Provisioning Client menu bar, select **System > Status Reason** to access the Status Reasons Service portlet.
2. On the **StatusReason** tab, from the **Select domain** list, select the domain and click `>>`.
3. To view or modify status reason information, click the link of the status you want to view or modify in the **Name** table column.
4. Configure the status reasons parameters.
5. Click **Save**.

Deleting a status reason

About this task
Use this procedure to delete a status reason no longer in use.

Procedure
1. From the Provisioning Client menu bar, select **System, Status Reason** to access the Status Reasons Service portlet.
2. On the **StatusReason** tab, from the **Select domain** list, select the domain, and click `>>`.
3. To delete a status reason, click **Delete** for the status you want to delete.
4. In confirmation dialog, type your administrator’ password and click **Continue**.

Configuring TR87 Client Control

TR87 Client Control allows a soft client to monitor and control the actions of a hard client. Use the procedures in this section to configure TR87 Client Control.

- **Assigning resources for TR87 Client Control** on page 162
- **Assigning TR87 Client Control to a Domain** on page 164
- **Setting up the TR87 Client Control profile** on page 162
Assigning resources for TR87 Client Control

Use this procedure to assign domain resources for TR87 Client Control.

**Before you begin**

- You must have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Resources to access the Resource Management portlet.
2. On the Domain Resources tab, select a domain in the Select domain pull-down and click >>
3. On the Domain Resources tab, scroll down to the TR87 Client Control row and assign the required number of units in the Assign column.
4. Click Save.

Assigning the TR87 Client Control profile to a Domain

Use this procedure to assign the TR87 Client Control profile to a Domain.

**Before you begin**

- You must have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Service Profiles to access the User Services portlet.
2. On the Services tab, scroll down to TR87 Client Control and then click on that service.
3. In the System Profile tab of the TR87 Client Control Service portlet select the row containing the profile you want to assign and click on Assign/Remove under the Domain column.
4. In the System Profile tab, click on a domain in the Available Domains column to which you want to assign the profile and click Copy.
5. Click Save.

Setting up the TR87 Client Control profile

Use this procedure to set up the TR87 Client Control profile.
Before you begin

• You must have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select **Domain > Domain Steps > Assign Service Profiles** to access the User Services portlet.
2. On the **Services** tab, scroll down to TR87 Client Control and then click on that service.
3. On the **System Profile** tab of the TR87 Client Control Service portlet, enter information for the profile.
4. Click **Save**.

Setting up the TR87 Client Control profile job aid

This job aid describes the data for the **System Profile** tab of the TR87 Client Control Service portlet.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The profile name you wish to use.</td>
</tr>
<tr>
<td>SIP Terminal</td>
<td>Indicates the client type.</td>
</tr>
<tr>
<td>Maximum CSTA Call</td>
<td>Controls the number of Computer Supported Telecommunications Applications (CSTA) calls based on subscriber.</td>
</tr>
<tr>
<td>Session Refresh Timer Enabled</td>
<td>Indicates whether the CSTA session is refreshed.</td>
</tr>
<tr>
<td>Session Refresh Timer</td>
<td>Indicates the session refresh time interval, in hours.</td>
</tr>
<tr>
<td>MakeCall</td>
<td>Indicates the signaling method used for a MakeCall request. The values available are 'Standard', 'Refer' and 'Refer URN'.</td>
</tr>
<tr>
<td>AnswerCall</td>
<td>Indicates the signaling method used for an AnswerCall request. The values available are 'Standard', 'Refer' and 'Refer URN'.</td>
</tr>
<tr>
<td>HoldCall</td>
<td>Indicates the signaling method used for a HoldCall request. The values available are 'Standard', 'Refer' and 'Refer URN'.</td>
</tr>
<tr>
<td>RetrieveCall</td>
<td>Indicates the signaling method used for a RetrieveCall request. The values available are 'Standard', 'Refer' and 'Refer URN'.</td>
</tr>
<tr>
<td>ClearConnection</td>
<td>Indicates the signaling method used for a ClearConnection request. The values available are 'Standard', 'Refer' and 'Refer URN'.</td>
</tr>
<tr>
<td>ConsultationCall</td>
<td>Indicates the signaling method used for a ConsultationCall request. The values available are 'Standard', 'Refer' and 'Refer URN'.</td>
</tr>
</tbody>
</table>
Assigning TR87 Client Control to a Domain

Use this procedure to assign the TR87 Client Control to a Domain.

Before you begin

• You must have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select **Domain > Domain Steps > Assign Services** to access the User Services portlet.

2. On the **Service Assignment** tab, select a domain in the **Select domain** pull-down and click **>>**

3. On the **Service Assignment** tab, scroll down the list of Service names and click the check-box next to TR87 Client Control.

4. Click **Save**.

Assigning TR87 Client Control to users

Use this procedure to assign TR87 Client Control to users.

Before you begin

• You must have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select **User > Search** to access the User portlet.

2. On the **Advanced Search** tab, enter the appropriate search information about the user to whom you want to assign this feature, and then click **Search**.

3. On the **Advanced Search** tab, click the name of the user in the Username column of the table.

4. Click the **Services** tab of the User portlet.

5. On the **Services** tab, scroll down the table and click the check-box next to TR87 Client Control.

6. Click **Save**.

7. On the **Services** tab, scroll down the table and click on **TR87 Client Control**.

8. Click the **User Data** tab of the TR87 Client Control Service window.

9. On the **User Data** tab, enter information for the user you want to assign this feature and then click **>>**.

10. Select the profile you want to assign from the User’s system profile list and then click **Save**.
Treatments service configuration

About this task

Use the procedures in this section to configure treatments for services.

- Assigning a pool to a domain or subdomain on page 165
- Treatment Media Management on page 167
- Adding announcement files to the servicing pool on page 169
- Configuring treatments for service on page 170

Assigning a pool to a domain or subdomain

About this task

Assign a pool to serve a domain or subdomain. You must also create a new treatment group for each MLPP announcement.

Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Treatment to access the Treatment Service portlet.
2. In the Treatment Service portlet, select the Assign Pool tab.
3. In the Select domain field of the Treatment Service portlet, select a domain to which you want to assign a pool and click >>.
4. In the Select pool field of the Treatment Service portlet, select a pool to assign and click Save.
5. In the Treatment Service portlet, select the Treatment/Cause Group tab.
6. In the Select pool field of the Treatment Service portlet, click >>.
7. In the Group Name field of the Treatment Services portlet, type a unique name for the group. The name must be unique within the subdomain, although a parent domain can have an identical group name. Examples of group names are: MlppUpaGroup and MlppBpaGroup.
8. From the Available Reasons list, select a reason.
9. From the Available Files list, select a file.
10. Click Copy.
11. Click up and down to change the order of the files that appear in the Selected Files list.
    The files play in the order in which they appear in the list.
12. From the Select repeat: (times played) list, select the number of times to play the announcement.
13. In the Route box, type a destination to which to forward the call after the announcement plays.
14. Click **Save**.

15. Repeat **7** on page 165 to **14** on page 166 to create each treatment group.

**Assigning a pool to a domain or subdomain job aid**

This job aid lists sample MLPP announcements and the audio files that play, in order, for each announcement.

<table>
<thead>
<tr>
<th>Announcement</th>
<th>Selected files</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Blocked Precedence Announcement (BPA)</strong></td>
<td>1. File to play switch name.</td>
</tr>
<tr>
<td></td>
<td>2. File—location name.</td>
</tr>
<tr>
<td></td>
<td>3. File—“Equal or higher precedence calls have prevented completion of your call. Please hang up and try again. This is a recording.”</td>
</tr>
<tr>
<td></td>
<td>4. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>5. File—location name.</td>
</tr>
<tr>
<td><strong>Unauthorized Precedence Level Announcement (UPA)</strong></td>
<td>1. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>2. File—location name.</td>
</tr>
<tr>
<td></td>
<td>3. File—“The precedence used is not authorized for your line. Please use an authorized precedence or ask your attendant for assistance. This is a recording.”</td>
</tr>
<tr>
<td></td>
<td>4. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>5. File—location name.</td>
</tr>
<tr>
<td><strong>Vacant Code Announcement (VCA)</strong></td>
<td>1. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>2. File—location name.</td>
</tr>
<tr>
<td></td>
<td>3. File—“Your call cannot be completed as dialed. Please consult your directory and call again or ask your operator for assistance. This is a recording.”</td>
</tr>
<tr>
<td></td>
<td>4. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>5. File—location name.</td>
</tr>
<tr>
<td><strong>Isolated Code Announcement (ICA)</strong></td>
<td>1. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>2. File—location name.</td>
</tr>
<tr>
<td></td>
<td>3. File—“A service disruption has prevented the completion of your call. Please wait 30 minutes and try again. In case of emergency call your operator. This is a recording.”</td>
</tr>
<tr>
<td></td>
<td>4. File—switch name.</td>
</tr>
<tr>
<td></td>
<td>5. File—location name.</td>
</tr>
</tbody>
</table>
Treatment Media Management

About this task
Use the procedures in this section to manage treatment media.

- Assigning Treatment media groups on page 167
- Adding Treatment media files on page 167
- Deleting Treatment media files on page 168
- Downloading Treatment media files on page 169

Assigning Treatment media groups

About this task
Use this procedure to assign media groups for service treatments.

Procedure
1. From the Provisioning Client menu bar, select Services > Announcements > Treatment to access the Treatment Service portlet.
2. In the Treatment Service portlet, in the Select domain field, select a domain in which to add a treatment and click >>.
3. In the Select domain list, select a domain to which you want to add Call Screening treatment and click >>.
4. In the Select pool list, select a pool and click Save.
5. In the Select pool list, select a pool and click Configure.
6. In the Group name list, select a Group.
7. Click Save.

Assigning Treatment media groups job aid

About this task
The following job aid describes the parameters for assigning treatments in the Treatment Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain in which to assign a group.</td>
</tr>
<tr>
<td>Select pool</td>
<td>From the list, select a pool in which to assign a group.</td>
</tr>
<tr>
<td>Group name</td>
<td>From the list, select the name of the group to assign.</td>
</tr>
</tbody>
</table>

Adding Treatment media files

About this task
Use this procedure to add media files.
Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Treatment to access the Treatment Service portlet.

2. In the Treatment Service portlet, in the Select domain field, select a domain to which you want to add media, and click >>.

3. In the Select pool list, select a pool, and click >>.

4. Click Browse and select the file to add.

5. In the Name field, type the name for the new media file.

6. In the Locale list, select the locale for the new media file.

7. Click Save.

8. Repeat steps 4 to 7 for each media file.

Adding Treatment media files job aid

About this task

The following job aid describes the parameters for adding media files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain in which to add a file.</td>
</tr>
<tr>
<td>Select pool</td>
<td>From the list, select a pool in which to add a file.</td>
</tr>
<tr>
<td>Name</td>
<td>Type a descriptive name for the new media file.</td>
</tr>
<tr>
<td>Locale</td>
<td>From the list, select a Locale in which to add the file.</td>
</tr>
</tbody>
</table>

Deleting Treatment media files

About this task

Use this procedure to delete media files.

Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Treatment to access the Treatment Service portlet.

2. In the Treatment Service portlet, in the Select domain field, select a domain, and click >>.

3. In the Select pool list, select a pool and click >>.

4. To delete one file, click Delete next to the file name, OR To delete all files, click Remove All.

5. Type your password, and click Confirm.

Deleting Treatment media files job aid

About this task

The following job aid describes the parameters for deleting media files.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain from which to delete a file.</td>
</tr>
<tr>
<td>Select pool</td>
<td>From the list, select a pool from which to delete a file.</td>
</tr>
</tbody>
</table>

### Downloading Treatment media files

#### About this task
Use this procedure to download and save media files on your local PC.

#### Procedure

1. From the Provisioning Client menu bar, select **Services > Announcements > Treatment** to access the Treatment Service portlet.
2. In the Treatment Service portlet, in the **Select domain** list, select a domain and click `>`.
3. In the **Select pool** list, select a pool and click `>`.
4. Next to a media file, click **Download**.
5. Select **OK** to save the file on your local PC, **OR** select an application with which to open the file and click **OK**.

### Downloading Treatment media files job aid

#### About this task

The following job aid describes the parameters for downloading media files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain from which to download the file.</td>
</tr>
<tr>
<td>Select pool</td>
<td>From the list, select a pool from which to download the file.</td>
</tr>
</tbody>
</table>

### Adding announcement files to the servicing pool

#### About this task

You must add the names of audio files to the servicing pool. The names must match those on the Avaya Media Server.

#### Procedure

1. From the Provisioning Client menu bar, select **Services > Announcements > Treatment** to access the Treatment Service portlet.
2. In the Treatment Service portlet, click the **Treatment/Cause File** tab.
3. In the **Select domain** field of the Treatment Service portlet, select a domain and click `>`.
4. In the **Select pool** field of the Treatment Service portlet, type the name of an audio file.
5. Click **Save**.
6. Repeat Steps 4 and 5 for each audio file.
Configuring treatments for service

About this task
Use this procedure to configure treatment for any service in the domain where service is needed.

Procedure
1. From the Provisioning Client menu bar, select Services > Announcements > Treatment to access the Treatment Service portlet.
2. In the Treatment Service portlet, select the Treatment/Cause Group tab.
3. In the Select domain field, select a domain to which you want to add service treatment, and click >>.
4. In the Select pool field, select a pool, and click >>.
5. In the Available reasons list, click an appropriate service reason or treatment name, and click Copy.
6. In the Available files list, click the corresponding sound file or Treatment cause, and click Copy.
7. Repeat step 5 and 6 for each service treatment name and associated treatment cause to be provisioned.
8. Click Save.

Configuring treatments for service common job aid

About this task
The following job aid describes the parameters for the Treatment/Cause Group tab in the Treatment Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group Name</td>
<td>Type a name for the group in the Group Name field.</td>
</tr>
<tr>
<td>Available Reasons</td>
<td>Select the appropriate reasons from the Available Reasons box.</td>
</tr>
<tr>
<td>Selected Reasons</td>
<td>The Selected Reasons box shows all the reasons you selected and added from the Available Reasons box.</td>
</tr>
<tr>
<td>Available Files</td>
<td>Select the appropriate files from the Available Files box.</td>
</tr>
<tr>
<td>Selected Files</td>
<td>The Selected Files box shows all the files you selected and added from the Available Files box.</td>
</tr>
<tr>
<td>Select Repeat: (Times Played)</td>
<td>Select the number of times to play a file from the list in the Select Repeat: (Times Played) field.</td>
</tr>
<tr>
<td>Route</td>
<td>Type the destination to reroute the call after the announcement has been played.</td>
</tr>
</tbody>
</table>

Table continues…
Available reasons for Call Screening service

The following list shows the available reasons you use to configure treatments for Call Screening service:

- 1050 Forbidden – All Incoming Calls Not Allowed
- 1051 Forbidden – All Outgoing Calls Not Allowed
- 1052 Forbidden – Local Calls Not Allowed
- 1053 Forbidden – Long Distance Calls Not Allowed
- 1054 Forbidden – International Calls Not Allowed
- 1055 Forbidden – Premium Calls Not Allowed
- 1056 Forbidden – Selective Reject Incoming
- 1057 Forbidden – Selective Reject Outgoing

Treatment names and causes for DCC

Use the following table to select the Treatment names and causes when assigning DCC Treatment Files to a domain.

**Table 15: DCC Treatment names and causes**

<table>
<thead>
<tr>
<th>Treatment name</th>
<th>Treatment cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>REJECTED_BY_DCC</td>
<td>1203</td>
</tr>
</tbody>
</table>

Treatment name and causes for the MCT service

Use the following table to select MCT Treatment names and causes when assigning MCT Treatment Files to a domain.

<table>
<thead>
<tr>
<th>Treatment name</th>
<th>Treatment cause</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCT_SUCCESS</td>
<td>498</td>
</tr>
<tr>
<td>MCT_FAILURE</td>
<td>499</td>
</tr>
</tbody>
</table>

Treatment names and causes for VSC

Use the following table to select the Treatment names and causes when assigning VSC Treatment Files to a domain.
Table 16: VSC Treatments

<table>
<thead>
<tr>
<th>Treatment Name / reason</th>
<th>Treatment cause</th>
<th>Indicates that</th>
<th>Used by VSCs associated with these features</th>
</tr>
</thead>
<tbody>
<tr>
<td>MCT_SUCCESS</td>
<td>498</td>
<td>Malicious Call Trace succeeded.</td>
<td>Malicious Call Trace</td>
</tr>
<tr>
<td>MCT_FAILURE</td>
<td>499</td>
<td>Malicious Call Trace failed.</td>
<td>Malicious Call Trace</td>
</tr>
<tr>
<td>STARCODE_STATUS_ENABLED</td>
<td>1003</td>
<td>The VSC is enabled.</td>
<td>Used by most VSCs</td>
</tr>
<tr>
<td>STARCODE_STATUS_DISABLED</td>
<td>1004</td>
<td>The VSC is disabled.</td>
<td>Used by most VSCs</td>
</tr>
<tr>
<td>STARCODE_SUCCESS</td>
<td>1001</td>
<td>VSC execution succeeded.</td>
<td>Used by most VSCs</td>
</tr>
<tr>
<td>STARCODE_CLIP_PER_CALL_SUCCESS</td>
<td>1005</td>
<td>Calling Line ID Restriction Enable Per Call activated successfully.</td>
<td>Calling Line ID</td>
</tr>
<tr>
<td>STARCODE_CLIP_PER_CALL_SUCCESS</td>
<td>1006</td>
<td>Calling Line ID Presentation Per Call activated successfully.</td>
<td>Calling Line ID</td>
</tr>
<tr>
<td>STARCODE_NCWD_PER_CALL_SUCCESS</td>
<td>1007</td>
<td>Network Call Waiting Disable Per Call activated successfully.</td>
<td>Network_Call_Waiting_Disable_per_Call</td>
</tr>
<tr>
<td>STARCODE_CLI_SUCCESS</td>
<td>1008</td>
<td>Calling Line Identifier (CLI) Notification VSC has successfully identified the most recent caller.</td>
<td>Call Return</td>
</tr>
<tr>
<td>STARCODE_CLI_FAILURE</td>
<td>1009</td>
<td>Calling Line Identifier (CLI) Notification VSC failed because the most recent caller is anonymous or there is no information about the most recent caller.</td>
<td>Call Return</td>
</tr>
<tr>
<td>ALL_INCOMING_CALLS_NOT_ALLOWED</td>
<td>1050</td>
<td>Called party has Call Screening feature activated and forbids all incoming calls.</td>
<td>Deny All Calls via VSC</td>
</tr>
<tr>
<td>ALL_OUTGOING_CALLS_NOT_ALLOWED</td>
<td>1051</td>
<td>Calling party has Call Screening feature activated and forbids all outgoing calls.</td>
<td>Deny All Calls via VSC</td>
</tr>
<tr>
<td>LOCAL_CALLS_NOT_ALLOWED</td>
<td>1052</td>
<td>Calling party has Call Screening feature activated and forbids local calls.</td>
<td>Deny All Calls via VSC</td>
</tr>
<tr>
<td>LONG_DISTANCE_CALLS_NOT_ALLOWED</td>
<td>1053</td>
<td>Calling party has Call Screening feature activated and forbids long distance calls.</td>
<td>Deny All Calls via VSC</td>
</tr>
<tr>
<td>INTERNATIONAL_CALLS_NOT_ALLOWED</td>
<td>1054</td>
<td>Calling party has Call Screening feature activated and forbids international calls.</td>
<td>Deny All Calls via VSC</td>
</tr>
<tr>
<td>Treatment Name / reason</td>
<td>Treatment cause</td>
<td>Indicates that</td>
<td>Used by VSCs associated with these features</td>
</tr>
<tr>
<td>-------------------------</td>
<td>----------------</td>
<td>----------------</td>
<td>--------------------------------------------</td>
</tr>
<tr>
<td>PREMIUM_CALLS_NOT_ALLOWED</td>
<td>1055</td>
<td>Calling party has Call Screening feature activated and forbids premium calls.</td>
<td>Deny All Calls via VSC</td>
</tr>
<tr>
<td>SELECTIVE_REJECT_INCOMING</td>
<td>1056</td>
<td>The calling party is banned.</td>
<td>Selective Call Reject</td>
</tr>
<tr>
<td>SELECTIVE_REJECT_OUTGOING</td>
<td>1057</td>
<td>The called party is banned</td>
<td>Selective Call Reject</td>
</tr>
<tr>
<td>QUEUE_CLOSURE</td>
<td>1082</td>
<td>The UCD Group is closed, or the system cannot provide queuing service.</td>
<td>Uniform Call Distribution</td>
</tr>
<tr>
<td>QUEUE_MAXIMUM_SIZE</td>
<td>1081</td>
<td>The maximum queue size of the UCD is exceeded.</td>
<td>Uniform Call Distribution</td>
</tr>
<tr>
<td>QUEUE_TIMEOUT</td>
<td>1080</td>
<td>A caller has been in the queue longer than the Maximum wait time, and the call is terminating.</td>
<td>Uniform Call Distribution</td>
</tr>
<tr>
<td>UCD_RINGBACK</td>
<td>1083</td>
<td>A caller is waiting in the queue. This treatment plays continuously while a caller waits in the queue (often a looping musical clip). If no treatment is provisioned, no sound plays.</td>
<td>Uniform Call Distribution</td>
</tr>
<tr>
<td>UCD_DELAY_ANNOUNCEMENT</td>
<td>1084</td>
<td>A caller is waiting in the queue. This treatment plays periodically while the caller waits in the queue (for example “Your call is important to us, please continue to hold”). If no treatment is provisioned, no sound plays.</td>
<td>Uniform Call Distribution</td>
</tr>
<tr>
<td>CALL_PICKUP_FORBIDDEN</td>
<td>1090</td>
<td>Call Pickup is not permitted for the incoming call.</td>
<td>Call Pickup</td>
</tr>
<tr>
<td>NO_CALL_AVAILABLE_FOR_PICKUP</td>
<td>1091</td>
<td>No call available for pickup.</td>
<td>Call Pickup</td>
</tr>
</tbody>
</table>

### User Routing service configuration

**About this task**

Use the procedures in this section to configure the User Routing service.

- [Adding a static route](#) on page 174
- [Assigning the Charge ID to a user](#) on page 174
Adding a static route

About this task
Use this procedure to add a static route.

If a user is in the system, you can provision a route for the user as a static route. When a call comes in, the system forwards the call to the user's registered and static routes.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Routing > User Routing to access the User Routing Service portlet.
2. On the Static Routes tab, type a user name in the Select user box and click >>.
3. In the Route Name box, type a name to identify the route.
4. Click Save.

Assigning the Charge ID to a user

Use this procedure to assign the Charge ID to a user.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Routing > User Routing to access the User Routing Service portlet.
2. On the Charge ID tab, configure the parameters as required.
3. Click Save.

Assigning the Charge ID to a user job aid
This job aid describes the parameters for the Charge ID tab in the User Routing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private Charge ID</td>
<td>The Private Charge ID of the user. The private charge ID, typically consists of a public or private directory number. Your charge ID may contain other numbers that are not directory numbers. They can be account numbers, your lucky number, any number the administrator wants to put in there to identify the user for accounting purposes. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
</tbody>
</table>

Table continues...
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public Charge ID</td>
<td>The 10-digit national dial plan number associated with the subscriber. This is required for the interworking with Public Switched Telephone Network (PSTN) switches in the Time Division Multiplex (TDM) network. The public charge ID typically consists of a public or private directory number. Your charge ID may contain other numbers that are not directory numbers. They can be account numbers, your lucky number, any number the administrator wants to put in there to identify the user for accounting purposes. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
</tbody>
</table>

### Vertical Service Code configuration

#### About this task

This work flow shows the sequence of tasks that you perform to configure and enable Vertical Service Codes (VSC).

- **Assigning services to a domain** on page 192 – Use this procedure to assign the Vertical Service Codes service to one or more domains.
• **Assigning services to a user** on page 303 – Use this procedure to assign the Vertical Service Codes service to one or more subscribers.

• **Provisioning Vertical Service Codes** on page 176

• **Creating a VSC PIN for a subscriber** on page 177

---

## Provisioning Vertical Service Codes

Use this procedure to provision Vertical Service Codes (VSC).

### Procedure

1. From the Provisioning Client menu bar, select **Services > Call Routing > Vertical Service Codes** to access the Vertical Service Codes Service portlet.

2. On the **Feature Translation** tab, select the domain from the list and click `>>`.

3. On the **Feature Translation** tab, configure the parameters as required.

4. Click **Save**.

---

### Provisioning Vertical Service Codes job aid

This job aid describes the parameters for the **Feature Translation** tab in the Vertical Service Codes Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a meaningful name that describes the translation record. The name must be unique in a domain and contain 1 to 32 characters.</td>
</tr>
</tbody>
</table>
| Prefix        | Specify the string that subscribers enter to use the VSC Service. The string must be 2 to 32 in length, and can begin with *, # or any digit, followed by one or more digits. For example, *123. **Note:**  
  - Do not define VSC prefixes that are a substring of other VSC prefixes. For example, if you define *123 for one VSC Service, you cannot define another as *12; if you do so, only *123 functions..  
  - VSC prefixes that you configure at the domain level override any VSC prefix configured at the subdomain level. For example, if you configure VSC Service x to use *123 on a domain, and configure VSC Service y to use *123 on a subdomain within that domain, the domain configuration overrides the subdomain configuration, and *123 triggers VSC Service x. |
| VSC Service   | Select the service from the list. This is the VSC-controlled function to enable, disable, and check the status of the service. |
Creating a VSC PIN for a subscriber

Use this procedure to create a VSC PIN for a subscriber.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Routing > Vertical Service Codes** to access the Vertical Service Codes Service portlet.
2. Click the **PIN** tab.
3. In the **Select user (user@domain)** field, type the username for which to create a PIN, and click `>>`
4. In the **New PIN** field, type a personal identification number (PIN).
5. In the **Confirm PIN** field, type the PIN that you typed in the **PIN** field.
6. Click **Save**.

   See the job aid for information about error messages that appear.

   The subscriber or the administrator can modify the VSC PIN using Personal Agent.

**Creating a VSC PIN for a subscriber job aid**

While entering the Vertical Service Codes PIN, you can receive error messages as follows:

- If services that use the Vertical Service Codes PIN are not assigned to a subscriber, the following error message appears:

  ![Error Message](image)

- If you enter any other characters except digits, or enter fewer than 4 or more than 10 digits, the following error message appears:

  ![Error Message](image)

Assigning the SIP PBX service to a domain

Use this procedure to assign the SIP PBX service to a domain.

**Before you begin**

- You have Services provisioning rights.
Procedure
1. From the Provisioning Client menu bar, select Solution, CS 2000, SIP PBX to access the SIP PBX portlet.
2. On the ISN Data tab, from the Select domain list, select a domain.
3. Click >.
4. To modify a node name, select the link for the node.
5. On the ISN Data tab, configure the parameters as required.
6. Click Save.

Assigning the SIP PBX service to a user job aid
This job aid describes the parameters for the ISN data tab in the SIP PBX Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Type a user name in this field.</td>
</tr>
<tr>
<td>New password</td>
<td>Type a password in this field.</td>
</tr>
<tr>
<td>Confirm password</td>
<td>Type the new password again in this field.</td>
</tr>
<tr>
<td>Charge DN</td>
<td>Type the Charge DN in this field.</td>
</tr>
<tr>
<td>Tel URI support</td>
<td>Select to enable telephone Uniform Resource Identifier (URI) support.</td>
</tr>
</tbody>
</table>

Assigning the SIP Line service to a user
Use this procedure to assign the SIP Line service to a user.

Before you begin
- You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Solution > CS 2000 > SIP Line to access the SIP Line Service portlet.
2. On the User Data tab, in the Select a user box, type a user name.
3. Click >.
4. On the User Data tab, configure the parameters as required.
5. Click Save.
Assigning the SIP Line service to a user job aid

This job aid describes the parameters for the User data tab in the SIP Line Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End point ID</td>
<td>Enter an ID in this field.</td>
</tr>
<tr>
<td>Virtual media gateway</td>
<td>Select a media gateway from the list.</td>
</tr>
<tr>
<td>Sip profiles</td>
<td>Select a profile from the list.</td>
</tr>
</tbody>
</table>

Provisioning PSI Distribution for a domain

About this task

Application Server 5300 does not support Provisioning PSI Distribution for a domain.
Chapter 15: Service set procedures

About this task
Use the procedures in this section to add and list service sets.

• Adding a service set on page 180
• Listing and modifying service sets on page 181
• Deleting a service set on page 181

Adding a service set

About this task
Use this procedure to add a service set.

Procedure

1. From the Provisioning Client menu bar, select Services > Service Set to access the Service Set portlet.
2. On the Add tab, from the Select domain list, select the domain to which you want to add a service set.
3. From the Type list, select the type of user for this service set.

<table>
<thead>
<tr>
<th>To add</th>
<th>Choose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Server 5300 subscriber</td>
<td>Standalone</td>
</tr>
<tr>
<td>TDM subscriber (External subscriber - does not register)</td>
<td>TDM Mirror</td>
</tr>
</tbody>
</table>
4. Click >>.
5. In the Name box, type the name of the service set.
6. Check the boxes for the services you want to add in the service set.
7. Click Save.
Listing and modifying service sets

About this task
Use this procedure to list and modify service sets for a domain.

Important:
Clients do not receive notification about changes to their service sets. Any changes (such as presence preferences) take effect after the next log on.

Procedure
1. From the Provisioning Client menu bar, select Services > Service Set to access the Service Set portal.
2. On the List tab, from the Select domain list, choose a domain, and then click >>
3. In the Name column of the table, click the service set that you want to modify.
4. In the Name box, type a new name for the service set.
5. Select the services that you want to assign.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Assign a service</td>
<td>Select the corresponding check box.</td>
</tr>
<tr>
<td>Remove a service from the service set</td>
<td>Clear the corresponding check box.</td>
</tr>
</tbody>
</table>

6. If a system profile applies to a specific service, select the system profile from the list. For example, you may have system profiles for the Presence service.
7. Click Save.

Deleting a service set

About this task
Use the following procedure to delete a service set no longer in use by the system.

Procedure
1. From the Provisioning Client menu bar, select Services > Service Set to access the Service Set portal.
2. On the List tab, from the Select domain list, choose a domain, and then click >>
3. To delete a service set, click Delete for the corresponding service set.
4. In the confirmation dialog, type your administrator password and click Confirm.
Chapter 16: User services management procedures

About this task
Use the procedures in this chapter to define and assign services to domains.

- Configuring system profiles for services on page 184
- Copying service profiles on page 191
- Listing, modifying and deleting system profiles on page 191
- Assigning or removing a system profile from a domain on page 192
- Assigning services to a domain on page 192
- Listing and modifying user system profile and user profile on page 193
- Ad Hoc Conferencing service configuration on page 194
- Advanced Screening service configuration on page 197
- Allowed Clients service configuration on page 198
- Call Forward Variants service configuration on page 200
- Call Grabber service configuration on page 202
- Call Park service configuration on page 206
- Call Pickup on page 208
- Call Return service configuration on page 216
- Call Type Based Screening service configuration on page 217
- Calling Line ID Restriction service configuration on page 220
- Configuring the Client Collaboration service on page 222
- Core Services Session Manager profile configuration on page 223
- Configuring the Deny All Calls service on page 225
- Configuring the Direct to Gateway service on page 226
- Configuring Hot Line service on page 227
- Configuring routable services information for IM Chat on page 228
- Configuring Low Bandwidth Link on page 229
- Configuring Media Portal Service on page 229
• Configuring Multiple Attendants service on page 230
• Configuring Meet Me Conferencing service on page 230
• Configuring routable services information to a Mobility Gateway on page 233
• Defining the match criteria for the advanced address book on page 233
• E911 Options service configuration on page 234
• Malicious Call Trace service configuration on page 241
• Mobile Extension service configuration on page 243
• MLPP service configuration on page 243
• Multiple Call Restriction service configuration on page 255
• Multiple Register service configuration on page 256
• Music On Hold service configuration on page 258
• Network Call Logs service configuration on page 262
• Network Call Waiting Disable service configuration on page 264
• PBX Communicator service configuration on page 266
• Personal Ringback Tones service configuration on page 266
• Presence service configuration on page 266
• Provisioning Short Dialing Codes on page 269
• Quality of Service configuration on page 269
• Routable services information configuration for Meet Me Audio Conferencing on page 271
• Routable services information configuration for the Music on Hold (MOH) feature on page 273
• Configuring Service Capabilities Interaction Manager on page 273
• Selective Call Reject service configuration on page 273
• TDM Message Waiting Indicator service configuration on page 276
• Configuring UCC Short Message Service on page 277
• Uniform Call Distribution service on page 278
• Routable services information configuration for Unified Communication service on page 278
• Video service configuration on page 280
• Voice mail configuration on page 283
• XMPP Gateway service configuration on page 292

For more information about possible service interactions, see Table 9: Service interactions on page 63.
Configuring system profiles for services

Use this procedure to configure system profiles for services.

⚠️ Important:

Do not modify the "_system_default_" profile.

⚠️ Note:

Not all services need system profiles. For more information, see Configuring system profiles for services job aid on page 184.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Service Profiles to access the User Services portlet.

2. On the Services tab, select the service for which you want to create a system profile.

3. From the portlet of the service you selected, configure the service data on the System Profile tab if applicable.

4. Click Save.

---

Configuring system profiles for services job aid

About this task

The following job aid describes the service data for the System Profile tab of all those services that require system profiles.

The following services do not require a system profile:

• Device Access Restrictions
• Malicious call trace
• Meet me conferencing
• Music on hold
• Short dialing code
• Unified communications

<table>
<thead>
<tr>
<th>Service</th>
<th>Service data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad Hoc Conferencing</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Maximum number of ports</td>
<td>Initiates an Ad Hoc audio conference call utilizing a SIP audio server. The number of users</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Service</th>
<th>Service data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ad hoc conferencing via VSC</td>
<td>Check the box to enable this service using Vertical Service Code (VSC).</td>
<td></td>
</tr>
<tr>
<td>Advanced Addressbook</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Maximum Number of address book entries allowed</td>
<td>Specifies the maximum number of entries in a Personal Address Book, up to 750 entries. If this service is not enabled, the maximum number of entries is 50.</td>
</tr>
<tr>
<td>Advanced screening</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Busy</td>
<td>Check this box to enable the busy indication.</td>
</tr>
<tr>
<td></td>
<td>Maximum number of ringlists</td>
<td>Specifies the maximum number of sequential ringlists.</td>
</tr>
<tr>
<td></td>
<td>Maximum Number of telephone numbers per ringlist</td>
<td>Specifies the maximum number of devices that are simultaneously rung at once, as defined in a route in the Personal Agent.</td>
</tr>
<tr>
<td></td>
<td>No answer</td>
<td>Check this box to enable the No answer capability.</td>
</tr>
<tr>
<td></td>
<td>Presence Based Routing</td>
<td>Specifies the ability to route calls and instant messages based on a user's presence status. For example, if the presence state is Unavailable Busy, then a route is created in the Personal Agent, which directs all the user's calls or IMs to voice mail.</td>
</tr>
<tr>
<td>Allowed Clients</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>PCCClientSet Control</td>
<td>Enables you to use your IP Deskphone for premium-quality voice calls.</td>
</tr>
<tr>
<td></td>
<td>PCCClient Voice</td>
<td>Enables the user to use the Avaya Aura® AS 5300 UC Client for premium-quality voice calls.</td>
</tr>
<tr>
<td></td>
<td>Multimedia Office Client</td>
<td>Enables the user to use the Avaya Aura® AS 5300 Office Client. This client is integrated with the Microsoft Outlook Client.</td>
</tr>
<tr>
<td></td>
<td>Web Client</td>
<td>Dedicated to the Web-based components of the multimedia conversation.</td>
</tr>
<tr>
<td>Call Forward Variants</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Call forward variants busy</td>
<td>Allows a user to forward calls whenever busy (that is, engaged in a call).</td>
</tr>
<tr>
<td></td>
<td>Call forward variants no answer</td>
<td>Allows a user to forward calls whenever the user does not answer.</td>
</tr>
<tr>
<td>Service</td>
<td>Service data</td>
<td>Description</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Call forward variants immediate</td>
<td></td>
<td>Allows a user to forward all incoming calls to a specified DN.</td>
</tr>
<tr>
<td>Call Park</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Autoretrieve Parked Calls</td>
<td>Check this box to enable automatically retrieve parked calls.</td>
</tr>
<tr>
<td></td>
<td>Autoretrieve Timer (in seconds)</td>
<td>Provides a default time period that a call can remain parked and unattended before a call is automatically retrieved to the user that parked the call. The user can configure the preferred Autoretrieve time through Preferences in the Personal Agent.</td>
</tr>
<tr>
<td>Call Return</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Call return via VSC</td>
<td>Check the box to enable this service using VSC.</td>
</tr>
<tr>
<td>Call Type Based Screening</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Call type based screening via VSC</td>
<td>Check the box to enable this service using VSC.</td>
</tr>
<tr>
<td>Calling Line ID Restriction</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Calling Name/Number Privacy</td>
<td>Enables a user to see the setting in their Personal Agent that provides the option to specify whether their name and number appear when they call someone.</td>
</tr>
<tr>
<td></td>
<td>Media Privacy (Media Portal Required)</td>
<td>Enable the media privacy capability. This service is available only if you have Media Portal on your system.</td>
</tr>
<tr>
<td></td>
<td>Calling name/number restriction per call via VSC</td>
<td>Check the box to enable this service using VSC.</td>
</tr>
<tr>
<td></td>
<td>Calling name/number presentation per call via VSC</td>
<td>Check the box to enable this service using VSC.</td>
</tr>
<tr>
<td></td>
<td>Calling name/number privacy permanent via VSC</td>
<td>Check the box to enable this service using VSC.</td>
</tr>
<tr>
<td>Client Collaboration</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>(not supported for Federal Service packages)</td>
<td>File Transfer</td>
<td>Enables users to transfer files.</td>
</tr>
<tr>
<td></td>
<td>Transfer Clipboard</td>
<td>Enables users to exchange contents of a Windows clipboard.</td>
</tr>
<tr>
<td></td>
<td>WebPush</td>
<td>Enables users to send and receive Web site URLs.</td>
</tr>
<tr>
<td></td>
<td>White Board</td>
<td>Enables users to share a common drawing window for entering text and graphics.</td>
</tr>
<tr>
<td>Colorful Ringback Tones</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>(not supported)</td>
<td>Personal Agent Enabled (ringtone selection)</td>
<td>Enables ringtone selection.</td>
</tr>
<tr>
<td>Service</td>
<td>Service data</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>--------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Deny All Calls</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Deny all incoming calls</td>
<td>Allows the administrator or user to block incoming calls.</td>
</tr>
<tr>
<td></td>
<td>Deny all outgoing calls</td>
<td>Allows the administrator or user to bar outgoing calls.</td>
</tr>
<tr>
<td></td>
<td>Deny all incoming calls via VSC</td>
<td>Allows the administrator or user to block incoming calls, using the VSC option.</td>
</tr>
<tr>
<td></td>
<td>Deny all outgoing calls via VSC</td>
<td>Allows the administrator or user to bar outgoing calls using the VSC option.</td>
</tr>
<tr>
<td>Hotline</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Protected Hotline</td>
<td>Select the check box to enable Protected Hotline. Protected Hotline supports only the SA user type; non-protected supports the SA, SSL, and IMS user types.</td>
</tr>
<tr>
<td></td>
<td>Hotline Type</td>
<td>Options: Origination Only, Termination Only, and Both Origination and Termination</td>
</tr>
<tr>
<td></td>
<td>Hotline Indicator</td>
<td>Options: Voice or Data</td>
</tr>
<tr>
<td>Mobile Extension</td>
<td>Not supported</td>
<td>Not supported</td>
</tr>
<tr>
<td>Multi-Level Precedence and Preemption</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Namespace name</td>
<td>Select one of the names from the list.</td>
</tr>
<tr>
<td></td>
<td>Maximum priority</td>
<td>Select the priority from the list.</td>
</tr>
<tr>
<td></td>
<td>Diversion destination</td>
<td>Specifies the diversion destination.</td>
</tr>
<tr>
<td></td>
<td>Audio DSCP Name</td>
<td>Choose the DSCP marking profile to use for Audio. The audio DSCP profile defines DSCP categories, values, marking states, and IP Tables rules for audio.</td>
</tr>
<tr>
<td></td>
<td>Video DSCP Name</td>
<td>Choose the DSCP marking profile to use for video. The video DSCP profile defines DSCP categories, values, marking states, and IP Tables rules for video.</td>
</tr>
<tr>
<td>Multiple Call Restriction</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Number of Simultaneous Calls</td>
<td>Specifies the number of calls permitted at the same time.</td>
</tr>
<tr>
<td>Multiple Register</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Maximum Number of Logins Allowed</td>
<td>Specifies the maximum number of logons for a user.</td>
</tr>
<tr>
<td>Network Call Logs</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
</tbody>
</table>

*Table continues…*
<table>
<thead>
<tr>
<th>Service</th>
<th>Service data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Maximum number of Inbox Call Logs</td>
<td>Specifies the maximum number of call logs for the Inbox. Range: 10–100</td>
</tr>
<tr>
<td></td>
<td>Maximum Number of Outbox Call Logs</td>
<td>Specifies the maximum number of call logs for the Outbox. Range: 10–100</td>
</tr>
<tr>
<td>Network Call Waiting disable</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Network call waiting disable via VSC</td>
<td>Disables network call waiting for a specific call through VSC.</td>
</tr>
<tr>
<td></td>
<td>Network call waiting disable permanent via VSC</td>
<td>Disables network call waiting permanently through VSC.</td>
</tr>
<tr>
<td>PBX Communicator (not supported)</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>OBG address name</td>
<td>Enter a valid address.</td>
</tr>
<tr>
<td></td>
<td>OBG port</td>
<td>Enter a valid TCP Port address.</td>
</tr>
<tr>
<td></td>
<td>CSTA switching function path for system services</td>
<td>As a CSTA switching function, the OBG provides web service endpoint for system services. The URL address for system services is derived from the OBG/PBX IP address at run-time.</td>
</tr>
<tr>
<td></td>
<td>CSTA switching function path for monitoring services</td>
<td>As a CSTA switching function, the OBG provides web service endpoint for monitoring services. The URL address for monitoring services is derived from the OBG/PBX IP address at run-time.</td>
</tr>
<tr>
<td></td>
<td>CSTA switching function path for call control features</td>
<td>As a CSTA switching function, the OBG provides web service endpoint for call control features. The URL address for call control features is derived from the OBG/PBX IP address at run-time.</td>
</tr>
<tr>
<td></td>
<td>CSTA switching function path for snapshot services</td>
<td>As a CSTA switching function, the OBG provides web service endpoint for snapshot services. The URL address for snapshot services is derived from the OBG/PBX IP address at run-time.</td>
</tr>
<tr>
<td></td>
<td>CSTA keepalive watchdog timer (in seconds)</td>
<td>This is a timer that the OPE waits for the “System Status” request from a PBX/OBG before considering the OBG/PBX unavailable. The value is defined in terms of seconds. A value of zero disables the keepalive mechanism.</td>
</tr>
<tr>
<td></td>
<td>CSTA keepalive retry timer (in seconds)</td>
<td>This is an interval at which the OPE retries the &quot;RequestSystemStatus&quot; requests to the OBG/ PBX. The value is specified in seconds. A value of zero disables the keepalive mechanism.</td>
</tr>
<tr>
<td></td>
<td>PBX communicator session timer (in hours)</td>
<td>Not currently supported.</td>
</tr>
</tbody>
</table>

*Table continues...*
<table>
<thead>
<tr>
<th>Service</th>
<th>Service data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Max number of retries before declaring out-of-sync</td>
<td>This is the number of the &quot;RequestSystemStatus&quot; requests that the OPE service will make before it declares the OBG/PBX unavailable, which causes all established uaCSTA sessions to be terminated and reset. A value of zero disables the session reset.</td>
</tr>
<tr>
<td></td>
<td>PBX communicator application ID</td>
<td>This is the ID of the OPE server sent to SOAP requests to the OBG. An empty string removes the ID from the SOAP requests.</td>
</tr>
<tr>
<td></td>
<td>Maximum number of TR-87 connections per OPE server</td>
<td>This the maximum number of TR-87 connections set up at an OPE server.</td>
</tr>
<tr>
<td>Presence</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>Maximum friends list</td>
<td>Specifies the number of people in a list of friends. A user can subscribe up to 100 people to view their presence. Although users can log on to numerous devices, the list of friends is a shared resource. For example, if the maximum list of friends size is configured to 10, then each of the client devices can hold 10 friends (the same 10 friends, not 10 per device). The client has the option of sending Presence status to any of the friends.</td>
</tr>
<tr>
<td></td>
<td>Report when inactive</td>
<td>Enables the autopresence (optional) feature that detects when a PC is not in use and updates their Presence status on the network.</td>
</tr>
<tr>
<td></td>
<td>Inactivity timer</td>
<td>Determines the length of time a user’s PC must be idle before their Presence status is updated on the network.</td>
</tr>
<tr>
<td></td>
<td>Enhanced authorization</td>
<td>Allows users to screen watchers. If this option is configured to Yes, the system prompts the user to authorize each watcher using the Avaya Aura® AS 5300 UC Client. The default value is Not Set, which allows watchers to see the user's presence, unless specifically banned.</td>
</tr>
<tr>
<td></td>
<td>Report when on the phone</td>
<td>Detects when a user is on an active call and updates the user’s Presence status on the network.</td>
</tr>
<tr>
<td>QoS</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td></td>
<td>QoS DiffServ Code for Audio</td>
<td>Specifies quality of service for client signaling.</td>
</tr>
<tr>
<td></td>
<td>QoS DiffServ Code for Video</td>
<td>Specifies quality of service for client video.</td>
</tr>
<tr>
<td>Selective Call Reject</td>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
</tbody>
</table>
### Service

<table>
<thead>
<tr>
<th>Service data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Incoming selective call reject</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict incoming calls.</td>
</tr>
<tr>
<td>Outgoing selective call reject</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict outgoing calls.</td>
</tr>
<tr>
<td>Incoming selective call reject via VSC</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict incoming calls through VSC.</td>
</tr>
<tr>
<td>Outgoing selective call reject via VSC</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict outgoing calls through VSC.</td>
</tr>
<tr>
<td>Add incoming call to selective reject list</td>
<td>Allows the administrator or user to add incoming calls to their Selective Reject List.</td>
</tr>
</tbody>
</table>

### Video

- **Profile name**: Type a profile name for this service.
- **Available video codecs**: The list of video codecs available on the system.
- **Selected video codecs**: List of video codecs that will be included to the selection list box in the Video Configuration dialog in the AS 5300 UC Client.
- **Maximum bitrate (in kbps)**: The maximum allowed bitrate for video, between 8 and 7000 kbps. This is a numeric field.
- **Maximum video width (in pixels)**: The maximum allowed width for video, between 32 and 1280 pixels. Pixel sizes should be multiples of 8. This is a numeric field.
- **Maximum video height (in pixels)**: The maximum allowed height for video, between 32 and 720 pixels. Pixel sizes should be multiples of 8. This is a numeric field.

### Voicemail

- **Profile name**: Type a profile name for this service.
- **Revertive call support**: Retrieve voice mail or, for other subscribers, to leave a voice mail message. Voice mail is retrieved from a network server. The user is aware of deposited voice mail since the user’s client’s message waiting indicator (MWI) is enabled.
- **Voice mail retrieve via VSC**: Retrieve voice mail using the Vertical Service Code.
Copying service profiles

About this task

Use this procedure to create a copy of the system service profile and to copy the system profile to a domain. This procedure does not remove any existing profiles in the domains to which you assign a profile.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Service Profiles to access the User Services portlet.
2. On the Services tab, select the service for which you want to copy the system profile.
3. On the System tab of the portlet for the service you have chosen, locate in the list of Profile names the profile you want to copy and click Copy.
4. On the Copy window of the System Profile tab, add a new Profile name and adjust any additional profile information, as required.
5. (Optional) To assign the copied profile to all domains, to which the original system profile is assigned, select Copy profile assignment to domains.
6. Click Save.

Listing, modifying and deleting system profiles

Use this procedure to list, modify, and delete system profiles of a service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain, Domain Steps, Assign Service Profiles to access the User Services portlet.
2. On the Services tab, select the service for which you want to modify the system profile.
3. To delete a system profile, select Delete for the profile name from the Delete table column.
4. To modify a system profile, click the link for the profile from the Profile name table column.
5. Modify the data of the service you selected in the System Profile tab.
6. Click Save.
Modifying system profiles job aid

About this task
To modify system profiles of services, see Configuring system profiles for services job aid on page 184.

Assigning or removing a system profile from a domain

Use this procedure to assign or remove a system profile from a domain

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Service Profiles to access the User Services portlet.
2. On the Services tab, select the service for which you want to modify the system profile.
3. Click Assign/Remove for the profile that you want to assign to a domain or remove from a domain.
4. From the Available Domains list, select a domain and click Copy
5. To remove a domain, select a domain from the Selected Domains field, and click Remove.
6. Click Save.

Assigning services to a domain

Use this procedure to assign services to a domain. After services are assigned, they are available to the domain.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services
2. On the Services Assignment tab, from the Select a domain list, select a domain and click >>.
3. If you want to assign all services to the domain you selected, select the Assign all services check box.
4. To assign a specific service, click to select the corresponding check box for the service.
5. Click **Save**.

---

**Listing and modifying user system profile and user profile**

Use this procedure to list and modify user system profile and user profile.

**Before you begin**
- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > Domain Steps > Assign Service Profiles** to access the User Services portlet.
2. On the **Services** tab, select the link of the service you want to modify.
3. On the service portlet, select the **User data** tab to modify the User system profile and User profile.
   
   Some services have both User system profile and User profile, and some services may have only one of them.
4. In the **Select user** box, type the user name that you want to modify and click `>>`
5. To modify the User system profile, select the profile from the list.
6. Click **Save**.
7. Configure the services for the User profile.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable a service</td>
<td>Select the corresponding check box.</td>
</tr>
<tr>
<td>Disable a service</td>
<td>Clear the corresponding check box.</td>
</tr>
</tbody>
</table>

---

**Listing and modifying user system profile and user profile job aid**

**About this task**

This job aid describes the parameters in the **User Data** tab of the service portlet you selected.

As an example, the following job aid shows you the parameters in the **User Data** tab of the Ad hoc conferencing service.

Some services require configuration for both User system profile and User profile; however, some services require configuration for only one of the profiles.
Parameter | Description
--- | ---
User system profile | Select the user system profile from the list.
User profile | Check the Ad hoc conferencing box to enable the service.

**Note:**
By default, Ad hoc conferencing is enabled.

---

# Ad Hoc Conferencing service configuration

## About this task

Use the procedures in this section to configure Ad Hoc Conferencing service.

- [Configuring Ad hoc audio conferencing service](#) on page 194
- [Configuring routable services information for Ad Hoc audio conferencing](#) on page 195
- [Assigning Ad Hoc Conferencing service to a domain](#) on page 196
- [Assigning Ad Hoc Conferencing service to a user](#) on page 196

## Configuring Ad hoc audio conferencing service

Use this procedure to configure Ad hoc audio conferencing service.

Ad hoc conferencing service has the following capabilities:

- allows multiple users to join together in a call
- provides on-demand conference, with no requirements for reservations
- requires a media server
- available to all clients

### Before you begin

- You have Services provisioning rights.

### Procedure

1. From the Provisioning Client menu bar, select Services > Conferencing > Ad Hoc Conferencing to access the Ad Hoc Conferencing Service portlet.
2. In the Ad Hoc Conferencing Service portlet, configure the service data on the System Profile tab.
3. Click Save.
Configuring Ad hoc audio conferencing service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Ad Hoc Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Maximum number of ports</td>
<td>Assign the maximum number of ports allowed from the list.</td>
</tr>
<tr>
<td>Ad hoc conferencing via VSC</td>
<td>Select the check box to enable Ad hoc conferencing, using the Vertical Service Code (VSC).</td>
</tr>
</tbody>
</table>

Configuring routable services information for Ad Hoc audio conferencing

About this task

Use this procedure to configure access to the Ad Hoc Audio Conferencing logical entity in the domain where you need service.

The Ad Hoc Audio Conferencing service is based on the Avaya Media Server platform and allows the network to support both Ad Hoc conferencing and consultative call transfers.

Procedure

1. From the Provisioning Client menu bar, select Services > Conferencing > Ad Hoc Conferencing to access the Ad Hoc Conferencing Service portlet.
2. In the Ad Hoc Conferencing Service portlet, select the Ad Hoc Conference tab.
3. From the Select domain list, select a domain to which you want to add Ad Hoc Conferencing Service and click >>.
4. In the Select Pool field, select the name of a pool and click >>.
5. In the Add locations area, select the check boxes for the locations that this logical entity will service.

⚠️ Important:

If user's location is not assigned to any pool, the AS 5300 Session Manager looks for the pool in the location "Other".

6. Click Save.

Ad Hoc Conferencing Service: Ad Hoc Conference parameters job aid

This job aid describes the parameters for the Ad Hoc Conference tab in the Ad Hoc Conferencing Service portlet.
User services management procedures

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select pool</td>
<td>Enables you to select another pool from the list.</td>
</tr>
<tr>
<td>Add locations (for the pool you selected)</td>
<td>Assign a location for the pool.</td>
</tr>
<tr>
<td>List assigned locations</td>
<td>Shows the currently selected locations for pool, if previously assigned.</td>
</tr>
</tbody>
</table>

Assigning Ad Hoc Conferencing service to a domain

Use this procedure to assign the Ad Hoc Conferencing service to a domain.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Domain > Domain Steps > Assign Services** to access the User Services portlet.
2. Select the **Service Assignment** tab.
3. From the **Select domain** list, select a domain and click `>>`.
4. Click to select the corresponding check box for Ad Hoc Conferencing.
5. Click **Save**.

Assigning Ad Hoc Conferencing service to a user

Use this procedure to assign the Ad Hoc Conferencing service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Services, Assign Services** to access the User Services portlet.
2. On the **Services** tab, select the **Ad Hoc Conferencing** link.
3. On the **User Data** tab, type a user name in the **Select user** field.
4. Click `>>`.
5. From the **User system profile** list, select a profile.
6. Click **Save**.
7. Check the **Ad hoc conferencing** box in User Profile.
8. Click **Save**.
**Assigning Ad Hoc Conferencing service to a user job aid**

This job aid describes the parameters for the **User Data** tab in the Ad Hoc Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User system profile</td>
<td>Select the user system profile from the list.</td>
</tr>
<tr>
<td>User profile</td>
<td>Check the Ad hoc conferencing box to enable the service.</td>
</tr>
</tbody>
</table>

*Note:* Ad hoc conferencing is enabled by default.

**Advanced Screening service configuration**

**About this task**

Use the procedures in this section to configure the Advanced Screening service.

- [Configuring the Advanced Screening service](#) on page 197
- [Assigning the Advanced Screening service to a user](#) on page 198

**Configuring the Advanced Screening service**

Use this procedure to configure the Advanced Screening service.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Routing > Advanced Screening** to access the Advanced Screening Service portlet.
2. Configure the parameters in the **System Profile** tab.
3. Click **Save**.

**Configuring the Advanced Screening service job aid**

**About this task**

This job aid describes the parameters for the **System Profile** tab in the Advanced Screening Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Busy</td>
<td>Specifies that the user is busy.</td>
</tr>
<tr>
<td>Maximum number of ringlists</td>
<td>Specifies the maximum number of sequential ringlists allowed.</td>
</tr>
<tr>
<td>Maximum Number of telephone numbers per ringlist</td>
<td>Specifies the maximum number of devices that can be simultaneously rung at once, as defined in a route in the Application Server 5300 Personal Agent.</td>
</tr>
<tr>
<td>No answer</td>
<td>Specifies that the user is not answering.</td>
</tr>
<tr>
<td>Presence Based Routing</td>
<td>Specifies the ability to route calls and instant messages based on a user's presence status. For example, if the presence state is Unavailable Busy, then a route is created in the Personal Agent which directs all the user's calls or IMs to voice mail.</td>
</tr>
</tbody>
</table>

### Assigning the Advanced Screening service to a user

Use this procedure to assign the Advanced Screening service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, select Advanced Screening.
3. On the User Data tab, add a user name in the Select user field.
4. Click >>.
5. From the User system profile list, select a profile.
6. Click Save.

### Allowed Clients service configuration

**About this task**

Use the procedures in this section to configure the Allowed Clients service.

- Configuring the Allowed Clients service on page 199
- Assigning the Allowed Clients service to a domain on page 199
- Assigning the Allowed Clients service to a user on page 200
Configuring the Allowed Clients service

Use this procedure to configure the Allowed Clients service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Client Interface > Allowed Clients to access the Allowed Clients Service portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.

Configuring the Allowed Clients service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Allowed Clients Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>PCClientSet control</td>
<td>Enables the user to use the IP Deskphone for premium-quality voice calls.</td>
</tr>
<tr>
<td>PCClient Voice</td>
<td>Enables the user to use the Avaya Aura® AS 5300 UC Client for premium-quality voice calls.</td>
</tr>
<tr>
<td>Avaya Aura AS 5300 Office Client</td>
<td>Enables the user to use the Avaya Aura® AS 5300 Office Client.</td>
</tr>
<tr>
<td>(Not supported)</td>
<td></td>
</tr>
<tr>
<td>Avaya Aura AS 5300 Web client</td>
<td>Enables the user to use the AS 5300 Web Client.</td>
</tr>
</tbody>
</table>

Assigning the Allowed Clients service to a domain

Use this procedure to assign the Allowed Clients service to a user.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. Select the Service Assignment tab.
3. From the Select domain list, select a domain and click >>.
4. Click to select the corresponding check box for Allowed Clients.
5. Click Save.

Assigning the Allowed Clients service to a user

Use this procedure to assign the Allowed Clients service to a user.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Allowed Clients.
3. On the User Data tab, add a user name in the Select user field.
4. Click >>.
5. From the User system profile list, select a profile.
6. Click Save.

Call Forward Variants service configuration

About this task

Use the procedures in this section to configure the Call Forward Variants service.

- Configuring the Call Forward Variants service profile on page 200
- Assigning the Call Forward Variants service profile to a domain on page 201
- Assigning the Call Forward Variants service profile to a user on page 202

Configuring the Call Forward Variants service profile

Use this procedure to configure the Call Forward Variants service profile.

Before you begin

- You have Services provisioning rights.
- You have Call Forward Management provisioning rights.
- You have assigned the Call Forward Variants service to the domain. See Assigning services to a domain on page 192
• You have assigned the Call Forward Subscribers license key resource to the domain. See Assigning resources to a domain on page 116.

Procedure
1. From the Provisioning Client menu, select Services > Call Routing > Call Forward Variants to access the portlet.
2. In the System Profile tab, configure the parameters as required.
3. Click Save.

Configuring the Call Forward Variants service profile job aid

About this task
This job aid describes the parameters for the System Profile tab in the Call Forward Variants Service portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Call forward variants busy</td>
<td>Allows a user to forward calls whenever the user’s device is busy (that is, engaged in a call).</td>
</tr>
<tr>
<td>Call forward variants no answer</td>
<td>Allows a user to forward calls whenever the user does not answer.</td>
</tr>
<tr>
<td>Call forward immediate</td>
<td>Allows a user to forward all incoming calls to a specified DN.</td>
</tr>
</tbody>
</table>

Assigning the Call Forward Variants service profile to a domain

Use this procedure to assign the Call Forward Variants service profile to a domain.

Before you begin
• You have Services provisioning rights.
• You have Call Forward Management provisioning rights.
• You have assigned the Call Forward Variants service to the domain. See Assigning services to a domain on page 192.
• You have assigned the Call Forward Subscribers license key resource to the domain. See Assigning resources to a domain on page 116.
• You have set up the service profile. See Configuring the Call Forward Variants service profile on page 200.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Routing > Call Forward Variants to access the portlet.
2. Click Assign/Remove for the profile that you want to assign to a domain from the Domain column.
3. From the Available Domains list, select a domain and click Copy.
4. To remove a domain, select a domain from the **Selected Domains** field and click **Remove**.
5. Click **Save**.

---

**Assigning the Call Forward Variants service profile to a user**

Use this procedure to assign the Call Forward Variants service profile to a user.

**Before you begin**

- You have Services provisioning rights.
- You have Call Forward Management provisioning rights.
- You have assigned the Call Forward Variants service to the domain. See **Assigning services to a domain** on page 192.
- You have assigned the Call Forward Subscribers license key resource to the domain. See **Assigning resources to a domain** on page 116.
- You have set up the service profile. See **Configuring the Call Forward Variants service profile** on page 200.
- You have assigned the service profile to a domain. See **Assigning the Call Forward Variants service profile to a domain** on page 201.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Routing > Call Forward Variants** to access the portlet.
2. From the **User Data** tab, add a user name in the **Select user** field.
3. Click `>>`.
4. From the **User system profile** list, select a profile.
5. Click **Save**.

---

**Call Grabber service configuration**

**About this task**

Use the procedures in this section to configure the Call Grabber service.

- **Assigning Call Grabber service to a domain** on page 203
- **Assigning resources for Call Grabber** on page 203
- **Configuring the Call Grabber service profile** on page 203
- **Assigning the Call Grabber service profile to a domain** on page 204
- **Assigning the Call Grabber service to users** on page 204
Assigning Call Grabber service to a domain

About this task
User this procedure to assign Call Grabber service to a domain.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. Click the Service Assignment tab.
3. From the Select domain list, select the domain to which you want to assign the Call Grabber service and click >>
4. On the Service Assignment tab, scroll through the list of services and select the corresponding check box for Call Grabber.
5. Click Save.

Assigning resources for Call Grabber

About this task
Use this procedure to assign resources for Call Grabber.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Resources to access the Resource Management portlet.
2. Click the Domain Resources tab.
3. From the Select domain list, select a domain and click >>.
4. On the Domain Resources tab, scroll to the Call Grabber row and assign the required number of units under the Assign column.
5. Click Save.

Configuring the Call Grabber service profile

About this task
Use this procedure to configure the Call Grabber service profile.
**Procedure**

1. From the Provisioning Client menu bar, select Services > Call Routing > Call Grabber to access the Call Grabber Service portlet.
2. On the System Profile tab, configure the parameters.
3. Click Save.

**Setting up the Call Grabber service profile job aid**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>A profile name for this service.</td>
</tr>
<tr>
<td>From Registered Clients</td>
<td>When selected, enables grabbing from registered clients.</td>
</tr>
<tr>
<td>From trusted Nodes</td>
<td>When selected, enables grabbing from trusted clients.</td>
</tr>
</tbody>
</table>

**Assigning the Call Grabber service profile to a domain**

**About this task**
Use this procedure to assign the Call Grabber service profile to a domain.

**Procedure**

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Service Profiles to access the User Services portlet.
2. On the Services tab, select Call Grabber in the Services column of the table.
3. On the System profile tab, click Assign/Remove in the Domain column of the table for the profile that you want to assign to a domain.
4. From the Available Domains list, select a domain and click Copy.
5. Click Save.

**Assigning the Call Grabber service to users**

**About this task**
Use this procedure to assign Call Grabber to users.

**Procedure**

1. From the Provisioning Client menu bar, select User > Search to access the User portlet.
2. On the Advanced Search tab, from the Domain list, select the domain.
3. From the Search by list, select the search criteria.
4. (Optional) In the Search for box, type the search string.
5. Click Search.
6. On the Advanced Search tab, in the Username column, click the name of the user.
7. Click the Services tab of the User portlet.
8. Scroll through the table and click the corresponding check box for Call Grabber.
9. Click Save.

Assigning the Call Grabber service profile to a user

About this task
Use this procedure to assign the Call Grabber service profile to a user.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Routing > Call Grabber to access the Call Grabber Service portlet.
2. On the User Data tab, type a user name in the Select user box and click >>.
3. On the User Data tab, from the User's system profile list, select a profile and click Save.
4. On the User Data tab, enter a calling party ID in the Authorized Calling Party Id field and click Save.

Assigning the Call Grabber service profile to a user job aid

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized Calling Party Id</td>
<td>The ID of the user authorized to grab active calls of this user, for example, PSTN DN.</td>
</tr>
</tbody>
</table>

Adding Call Grabber feature translation triggers in a domain

Use this procedure to add new Call Grabber feature translation triggers in a domain.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Routing > Vertical Service Codes to access the Vertical Service Codes Service portlet.
2. On the Feature Translation tab, select the domain from the list and click >>.
3. On the Feature Translation tab, in the Name box, type a name for the translation record.
4. In the Prefix box, type the DN for Call Grabber.
5. From the VSC service list, select Call Grabber.
6. Click Save.
Adding Call Grabber feature translation triggers in a domain job aid

About this task

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name to identify the translation record. The name must be unique in a domain and contain 1 to 32 characters.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The Call Grabber DN. The DN can be 2 to 32 characters long. It can begin with *, # or any digit, but must have digits for the remainder of the DN.</td>
</tr>
<tr>
<td>VSC Service</td>
<td>Select Call_Grabber for Call Grabber DN.</td>
</tr>
</tbody>
</table>

Call Park service configuration

About this task

Use the procedures in this section to configure the Call Park service.

- Configuring the Call Park service on page 206
- Assigning the Call Park service to a domain on page 207
- Assigning the Call Park service to a user on page 207

Configuring the Call Park service

Use this procedure to configure the Call Park service.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Routing > Call Park to access the Call Park Service portlet.
2. On the System Profile tab, configure the parameters as required.
3. Click Save.

Configuring the Call Park service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Call Park Service portlet.
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Auto-retrieve parked calls</td>
<td>Check this box to enable automatic retrieval of parked calls.</td>
</tr>
<tr>
<td>Auto-retrieve timer (in seconds)</td>
<td>Provides a default time period that a call can remain parked and unattended before the system automatically returns the call to the user who parked the call. The user can configure the preferred Autoretrieve time through Preferences in the Personal Agent.</td>
</tr>
</tbody>
</table>

### Assigning the Call Park service to a domain

Use this procedure to assign the Call Park service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. Select the Services Assignment tab.
3. From the Select a domain list, select a domain and click >>.
4. Click to select the corresponding check box for Call Park.
5. Click Save.

### Assigning the Call Park service to a user

Use this procedure to assign the Call Park service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Call Park.
3. On the User Data tab, type a user name in the Select user field.
4. Click >>.
5. From the User system profile list, select a profile.
6. In the System profile section, configure the Auto-retrieve parked calls and Auto-retrieve timer (in seconds) parameters, as required.
7. Click **Save**.

## Assigning the Call Park service to a user job aid

This job aid describes the parameters for the **User Data** tab in the Call Park Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>System profile</td>
<td>From the list, select the system profile for the user.</td>
</tr>
<tr>
<td>Auto-retrieve parked calls</td>
<td>Check this box to enable automatic retrieval of parked calls.</td>
</tr>
<tr>
<td>Auto-retrieve timer (in seconds)</td>
<td>Provides a default time period (in seconds) that a call can remain parked and unattended before the system automatically returns the call to the user who parked the call. The user can configure the preferred Autoretrieve time through Preferences in the Personal Agent.</td>
</tr>
</tbody>
</table>

---

## Call Pickup

Call Pickup allows users that are part of the same Call Pickup group to answer calls ringing devices belonging to other members in the group. Use the procedures in this section to configure Call Pickup group service.

### Related links

- [Configuring the Call Pickup service profile](#) on page 208
- [Assigning the Call Pickup group service profile to a domain](#) on page 209
- [Assigning the Call Pickup service to user](#) on page 210
- [Configuring the Call Pickup service group](#) on page 211
- [Searching for the Call Pickup group](#) on page 212
- [Assigning the Session Manager for the Call Pickup service group](#) on page 212
- [Adding members to the Call Pickup group](#) on page 212
- [Assigning a Group Administrator for a Call Pickup group](#) on page 213
- [Adding Call Pickup feature translation triggers in a domain](#) on page 214

---

## Configuring the Call Pickup service profile

### Before you begin

Ensure that:

- You have Services provisioning rights.
- You have Call Pickup Management provisioning rights.
- You have assigned the Call Pickup group service to the domain.
- You have assigned the Call Pickup group license key resource to the domain.
Procedure

1. From the **Provisioning client** menu bar, click **Services > Group services > Call Pickup** to access the Call Pickup service portlet.
2. Configure the parameters in the **System Profile** tab.
3. Click **Save**.

Call Pickup service configuration job aid

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Profile name for the service.</td>
</tr>
<tr>
<td>Group Call Pick-up</td>
<td>If you select this field, a user can pick up a call that is presented to any member of the group.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This feature is supported only with Avaya Aura® AS 5300 UC Client.</td>
</tr>
<tr>
<td>Directed Call Pick-up</td>
<td>If you select this field, a user can pick up a call that is presented to any member of the group by explicitly specifying the Group ID.</td>
</tr>
<tr>
<td>Targeted Call Pick-up</td>
<td>If you select this field, a user configured with targeted call pickup service can specify the DN or user ID for the ringing call within the assigned Call Pickup group. The pickup mechanism is similar to Directed Call Pick-up.</td>
</tr>
</tbody>
</table>

Assigning the Call Pickup group service profile to a domain

**Before you begin**

Ensure that:

- You have Services provisioning rights.
- You have Call Pickup Management provisioning rights.
- You have assigned the Call Pickup group service to the domain.
- You have assigned the Call Pickup group license key resource to the domain.
- You have set up the service profile.

**Procedure**

1. From the **Provisioning client** menu bar, click **Services > Group services > Call Pickup** to access the Call Pickup service portlet.
2. In the **Domain** column, click **Assign/Remove** for the profile that you want to assign to a domain.
3. From the **Available Domains** list, select a domain and click **Copy**.
4. **(Optional)** In the Selected **Domains** field, click a domain, and click **Remove**.  
The system removes the selected domain.
5. Click **Save**.

---

**Assigning the Call Pickup service to user**

**Before you begin**

Ensure that you have the Services provisioning rights.

**Procedure**

1. From the **Provisioning** menu bar, click **User > Search** to access the User portlet.
2. In the **Advanced Search** tab, type appropriate information about the user to whom you want to assign the feature, and click **Search**.
3. In the **Services** tab, select the check box next to the **Call Pickup** item, and click **Save**.
4. Click the **Call Pickup** link.
   
The system displays the **User Data** tab.
5. In the **Select user** field, type the user name, and click `>>`.
6. In the **User system profile** list, select a profile, and click **Save**.
7. Configure the parameters in the User Profile, and click **Save**.

**Call Pickup service assignment to a user job aid**

This job aid describes the **User Profile** fields on the **User Data** tab in the Call Pickup Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent Status</strong></td>
<td>Determines whether Call Pickup agents are active in a Call Pickup group. To be able to receive Call Pickup group calls, Call Pickup agents must be active in a Call Pickup group. If the <strong>Agent Status</strong> field is selected, the user is in the active state and can pick up the calls ringing to the group. The <strong>Agent Status</strong> field is selected by default.</td>
</tr>
</tbody>
</table>
Configuring the Call Pickup service group

Procedure

1. From the Provisioning Client menu bar, click Services > Group Services > Call Pickup to access the Call Pickup Service portlet.
2. Click the Add tab.
3. Select the domain and click >>.
4. In the Add tab, configure the required parameters.
5. Click Save.

Call Pickup group configuration job aid

This job aid describes the parameters for the Add tab in the Call Pickup Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>Name of the group.</td>
</tr>
<tr>
<td>Group identifier</td>
<td>Identifier for the group, similar to the AOR for the subscriber. The Group Identifier must be unique on the domain.</td>
</tr>
<tr>
<td>Group display name</td>
<td>Display name used for the group in all places visible to the user. For example, Group name displayed in Personal Agent.</td>
</tr>
<tr>
<td>Group aliases</td>
<td>String used to identify the group. You can specify multiple aliases for a group. Begin every alias on a new line.</td>
</tr>
<tr>
<td>Group directory number(s)</td>
<td>Directory number used to identify the group. You can specify multiple directory numbers for a group. Begin every directory number on a new line.</td>
</tr>
<tr>
<td>Maximum group size</td>
<td>Maximum number of members permitted for a group.</td>
</tr>
<tr>
<td>Maximum call queue size</td>
<td>Maximum number of simultaneous ringing calls permitted for the group. You must use a call queue size between 10 to 10000 calls.</td>
</tr>
<tr>
<td>Locale</td>
<td>Locale of the group.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Time zone to which the group belongs.</td>
</tr>
</tbody>
</table>
Call Pickup group modification

You can use any of the following tasks while modifying the Call Pickup group:

- Search for a Call Pickup group.
- Assign the Session Manager for the Call Pickup group.
- Add members to the Call Pickup group.
- Assign a group administrator for the Call Pickup group.

Searching for the Call Pickup group

Procedure

1. From the Provisioning Client menu bar, click Services > Group Services > Call Pickup to access the Call Pickup Service portlet.
2. Click the Search tab.
3. Type the domain name.
4. (Optional) Type the group name or DN.
5. Click Search.

The system displays a list of groups matching the criteria you specified.
You can select a group from the list of search results and modify the group as required.

Assigning the Session Manager for the Call Pickup service group

About this task
The system configures every Call Pickup group as a special user. Every Call Pickup group must have a unique user name and must be assigned to a Session Manager.

Use this procedure to assign a Session Manager for a Call Pickup group.

Procedure

1. Search for the Call Pickup group.
2. On the modify page, click the Session Manager tab.
3. Select a Session Manager profile.
4. Click Save.

Adding members to the Call Pickup group

About this task
Use this procedure to add members to a Call Pickup group.

The system validates the subscriber addition to check whether a Call Pickup service is assigned to the subscriber.
Before you begin

Ensure that you:

- have Services provisioning rights.
- have assigned a Session Manager to the Call Pickup group.

Procedure

1. Search for the Call Pickup group.
2. On the Modify page, click the Modify tab.
3. In the Group Members field, type `username@domain`.

   You can only add users that belong to the domain or subdomain of the domain that owns the Call Pickup group.

   You can add multiple users in the Group Members field, separated by a new line. Add one user in each line.

4. Click Save.

Assigning a Group Administrator for a Call Pickup group

About this task

You can assign an administrator for every Call Pickup group. Administrators can change group settings, and add or remove members.

Procedure

1. Search for the Call Pickup group.
2. On the Modify page, click the Group Administrator tab.
3. In the Group Members field, type `username@domain`.

   Ensure that the user is from the domain that owns the Call Pickup group.

   You can specify multiple Group Administrators, separated by a new line. Add one Group Administrator on every line.

   The Group Administrators included in this list can use their Personal Agent to modify the list of members and group parameters for the Call Pickup group.

4. Click Save.

Call Pickup VSCs

The system supports VSCs with the Call Pickup service.

VSCs can be used to grab or answer ringing calls and to check and change agent status. There are four VSC related for Call Pickup service.
Adding Call Pickup feature translation triggers in a domain

Before you begin
Ensure that you have Service provisioning rights.

Procedure
1. From the Provisioning Client menu bar, click Services > Call Routing > Vertical Service Codes to access the Vertical Service Codes service portlet.
2. On the Feature translation tab, select the domain, and click >>.
3. In the Name field, type a name for the translation record.
4. In the Prefix field, type the DN for the Call Pickup group.
5. In the VSC service field, select the VSC service related to the Call Pickup service.
6. Click Save.
7. Repeat these steps for all Call Pickup VSCs that you want to configure on the domain.

Call Pickup feature translation triggers in a domain job aid

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name to identify the translation record. The name must be unique in a domain and must contain 1–32 characters.</td>
</tr>
<tr>
<td>Prefix</td>
<td>DN for a Call Pickup group. The prefix can contain 2–32 characters. The prefix can begin with *, #, or any number. The remaining characters in the prefix must be numbers.</td>
</tr>
</tbody>
</table>
| VSC service           | • Call_Pickup_Agent_Active: Used to set own CPU agent status to active by dialing VSC code only  
                         • Call_Pickup_Agent_Inactive: Used to set own CPU agent status to inactive by dialing VSC code only  
                         • Call_Pickup_Check_Agent_Status: Used to check own CPU agent status by dialing VSC code only |

Table continues…
Parameters | Description
---|---
• Call_Pickup_for_GroupDN/UserDN: Used to retrieve ringing calls on the group or user. Usage- - By dialing VSC+GroupID/DN for Group and Directed Call Pickup - By dialing VSC+UserDN for Targeted Call Pickup

**Note:**
You must configure treatment causes appropriately to ensure that the VSC CPU works correctly.

**Treatment causes configuration for Call Pickup VSC**

To correct the behavior of CPU VSC you need to configure appropriate treatment causes. Special announcement will be played over Avaya Media Server to indicate whether or not the operation was successful.

<table>
<thead>
<tr>
<th>VSC service</th>
<th>Treatment name/ reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call_Pickup_Agent_Active</td>
<td>• STARCODE_SUCCESS: Used to indicate that user CPU agent status was successfully changed to Active • STARCODE_FAILURE: Used to indicate that some error occurred and CPU agent status was not successfully updated to Active</td>
</tr>
<tr>
<td>Call_Pickup_Agent_Inactive</td>
<td>• STARCODE_SUCCESS: Used to indicate that user CPU agent status was successfully changed to Inactive • STARCODE_FAILURE: Used to indicate that some error occurred and CPU agent status wasn’t successfully updated to Inactive</td>
</tr>
<tr>
<td>Call_Pickup_Check.Agent_Status</td>
<td>• STARCODE_STATUS_ENABLED: Used to indicate that user has Active CPU agent status • STARCODE_STATUS_DISABLED: Used to indicate that user has Inactive CPU agent status</td>
</tr>
<tr>
<td>Call_Pickup_for.GroupDN/UserDN</td>
<td>• CALL_PICKUP_FORBIDDEN: Used to indicate that user cannot perform the call pickup operation. For example, if particular Call Pickup variants are unavailable for user • NO_CALLAVAILABLE_FOR_PICKUP: Used to indicate that user currently has no calls for pickup</td>
</tr>
</tbody>
</table>

Related links
[Treatments service configuration](#) on page 165
Call Return service configuration

About this task

Use the procedures in this section to configure the Call Return service.

• Configuring the Call Return service on page 216
• Assigning the Call Return service to a user on page 217

Configuring the Call Return service

Use this procedure to configure the Call Return service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Origination > Call Return to access the Call Return Service portlet.
2. Configure the parameters in the System Profile tab.
3. Click Save.
Configuring the Call Return service job aid

About this task
This job aid describes the parameters for the System Profile tab in the Call Return Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Call return via VSC</td>
<td>Check the box to enable this service, using the Vertical Service Code (VSC).</td>
</tr>
</tbody>
</table>

Assigning the Call Return service to a user

Use this procedure to assign the Call Return service to a user.

Before you begin
- You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. From the Services tab, click Call Return.
3. On the User Data tab, add a user name in the Select user field.
4. Click >>.
5. From the User system profile list, select a profile.
6. Click Save.
7. Check the Call Return box in User Profile.
8. Click Save.

Call Type Based Screening service configuration

About this task
Use the procedures in this section to configure Call Type Based Screening
- Configuring Call Type Based Screening service on page 218
- Defining the Call Type for a domain on page 218
- Assigning the Call Type Based Screening service to a domain on page 219
- Assigning the Call Type Based Screening service to a user on page 220
Configuring Call Type Based Screening service

Use this procedure to configure the Call Type Based Screening service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Routing > Call Type Based Screening to access the Call Type Based Screening Service portlet.
2. On the System Profile tab, configure the parameters as required.
3. Click Save.

Configuring Call Type Based Screening service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Call Type Based Screening Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Call type based screening via VSC</td>
<td>Check this box to enable the service using the Vertical Service Code (VSC).</td>
</tr>
</tbody>
</table>

Defining the Call Type for a domain

Use this procedure to define the type of call you want to provision for a domain.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click Call Type Based Screening.
3. On the Feature Translation tab, select the domain from the list and click >>.
4. Configure the parameters for this service.
5. Click Save.
## Provisioning Call Type Based Screening service job aid

This job aid describes the parameters for the Feature Translation tab in the Call Type Based Screening Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a meaningful name in the Name field. For example, if you choose International from the list in the Call type name field, then you can type International in the Name field.</td>
</tr>
<tr>
<td>From Digits</td>
<td>This field determines the digit range. For example if you enter From Digit= 32 and To Digit = 35, it means that the translation is defined for digits 32, 33, 34 and 35.</td>
</tr>
<tr>
<td>To Digits</td>
<td>This field determines the digit range. For example if you enter From Digit= 32 and To Digit = 35, it means that the translation is defined for digits 32, 33, 34 and 35.</td>
</tr>
<tr>
<td>Min Digits</td>
<td>This field determines the digit number range. For example, if you enter Min Digits = 5 and Max Digits = 7, then the customer-dialed digits that are between 5 and 7 are looked for determining call types.</td>
</tr>
<tr>
<td>Max Digits</td>
<td>This field determines the digit number range. For example, if you enter Min Digits = 5 and Max Digits = 7, then the customer-dialed digits that are between 5 and 7 are looked for determining call types.</td>
</tr>
<tr>
<td>Call type name</td>
<td>Select the value from the list in the Call type name field. Select from the following options:</td>
</tr>
<tr>
<td></td>
<td>• international</td>
</tr>
<tr>
<td></td>
<td>• long_distance_inter_ratearea</td>
</tr>
<tr>
<td></td>
<td>• local</td>
</tr>
<tr>
<td></td>
<td>• premium</td>
</tr>
<tr>
<td></td>
<td>• long_distance_intra_ratearea</td>
</tr>
</tbody>
</table>

## Assigning the Call Type Based Screening service to a domain

Use this procedure to assign the Call Type Based Screening service to a user.

### Before you begin
- You have Services provisioning rights.

### Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. Select the Services Assignment tab.
3. On the Select a domain list, select a domain and click >>.
4. Click to select the corresponding check box for Call Type Based Screening.
5. Click Save.

Assigning the Call Type Based Screening service to a user

Use this procedure to assign Call Type Based Screening service to a user.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Call Type Based Screening.
3. On the User Data tab, type the name of the user to whom you want to assign this service and click >>.
4. On the User Data tab, configure the parameters as required.
5. Click Save.

Assigning Call Screening to a user job aid

The following job aid describes the parameters for the User Data tab in the Call Type Based Screening Service portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User system profile</td>
<td>Select a profile from the list.</td>
</tr>
<tr>
<td>International</td>
<td>Select the check box to block International call type.</td>
</tr>
<tr>
<td>Long distance inter rate area</td>
<td>Select the check box to block Long distance inter rate area call type.</td>
</tr>
<tr>
<td>Long distance intra rate area</td>
<td>Select the check box to block Long distance intra rate area call type.</td>
</tr>
<tr>
<td>Local</td>
<td>Select the check box to block Local call type.</td>
</tr>
<tr>
<td>Premium</td>
<td>Select the check box to block Premium call type.</td>
</tr>
</tbody>
</table>

Calling Line ID Restriction service configuration

About this task

Use the procedures in this section to configure the Calling Line ID Restriction service.

• Configuring the Calling Line ID Restriction service on page 221
• Assigning the Calling Line ID Restriction service to a domain on page 221
• Assigning the Calling Line ID Restriction service to a user on page 222
Configuring the Calling Line ID Restriction service

Use this procedure to configure the Calling Line ID Restriction service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services, Privacy/SecurityRestriction, Calling Line ID Restriction to access the Calling Line ID Restriction Service portlet.
2. On the System Profile tab, configure the parameters as required.
3. Click Save.

Configuring the Calling Line ID Restriction service job aid

About this task
This job aid describes the parameters for the System Profile tab in the Calling Line ID Restriction Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Calling name/number privacy</td>
<td>Enables a user to see the setting in their Avaya Aura® Application Server 5300 Personal Agent that provides the option to specify whether their name and number appear when they call someone.</td>
</tr>
<tr>
<td>Media privacy (media portal required)</td>
<td>Enable the media privacy capability. This service is available only if you have Media Portal on your system.</td>
</tr>
<tr>
<td>Calling name/number restriction per call via VSC</td>
<td>Dedicated to the Web-based components of the multimedia conversation.</td>
</tr>
<tr>
<td>Calling name/number presentation per call via VSC</td>
<td>Check the box to enable this service using Vertical Service Code (VSC).</td>
</tr>
<tr>
<td>Calling name/number privacy permanent via VSC</td>
<td>Check the box to enable this service using VSC.</td>
</tr>
</tbody>
</table>

Assigning the Calling Line ID Restriction service to a domain

Use this procedure to assign the Calling Line ID Restriction service to a user.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. Select the **Service Assignment** tab.
3. On the **Select a domain** list, select a domain and click >>.
4. Click to select the corresponding check box for **Calling Line ID Restriction**.
5. Click **Save**.

---

### Assigning the Calling Line ID Restriction service to a user

Use this procedure to assign the Calling Line ID Restriction service to a user.

**Before you begin**
- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Calling Line ID Restriction Service** to access the Calling Line ID Restriction Service portlet.
2. On the **User Data** tab, add a user name in the **Select user** field.
3. Click >>.
4. From the **User system profile** list, select a profile.
5. Click **Save**.
6. Select the **Calling name/number privacy** check box.
7. Click **Save**.

---

### Configuring the Client Collaboration service

Use this procedure to configure the Client Collaboration service.

**Note:**

Client Collaboration is not provisioned in Federal Service Package.

**Before you begin**
- You have Services provisioning rights to define and assign services to domains.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Media > Client Collaboration** to access the Client Collaboration Service portlet.
2. On the Client Collaboration Service portlet, configure the parameters on the **System Profile** and **User Data** tabs as required.
3. Click **Save**.
Assigning the Equal Access prefix data for Converged Desktop service

Converged Desktop (CD) is not supported in Application Server 5300.

Core Services Session Manager profile configuration

About this task
This section contains the procedures for configuring and assigning the Core Services Session Manager profile.

- Configuring the Core Services Session Manager profile on page 223
- Assigning the Core Services Session Manager profile to a domain on page 224
- Assigning the Core Services Session Manager profile to a user on page 224

Configuring the Core Services Session Manager profile

About this task
The Core Services Session Manager profile specifies the AS 5300 Session Manager home for a user. Use this procedure to configure the Core Services Session Manager profile.

⚠️ Important:
Provision a SIP Proxy to route calls to an external AS 5300 Session Manager defined in the Core Services Session Manager Service portlet. To provide correlation between SIP proxy and AS 5300 Session Manager, match the SIP proxy short name with the AS 5300 Session Manager alias defined in this procedure. For more information about SIP proxy configuration, see Avaya Aura® Application Server 5300 Configuration, NN42040-500

Procedure

1. From the Provisioning Client menu bar, select User > Core Services Session Manager to access the Core Services Session Manager Service portlet.
2. On the System Profile tab, configure the Profile name, Session Manager, Session Manager alias, and Session Manager URL parameters.
3. Click Save.
Configuring the Core Services AS 5300 Session Manager profile job aid

About this task

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The name of the profile.</td>
</tr>
<tr>
<td>Session Manager</td>
<td>The name of the AS 5300 Session Manager.</td>
</tr>
<tr>
<td>Session Manager alias</td>
<td>Used as a globally-unique alias for the AS 5300 Session Manager for all systems that may need to route to this AS 5300 Session Manager using Subscriber Lookup and Routing. Other systems are provisioned with a Service Node with a name matching this alias to enable calls to be routed to this AS 5300 Session Manager. This alias is pushed to the LDAP server to allow routing calls to multisite users. The alias may be a maximum of six characters in length.</td>
</tr>
<tr>
<td>Session Manager URL</td>
<td>Used by other features as a globally-unique virtual DN for the AS 5300 Session Manager. The field is populated with a numeric string. Other systems requiring a route to the AS 5300 Session Manager as an endpoint are provisioned with translations that include the remote AS 5300 Session Manager URL.</td>
</tr>
</tbody>
</table>

Assigning the Core Services Session Manager profile to a domain

About this task

Use this procedure to assign the Core Services Session Manager profile to a domain.

Procedure

1. From the Provisioning Client menu bar, select User > Core Services Session Manager to access the Core Services Session Manager Service portlet.
2. On the System Profile tab, click the Assign/Remove link in the Domain column of the row containing the Profile name you want to assign.
3. Select a domain in the Available Domains list to which you want to assign the profile and click Copy.
4. Click Save.

Assigning the Core Services Session Manager profile to a user

About this task

Use this procedure to assign the Core Services Session Manager profile to a user.
Important:
When you add an ANI to an ERL, the system automatically adds a new ANI user to the list of users. For example, when you add the 9724449105@multi1.com ANI, the system creates a new user called ani_9724449105@multi1.com.

You must assign the Core Services Session Manager profile to each new ANI user to enable E911 ANI call back.

Procedure
1. From the Provisioning Client menu bar, select User > Core Services Session Manager to access the Core Services Session Manager Service portlet.
2. On the User Data tab, enter a user name in the Select user field and click ».
3. On the User Data tab, from the User's system profile list, select the system profile for the user and click Save.

Configuring Access Gateway Control Function
Application Server 5300 does not support Access Gateway Control Function.

Configuring Colorful Ringback Tones
Application Server 5300 does not support Colorful Ringback Tones / Personal Ringback Tones.

Configuring the Deny All Calls service
Use this procedure to configure the Deny All Calls service.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Restrictions, Deny All Calls to access the Deny All Calls Service portlet.
2. Configure the parameters in the System Profile tab.
3. Click Save.
Configuring the Deny All Calls service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Deny All Calls Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Deny all incoming calls</td>
<td>Allows the administrator or user to block incoming calls.</td>
</tr>
<tr>
<td>Deny all outgoing calls</td>
<td>Allows the administrator or user to bar outgoing calls.</td>
</tr>
<tr>
<td>Deny all incoming calls via VSC</td>
<td>Allows the administrator or user to block incoming calls, using the Vertical Service Code (VSC) option.</td>
</tr>
<tr>
<td>Deny all outgoing calls via VSC</td>
<td>Allows the administrator or user to bar outgoing calls using the VSC option.</td>
</tr>
</tbody>
</table>

Configuring the Direct to Gateway service

Use this procedure to configure the Direct to Gateway service. This procedure allows you to provision destination prefix numbering.

⚠️ Important:

When both a subdomain and a root domain have a prefix provisioned, then the system uses the root domain prefix.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Converged Clients > Direct To Gateway to access the Direct to Gateway Service.
2. In the Direct to Gateway Service portlet, select the DTG Domain tab.
3. In the Select domain field, select the appropriate domain and click >>.
4. In the Direct to Gateway Service portlet, configure the gateway prefix.
5. Click Save.
Configuring the Direct to Gateway service

The Direct to Gateway service job aid

About this task

This job aid describes the parameters on the Direct to Gateway Service portlet DTG Domain tab.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Direct to gateway prefix</td>
<td>Type the prefix for Direct to gateway.</td>
</tr>
<tr>
<td>Call forward prefix</td>
<td>Type the prefix for forwarding a call.</td>
</tr>
<tr>
<td>Call transfer prefix</td>
<td>Type the prefix for transferring a call.</td>
</tr>
<tr>
<td>VOIP origination prefix</td>
<td>Type the prefix for calls of VOIP origin.</td>
</tr>
<tr>
<td>VOIP forward prefix</td>
<td>Type the prefix for forwarding a VOIP call.</td>
</tr>
<tr>
<td>VOIP transfer prefix</td>
<td>Type the prefix for transferring a VOIP call.</td>
</tr>
</tbody>
</table>

Configuring Hot Line service

Use this procedure to configure the Hot Line service.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Origination > Hot Line to access the Hot Line Service portlet.
2. On the User Data tab, in the Select user box, type the name of the user to whom you want to assign this service.
3. Click >>.
4. From the User's system profile list, select the system profile for the user.
5. In the User Profile section, configure the Called URL and Key Label parameters as required.
6. Click Save.

Configuring the Hot Line service user job aid

About this task

This job aid describes the parameters for the User Data tab in the Hot Line Service portlet.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Called URL</td>
<td>This field provides the ability to configure an Avaya IP Deskphone such that a specific hotline number is called when the subscribed user that is registered on the Avaya IP Deskphone goes off hook.</td>
</tr>
<tr>
<td>Key label</td>
<td>This field is commonly configured with the Device Access Restriction service so that when a subscriber is logged on to the Avaya IP Deskphone, the device is both a Hotline and a restricted device.</td>
</tr>
</tbody>
</table>

### Configuring the Device Access Restrictions service

IP Client Manager (IPCM) is not supported in Application Server 5300.

### Configuring routable services information for IM Chat

**About this task**

Use this procedure to configure routable services information for IM Chat.

The IM Chat service allows two or more users (with AS 5300 UC Client or AS 5300 Web Client) to send text messages to a chat room consisting of a single on-screen window.

Within the IM Chat room window, each participant can send an instant message to any or all of the participants in that chat room. In other words, a single participant can send an IM to several participants within the same window. In addition, the IM Chat service allows users to invite other people to join the chat room, to browse available online chat rooms, or to select a specific chat room to join. The user can also join multiple chat rooms simultaneously. In this case, each chat room appears in a separate window.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Conferencing > IM Chatroom** to access the IM Chatroom Service portlet.
2. In the **Select domain** field, select domain to which you want to assign routable services for IM Chatroom.
3. Click `>>`.
4. From the **Select pool** list, select an IM Chatroom pool.
5. Click **Save**.
Configuring Low Bandwidth Link

About this task
Use this procedure to configure the Low Bandwidth Link service on the system.

Procedure
1. From the Provisioning Client menu bar, select Services > Media > Low Bandwidth Link.
2. In the Low Bandwidth Link Service portlet, configure parameters as required.
3. Click Save.

Configuring Low Bandwidth Link job aid

About this task
This job aid describes the parameters that appear on the Low Bandwidth Link tab.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBL Name</td>
<td>Type a descriptive name for the Low Bandwidth Link profile you are creating.</td>
</tr>
<tr>
<td>Zone ID</td>
<td>Type the zone ID for the Low Bandwidth Link. Default: 0</td>
</tr>
</tbody>
</table>

Configuring Media Portal Service

About this task
Use this procedure to configure the Media Portal Service.

Procedure
1. From the Provisioning Client menu bar, select Services > Media > Media Portal to access the Media Portal Service portlet.
2. In the Media Portal Service portlet, in the Group name field, enter a name for the group.
3. Use the Copy, Copy All, Remove, and Remove All buttons to populate the Selected Resources list with the resources you want to include.
4. Use the Copy, Copy All, Remove, and Remove All buttons to populate the Selected Foreign Domains list with the domains you want to include.
5. Click Save.
Configuring Multiple Attendants service

About this task
Avaya Aura® Application Server 5300 does not support the Multiple Attendants service.

Configuring Meet Me Conferencing service

Use this procedure to configure Meet Me Conferencing services.

Before you begin
• You have Services provisioning rights to define and assign services to domains.

Procedure
1. From the Provisioning Client menu bar, select Services > Conferencing > Meet-Me Conferencing to access the Meet Me Conferencing Service portlet.
2. From the Meet Me Conferencing Service portlet, configure the parameters on the Domain properties, Conference Pool, Service Alias, Lookup Users, and Active Conferences tabs.
3. Click Save.

Meet Me Conferencing Service: Domain Properties tab job aid

This job aid describes the parameters for the Domain Properties tab in the Meet Me Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Chair ends conference</td>
<td>Enables the conference to end if the chairperson hangs up the call.</td>
</tr>
<tr>
<td>Entry/Exit indication</td>
<td>Indicates which conference participant entered or existed the conference.</td>
</tr>
<tr>
<td>IM enabled</td>
<td>Enables participants to exchange instant messages during the conference.</td>
</tr>
<tr>
<td>Operator user ID</td>
<td>Specifies user ID of the operator.</td>
</tr>
</tbody>
</table>
Meet Me Conferencing Service: Conference Pool parameters job aid

This job aid describes the parameters for the Conference Pool tab in the Meet Me Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Current pool</td>
<td>Shows the currently selected pool if previously assigned.</td>
</tr>
<tr>
<td>Select pool</td>
<td>Enables you to select another pool from the list.</td>
</tr>
</tbody>
</table>

Meet Me Conferencing Service: Service Alias parameters job aid

This job aid describes the parameters for the Service Alias tab in the Meet Me Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Alias</td>
<td>Type an alias for this service.</td>
</tr>
<tr>
<td>Select pool</td>
<td>Enables you to selected another pool from the list.</td>
</tr>
<tr>
<td>Locale</td>
<td>Select the language from the list.</td>
</tr>
</tbody>
</table>

Meet Me Conferencing Service: PSI Data parameters job aid

This job aid describes the parameters for the PSI Data tab in the Meet Me Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Name</td>
<td>Type a name for this distribution list.</td>
</tr>
<tr>
<td>Distributor</td>
<td>Select the distributing AS 5300 Session Manager from the list.</td>
</tr>
<tr>
<td>Distribution servers</td>
<td>Select the distribution servers from the list.</td>
</tr>
</tbody>
</table>
Meet Me Conferencing Service: User Data parameters job aid

This job aid describes the parameters for the User Data tab in the Meet Me Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Chair ends conference</td>
<td>Enables the chairperson to end the conference.</td>
</tr>
<tr>
<td>Access code</td>
<td>Enter a number (between 4- and 10-digits long) that a conference participant must use to enter the conference. The Access Code text box field is automatically populated with a 7- to 10-digit valid number when adding a new user. The system searches through Business phone, Username, and Aliases parameters in the respective order before validating a new access code.</td>
</tr>
<tr>
<td>Audio recording email ID</td>
<td>Type email ID for audio recording, for example, <a href="mailto:user2@abc.com">user2@abc.com</a>.</td>
</tr>
<tr>
<td>Send instant messages</td>
<td>Enables participants to exchange instant messages during the conference.</td>
</tr>
<tr>
<td>Allow fast start</td>
<td>Enables participants to enter the bridge without the chairperson.</td>
</tr>
<tr>
<td>Allow audio emoticons</td>
<td>Enables participants to use audio emoticons during the conference.</td>
</tr>
<tr>
<td>Entry/Exit announcements</td>
<td>Generates a tone when participants join or leave the bridge. Select a tone from the list.</td>
</tr>
<tr>
<td>Change Chair PIN</td>
<td>Enables the chairperson to create a new pin. In the Chairperson PIN text box, enter a number (between 4- and 10-digits long) that the chairperson uses for identification.</td>
</tr>
<tr>
<td>Maximum number of participants</td>
<td>Specifies the maximum number of participants allowed to join the conference.</td>
</tr>
<tr>
<td>Premium conferencing enabled</td>
<td>Enables premium conferencing capabilities.</td>
</tr>
<tr>
<td>Video conferencing enabled</td>
<td>Enables video conferencing.</td>
</tr>
<tr>
<td>Web collaboration enabled</td>
<td>Not supported.</td>
</tr>
<tr>
<td>Audio recording enabled</td>
<td>Enables audio recording.</td>
</tr>
</tbody>
</table>

Meet Me Conferencing Service: Lookup Users job aid

This job aid describes the parameters for the Lookup Users tab in the Meet Me Conferencing Service portlet.
### Meet Me Conferencing Service: Active Conferences job aid

This job aid describes the parameters for the **Active Conferences** tab in the Meet Me Conferencing Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>Select the domain from the list for configuring or modifying the parameters.</td>
</tr>
<tr>
<td>Search by</td>
<td>Select <strong>Access Code</strong> or <strong>Domain Name</strong> from the list to search an active conference.</td>
</tr>
<tr>
<td>Search</td>
<td>Click <strong>Search</strong> to find an ongoing conference.</td>
</tr>
</tbody>
</table>

### Configuring routable services information to a Mobility Gateway

**About this task**

Use this procedure to configure access to the Mobility Gateway logical entity in the domain where service is needed.

**Procedure**

1. From the Provisioning Client menu bar, select **Translations > Mobility Gateway** to access the Mobility Gateway Service portlet.
2. In the **Select domain** field, select a domain to which you want to add Mobility Gateway service and click «.».
3. In the **Select pool** field, select the name of the pool you want to assign.
4. Click **Save**.

### Defining the match criteria for the advanced address book

Use this procedure to define the match criteria for the advanced address book.
Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Client Interface > Advanced Address Book to access the Advanced Address Book Service portlet.
2. From the Advanced Address Book Service portlet, select the Match Criteria Number tab.
3. In the Match Criteria Number box, type the value for the match criteria.
4. Click Save.

E911 Options service configuration

About this task

Use the procedures in this section to configure E911 Options service.

You require a license key to enable this feature. Use the AS 5300 Element Manager Console to enable the E911 feature. For more information, see Avaya Aura® Application Server 5300 Configuration, NN42040-500.

- Adding an emergency number on page 234
- Configuring the E911 service on page 235
- Assigning the E911 system parameter on page 235
- Assigning the Emergency Calling Service on page 236
- Creating or modifying an enterprise ERL on page 237
- Creating or modifying a residential ERL on page 238
- Deleting an ERL on page 239
- Capturing ERL additions, deletions, and modifications on page 240
- Assigning the E911 Options service to a user on page 240

Adding an emergency number

Add an emergency number to provide support for Enhanced 911 emergency calls.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > E911 Options.
2. On the Emergency Number tab, type an emergency number in the Emergency number field.
3. In the **Emergency alias** box, type one or more emergency aliases.
4. Click **Add**.
5. To delete the alias, select the alias from the text box and click **Delete**.
6. Click **Save**.

---

### Configuring the E911 service

Use this procedure to configure the E911 service.

**Before you begin**

- You have Services provisioning rights to define and assign services to domains.
- You require a license key to enable this feature.

You can enable this feature using the AS 5300 Element Manager Console. For more information, see *Avaya Aura® Application Server 5300 Configuration, NN42040-500*. If this feature is not enabled, you cannot assign E911 Options to a domain, and you receive the following error message:

The parameter Public IP Address of the service E911 Options is disabled in the license key. Please deselect the parameter, or try again with a valid license key.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > E911 Options** to access the E911 Options Service portlet.
2. On the **System Profile** tab, configure the parameters as required.
3. Click **Save**.

### Configuring the E911 Options service job aid

**About this task**

This job aid describes the parameters for the **System Profile** tab in the E911 Options Service portlet.

**Table 17: Regulatory parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Public IP address</td>
<td>Enables the public IP address of the user in case of an emergency call.</td>
</tr>
</tbody>
</table>

### Assigning the E911 system parameter

Use this procedure to assign E911 system parameter.
Before you begin

- You have Services provisioning rights to define and assign services to domains.

Procedure

1. From the Provisioning Client menu bar, select **Services > E911 Options** to access the E911 Options Service portlet.
2. Select the **System Data** tab.
3. From the Parm name list, choose **E911** and click `>>`.
4. Select the check box to enable **E911 number or alias exact match**.
5. Click **Save**.

Assigning the Emergency Calling Service

Use this procedure to assign Emergency Calling Service (ECS) to a domain.

The Regulatory parameter is assigned so that if a user calls an E911 operator during an emergency, the user cannot put the operator on hold.

Before you begin

- Ensure that the E911 parameter is already assigned to the domain.

Procedure

1. From the Provisioning Client menu bar, select **Services > E911 Options** to access the E911 Options Service portlet.
2. On the **Domain Data** tab, select the domain from the list and click `>>`.
3. Configure the parameters for this service.
4. Click **Save**.

Assigning the Emergency Calling Service job aid

This job aid describes the parameters for the **Domain Data** tab in the E911 Options Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Routing server to E911public IP</td>
<td>Select the server from the list.</td>
</tr>
<tr>
<td>E911 originator hold</td>
<td>Select the check box for this regulatory parameter.</td>
</tr>
</tbody>
</table>

**Note:**

For Avaya 1100 IP series phones (for example, 1140E sets) E911 originator hold regulatory parameter is not applicable. You cannot place an emergency call on hold, irrespective of the status of this regulatory parameter.
Creating or modifying an enterprise ERL

About this task

You can create or modify an enterprise ERL for an existing location on the system.

Procedure

1. From the Provisioning Client menu bar, select Services > E911 Options to access the E911 Options Service portlet.

2. On the E911 Options Service portlet, click the ERL tab.

3. Select the domain and click >>.

4. From the Locations list, select the location for which you want to create or modify an ERL.

5. Configure the Residential ERL, Service node, Profile override, ANI registration time (hours), and OSN instant message SIP address parameters as required.

6. In the ANI box, type a new automatic number identification (ANI) and then click Add.

⚠️ Important:

At least one configured ANI must exist for the ERL. Otherwise, when you try to save your changes, the following error message appears: Unable to create Emergency Response Location. At least 1 ANI is required.

The system adds all new ANIs to the root domain. To add an ANI to a subdomain, use the ANI@subdomain format.

⚠️ Important:

If E911 Manager is part of the deployment, it is very important to synchronize ANIs between E911 Manager and Application Server 5300. Contact the E911 Manager administrator and provide the current configuration of ERLs and ANIs. See Capturing ERL additions deletions and modifications on page 240 to check the configuration ANI with E911 Manager. To be in the synchronized state, go through this procedure when changes in Locations, ERLs or ANIs are performed.

7. (Optional) To delete an existing ANI, from the list box, select the ANI to delete and click Delete.

8. Click Save.

Creating an enterprise ERL job aid

About this task

This job aid describes the parameters for the E911 Options Service portlet.
### Parameter Description

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential ERL</td>
<td>Specifies whether an ERL is residential. Clear the check box for enterprise and carrier-hosted configurations.</td>
</tr>
<tr>
<td>Service node</td>
<td>The logical entity that terminates the Public Safety Answering Point (PSAP) for 911 services. The list contains all logical entities for the domain.</td>
</tr>
<tr>
<td>Profile override</td>
<td>Associates a CS 2000 profile to an ERL location. This simplified routing does not use translation triggers to override the profile. The list contains all CS 2000 profiles available for the domain and subdomains, as well as the default None - Use Orig option.</td>
</tr>
<tr>
<td>ANI registration time (hours)</td>
<td>Specifies the length of time an enterprise callback number remains bound to the originating E911 subscriber. (Not available if you select Residential ERL.)</td>
</tr>
<tr>
<td>OSN instant message SIP address</td>
<td>Optional. Specifies the SIP address to send an OSN instant message to when a user with the current ERL selected as their location makes an emergency call. (Not available if you select Residential ERL.)</td>
</tr>
</tbody>
</table>

### Creating or modifying a residential ERL

**About this task**

You can create or modify a residential ERL for an existing location on the system.

**Procedure**

1. From the Provisioning Client menu bar, select Services > E911 Options to access the E911 Options Service portlet.
2. On the E911 Options Service portlet, select the ERL tab.
3. Click an existing location name to create or modify an ERL for that location.
4. Configure the Residential ERL, Service Node, and Profile Override parameters as required.
5. Click Save.

### Creating a residential ERL job aid

**About this task**

This job aid describes the parameters for the E911 Options Service portlet, after you select Residential ERL.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Residential ERL</td>
<td>Specifies whether an ERL is residential. Clear the check box for enterprise and carrier-hosted configurations.</td>
</tr>
</tbody>
</table>
### Parameter Table

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service node</td>
<td>The logical entity that terminates the Public Safety Answering Point (PSAP) for 911 services. The list contains all logical entities for the domain.</td>
</tr>
<tr>
<td>Profile override</td>
<td>Associates a CS 2000 profile to an ERL location. This simplified routing does not use translation triggers to override the profile. The list contains all CS 2000 profiles available for the domain and subdomains, as well as the default None - Use Orig option.</td>
</tr>
</tbody>
</table>

### Deleting an ERL

You can delete an enterprise Emergency Response Location (ERL) from the system.

**Before you begin**

- You must have system administrator rights to delete an enterprise ERL.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > E911 Options** to access the E911 Options Service portlet.
2. On the **E911 Options Service** portlet, select the **ERL** tab.
3. Select the domain and click `>>`.
4. From the **Locations** list, choose the location for which you want to delete the ERL.

   **Caution:**
   
   If you do not have system privileges to delete an ERL, the **Delete ERL** button does not appear.
5. Verify that this is the ERL you want to delete.
6. Click **Delete**.
7. To continue with the delete operation, type your password in the confirmation window and click **Confirm**.

**Job Aid: Guidelines to deleting an ERL**

The following points apply when you delete an ERL.

- Deleting an ERL does not delete the location. Locations must be deleted from the Location Management provisioning page in the Location Services, Locations window.
- Deleting an ERL does not remove the ERL or Automatic Number Identification (ANI) from the ERL and ANI database tables immediately. Instead, a time stamp of the current time plus two days (twice the longest configurable client reregistration interval) is written to the database tables DEPRECATED field. This is required because users are not forced to select a new location immediately after their currently selected location is deleted. The user is prompted to
select a new location only after the latest location list is downloaded, which occurs once the reregistration interval expires.

- A deleted ERL no longer appears on provisioning pages and is treated as if it was deleted.
- From a call-processing perspective, the deleted ERL details are accessible for two days, in case a user with a deleted ERL makes an emergency call.
- A process runs once every 24 hours to remove location and ERL database entries that have expired DEPRECATED field values.

**Note:**

If E911 Manager is part of the deployment, contact the E911 Manager administrator to synchronize the list of ERLs and ANIs after delete operations. See [Capturing ERL additions deletions and modifications](#) on page 240 to check ANIs configuration with E911 Manager.

---

### Capturing ERL additions, deletions, and modifications

**About this task**

Use this procedure to capture ERL additions, deletions, and modifications to display and print a list of currently provisioned ERLs.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > E911 Options** to access the E911 Options Service portlet.
2. On the **E911 Options Service** portlet, select the **ERL** tab.
3. Select the domain, and click `>>`.
4. Click **Get Printable ERL List**.
5. From the window, print the list of currently provisioned ERLs to include in a letter to the PSAP for ALI database update purposes.
6. Close the window and return to the Provisioning Client.

**Note:**

If E911 Manager is a part of deployment, there is no need to send a letter to the PSAP with a request about update records. E911 Manager performs automatic synchronization with the ALI database. Contact the E911 Manager administrator to ensure that it is properly configured.

---

### Assigning the E911 Options service to a user

**About this task**

Use this procedure to assign the E911 Options service to a user.
Procedure
1. From the Provisioning Client menu bar, select Services > E911 Options to access the E911 Options Service portlet.
2. On the User Data tab, type the name of the user you to whom you want to assign this service.
3. Click >>.
4. From the User system profile list, select a profile.
5. Click Save.

Malicious Call Trace service configuration

About this task
Use the procedures in this section to configure Malicious Call Trace (MCT) service.

• Adding Malicious Call Trace translation triggers in a domain on page 241
• Assigning domain data for the Malicious Call Trace service on page 242
• Assigning Malicious Call Trace service to a user on page 243

Adding Malicious Call Trace translation triggers in a domain

Use this procedure to add new Malicious Call Trace (MCT) translation triggers in a domain.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Routing > Vertical Service Codes to access the Vertical Service Codes Service portlet.
2. On the Feature Translation tab, select the domain from the list and click >>
3. On the Feature Translation tab, in the Name box, type a name for the translation record.
4. In the Prefix box, type the DN for Malicious Call Trace.
5. From the VSC service list, select Malicious Call Trace.
6. Click Save.
Adding Malicious Call Trace translation triggers in a domain job aid

About this task

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A meaningful name to identify the translation record. The name must be unique in a domain and contain 1 to 32 characters.</td>
</tr>
<tr>
<td>Prefix</td>
<td>The Malicious Call Trace DN. The DN can be 2 to 32 characters long. It can begin with *, # or any digit, but must have digits for the remainder of the DN.</td>
</tr>
<tr>
<td>VSC Service</td>
<td>Select Malicious_Call_Trace for Malicious Call Trace DN.</td>
</tr>
</tbody>
</table>

Assigning domain data for the Malicious Call Trace service

Use this procedure to assign Malicious Call Trace service domain data.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Malicious Call Trace to access the Malicious Call Trace Service portlet.
2. On the Domain Data tab, select the domain from the list and click >>.
3. Configure the parameters for this service.
4. Click Save.

Assigning domain data for the Malicious Call Trace service job aid

The following job aid describes the parameters for the Domain Data tab in the Malicious Call Trace Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Success announcement</td>
<td>Select a file from the list.</td>
</tr>
<tr>
<td>Failure announcement</td>
<td>Select a file from the list.</td>
</tr>
<tr>
<td>Malicious call trace service components</td>
<td>Select the check box to enable automatic call tracing</td>
</tr>
<tr>
<td>Enable automatic call tracing</td>
<td>Select the check box to enable mid-call tracing</td>
</tr>
<tr>
<td>Enable after-call tracing</td>
<td>Select the check box to enable after-call tracing</td>
</tr>
</tbody>
</table>
Assigning Malicious Call Trace service to a user

Use this procedure to assign Malicious Call Trace service to a user.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Malicious Call Trace.
3. On the Configure MCT tab, type the name of the user to whom you want to assign this service and click >>.
4. Configure the Enable automatic call tracing, Enable terminating call tracing, and Caller URI parameters.
5. Click Save.

Assigning Malicious Call Trace service to a user job aid

This job aid describes the parameters for the Configure MCT tab in the Malicious Call Trace Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic call tracing</td>
<td>Enables call tracing automatically.</td>
</tr>
<tr>
<td>Enable terminating call tracing</td>
<td>Enables terminating call tracing.</td>
</tr>
<tr>
<td>Caller URI</td>
<td>Type a valid SIP address of a user (for example, user@domain)</td>
</tr>
</tbody>
</table>

Mobile Extension service configuration

About this task

Application Server 5300 does not support Mobile Extension service.

MLPP service configuration

Use the procedures in this section to configure multilevel precedence and preemption (MLPP) to ensure that calls complete based on level of precedence—preempting calls with lower precedence if necessary. The system diverts precedence calls that are not answered after a specified time to a designated Diversion Destination.
User services management procedures

The levels of precedence from lowest to highest are: ROUTINE, PRIORITY, IMMEDIATE, FLASH, and FLASH-OVERRIDE.

⚠️ Important:

When the system cannot deliver a diverted call, the message BLOCKED_PRECEDENCE appears on the caller’s display, and a recorded message informs the caller that the call was blocked.

Prerequisites

- You have Telephony Routes privileges.

MLPP configuration procedures

About this task

This task flow shows the sequence of procedures you perform to configure MLPP.
Figure 23: MLPP Configuration

Navigation

- Creating custom network domains on page 246
- Deleting custom network domains on page 247
- Creating an MLPP namespace on page 247
- Configuring MLPP feature translation on page 248
- Configuring DSCP marking for the MLPP service on page 249
Creating custom network domains

Use this procedure to create custom network domains. You can add a maximum of five custom network domains.

🌟 Note:
Creating custom network domains is optional. Add a new network domain only if you are unable to use the system-defined DSN, UC, or CUC network domains.

Before you begin
• You have the MLPP Management right.

Procedure
1. From the Provisioning Client menu bar, select Services > Privacy/Security, > Multi-Level Precedence and Preemption to access the Multi-Level Precedence and Preemption Service portlet.
2. In the Multi-Level Precedence and Preemption Service portlet, select the Custom network domains tab.
3. In the Domain Name box, type a name for the new network domain.
4. Click Save.

Creating custom network domains job aid
This job aid describes the parameters for the Custom network domains tab in the Multilevel Precedence and Preemption Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain Name</td>
<td>This text field specifies a unique name for the custom network domain. You can specify a maximum of 10 alphanumeric characters for the network domain name. You cannot use the following names: UC, CUC, DSN, DRSN, ETS, or EMRG.</td>
</tr>
</tbody>
</table>
Deleting custom network domains

Use this procedure to delete custom network domains.

**Before you begin**

- You have the MLPP Management right.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Multi-Level Precedence and Preemption** to access the Multi-Level Precedence and Preemption Service portlet.
2. In the Multi-Level Precedence and Preemption Service portlet, select the **Custom network domains** tab.
   
   The custom network domains that are already configured are listed in a table.
3. Click **Delete** next to the custom network domain you want to delete.
4. In the confirmation window, type your administration password and click **Confirm**.

Creating an MLPP namespace

To configure multilevel precedence and preemption (MLPP), you must first create an MLPP namespace. Use this procedure to create an MLPP namespace.

**Before you begin**

- You have the MLPP Management right.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Multi-Level Precedence and Preemption** to access the Multi-Level Precedence and Preemption Service portlet.
2. In the Multi-Level Precedence and Preemption Service portlet, select the **Namespace** tab.
3. In the **Namespace name** box, type a name for the namespace.
4. From the **Network domain** list, select a network domain.
5. In the **Namespace name** box, type the precedence domain.
6. Click **Save**.

Creating an MLPP namespace job aid

**About this task**

This job aid describes the parameters for the **Namespace** tab in the Multilevel Precedence and Preemption Service portlet.
## Configuring MLPP feature translation

Use this procedure to configure nine digit or twelve digit feature translation for MLPP.

### Note:

If you configure two or more translations in the same domain with identical To, From, Min, or Max Digits parameter values, the system uses the last translation added. Avaya does not recommend this configuration.

### Before you begin

- You have the MLPP Management right.

### Procedure

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Multi-Level Precedence and Preemption** to access the Multi-Level Precedence and Preemption Service portlet.

2. In the Multi-Level Precedence and Preemption Service portlet, select the **Feature Translation** tab.

3. From the **Select domain** list, select a domain and click `>>`.

4. On the **Feature Translation** tab, enter values for **Name**, **From digits**, **To digits**, **Min digits** and **Max digits**.

5. Select the **Remove digits** check box, if you want to remove the MLPP precedence prefix digits.

6. In the **Network domain** field, click the network domain that matches the network domain configured in the **Namespace** tab.
7. Click **Save**.

**Example**

To dial a seven digit number 778-1234 using MLPP FLASH precedence prefix, dial 91 followed by the user’s number (917781234). To dial a ten digit number 972-778-1234 using MLPP Flash precedence prefix, dial 91 followed by the user’s number (919727781234).

### Configuring MLPP feature translation job aid

#### About this task

This job aid describes the parameters for the **Feature Translation** tab in the Multi-Level Precedence and Preemption Service portlet.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a meaningful name that specifies the translation record. The name must be 1 to 32 characters in length.</td>
</tr>
<tr>
<td>From digits</td>
<td>Enter the minimum digit for MLPP precedence prefix. Minimum value for this field is 90.</td>
</tr>
<tr>
<td>To digits</td>
<td>Enter the maximum digit for MLPP precedence prefix. Minimum value for this field is 94.</td>
</tr>
<tr>
<td>Min digits</td>
<td>Enter the minimum number of digits for a number (including MLPP prefix).</td>
</tr>
<tr>
<td>Max digits</td>
<td>Enter the maximum number of digits for a number (including MLPP prefix).</td>
</tr>
<tr>
<td>Remove digits</td>
<td>Select this check box to remove the MLPP precedence prefix digits and clear this check box to retain the MLPP precedence prefix digits.</td>
</tr>
<tr>
<td>Network domain</td>
<td>Select the network domain that matches the network domain configured in <strong>Namespace</strong> tab.</td>
</tr>
</tbody>
</table>

### Configuring DSCP marking for the MLPP service

Configure the Differentiated Services Code Point (DSCP) marking parameters to prioritize audio and video according to the following Multi-Level Precedence and Preemption (MLPP) precedence levels:

- Routine
- Priority
- Immediate
- Flash
- Flash Override

#### Before you begin

- You have Services provisioning rights.
Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Multi-Level Precedence and Preemption Service to access the Multi-Level Precedence and Preemption Service portlet.
2. Click the DSCP Marking tab.
3. In the Name box, type a name for the DSCP configuration.
4. From the Media type, select audio or video.
5. In the Routine, Priority, Immediate, Flash, and Flash override boxes, type the value for each precedence level.
6. Click Save.

Configuring DSCP marking for the MLPP service job aid

About this task

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a meaningful name to identify the DSCP configuration. The name must be unique in a domain and contain 1 to 32 characters.</td>
</tr>
<tr>
<td>Media type</td>
<td>Select the type of media traffic: audio or video.</td>
</tr>
<tr>
<td>Routine</td>
<td>Type a value between 0 and 63 for the Routine precedence level.</td>
</tr>
<tr>
<td>Priority</td>
<td>Type a value between 0 and 63 for the Priority precedence level.</td>
</tr>
<tr>
<td>Immediate</td>
<td>Type a value between 0 and 63 for the Immediate precedence level.</td>
</tr>
<tr>
<td>Flash</td>
<td>Type a value between 0 and 63 for the Flash precedence level.</td>
</tr>
<tr>
<td>Flash override</td>
<td>Type a value between 0 and 63 for the Flash override precedence level.</td>
</tr>
</tbody>
</table>

Creating an MLPP profile

Create a Multilevel Precedence and Preemption (MLPP) profile to assign to root domains, and subsequently to the users of the root domains and their subdomains. You can assign only one MLPP profile to a user.

Before you begin

- You have the MLPP Management right.
Procedure

1. From the Provisioning Client menu bar, select **Services > Privacy/Security > Multi-Level Precedence and Preemption** to access the Multi-Level Precedence and Preemption Service portlet.
2. In the Multi-Level Precedence and Preemption Service portlet, select the **System Profile** tab.
3. In the **Profile name** box, type a profile name.
4. From the **Namespace** list, select a namespace name.
5. From the **Maximum priority** list, select a priority.
6. In the **Diversion destination** box, type the diversion destination.
7. From the **Audio DSCP Name** list, select a DSCP marking profile for audio.
8. From the **Video DSCP Name** list, select a DSCP marking profile for video.
9. Click **Save**.

Creating an MLPP profile job aid

**About this task**

This job aid describes the parameters for the **System Profile** tab in the Multi-Level Precedence and Preemption Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile Name</td>
<td>Enter a name for the new MLPP profile. The name can be a maximum of 30 characters and can include alphanumeric as well as underscore (_), dash (-) and dot (.) characters.</td>
</tr>
<tr>
<td>Namespace Name</td>
<td>From the list, select a namespace.</td>
</tr>
<tr>
<td>Maximum Priority</td>
<td>From the list, select the highest priority for calls.</td>
</tr>
<tr>
<td>Diversion Destination</td>
<td>Enter a destination, such as the Diversion Directory Number (DN), with a maximum of 128 characters (SIP URI or another destination) for unanswered calls. Note: Ensure that users do not specify themselves as a Diversion Destination in their MLPP profile.</td>
</tr>
<tr>
<td>Audio DSCP Name</td>
<td>Choose the DSCP marking profile to use for Audio. The audio DSCP profile defines DSCP categories, values, marking states, and IP Tables rules for audio.</td>
</tr>
<tr>
<td>Video DSCP Name</td>
<td>Choose the DSCP marking profile to use for video. The video DSCP profile defines DSCP categories, values, marking states, and IP Tables rules for video.</td>
</tr>
</tbody>
</table>

Assigning an MLPP profile to a domain

Assign an Multilevel Precedence and Preemption (MLPP) profile to a domain so you can assign it to the domain users and subdomain users.
Before you begin

• You have the MLPP Management right.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Service Profiles to access the User Services portlet.
2. In the User Services portlet, select the Services tab.
3. In the Services list, select Multi-Level Precedence and Preemption.
4. In the Multi-Level Precedence and Preemption portlet, select the System Profile tab.
5. In the list of profiles, locate the row containing the profile you want to assign. Click Assign/Remove in the Domain column of the row.
6. Select the System Profile tab.
7. In the Available Domains list, select the domain to which you want to assign the profile.
8. Click Copy.
9. Click Save.

Assigning the MLPP service to a domain

Use this procedure to assign the MLPP service to a domain.

Before you begin

• You have the MLPP Management right.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. In the User Services portlet, select the Service Assignment tab.
3. From the Select domain list, select a domain and click >> .
4. In the services list, select the check box located next to Multi-Level Precedence and Preemption.
5. Click Save.

Configuring a global diversion destination

You can configure a global diversion DN in addition to the diversion destination that you configure for MLPP profiles. The system uses the global diversion destination when a profile is not assigned to the called party and diversion must occur.
Before you begin

- You have the MLPP Management right.

Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Multi-Level Precedence and Preemption to access the Multi-Level Precedence and Preemption portlet.
2. In the Multi-Level Precedence and Preemption portlet, select the Domain Data tab.
3. In the Select domain field, select a domain from the list and click >>.
4. In the Multi-Level Precedence and Preemption Service portlet, enter a valid destination, such as SIP URI, user, number, or alias in the Default diversion destination field.
   The Diversion Destination is an alphanumeric string with a maximum length of 128 characters.
5. Click Save.

Configuring MLPP domain data

Use this procedure to configure the domain data for MLPP.

Before you begin

- You have the MLPP Management right.

Procedure

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Multi-Level Precedence and Preemption to access the Multi-Level Precedence and Preemption Service portlet.
2. In the Multi-Level Precedence and Preemption Service portlet, select the Domain Data tab.
3. From the Select domain list, select a domain and click >>
4. In the Default Diversion Destination field, enter the default destination number for MLPP precedence calls that are diverted.
5. In the Namespace list, select the namespace that matches the namespace defined in Namespace tab.
6. Select the Normalization check box to normalize the precedence domain to default value 000000 or to value the set in Namespace tab, if precedence domain is missing in the signal.
7. Click Save.

Configuring MLPP domain data job aid

About this task

This job aid describes the parameters for the Domain Data tab in the Multi-Level Precedence and Preemption Service portlet.
User services management procedures

### Data Description

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default diversion destination</td>
<td>Enter the number of the attendant who will answer the MLPP precedence calls that are diverted.</td>
</tr>
<tr>
<td>Namespace</td>
<td>Select the namespace that matches the namespace defined in Namespace tab.</td>
</tr>
<tr>
<td>Normalization</td>
<td>Select this check box to normalize the precedence domain to default value 000000 or to the value set in Namespace tab, if precedence domain is missing in the signal.</td>
</tr>
</tbody>
</table>

### Assigning an MLPP profile to a user

All users must be Multi-Level Precedence and Preemption (MLPP) subscribers. You can assign only one MLPP profile to a user.

**Before you begin**

- You have the MLPP Management right.

**Procedure**

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Multi-Level Precedence and Preemption to access the Multi-Level Precedence and Preemption portlet.
2. In the Multi-Level Precedence and Preemption portlet, select the User Data tab.
3. In the Select user field, enter the name of the user and click >>.
4. In the User system profile field, select a profile from the list.
5. Click Save.

### Modifying network domain of an existing MLPP namespace

Use this procedure to modify the network domain of an existing MLPP namespace.

**Note:**

For MLPP calls to work properly, all subscriber endpoints and gateways should also be modified to match the new Network domain configured in this section.

**Before you begin**

- You have the MLPP Management right.
- You have already created an MLPP namespace, System Profiles entries, Feature Translation entries, and assigned namespace to a domain under Domain Data.

**Procedure**

1. From the Provisioning Client menu bar, select Services > Privacy/Security > Multi-Level Precedence and Preemption to access the Multi-Level Precedence and Preemption Service portlet.
2. In the Multi-Level Precedence and Preemption Service portlet, select the Namespace tab.
   The namespace names that are already added are listed.
3. Click to select the namespace you want to modify.
4. From the Network domain list, select the new network domain that you want to configure.
5. Click Save.
   The row displays the new network domain that you configured.
6. Select the System Profile tab from MLPP portlet.
   The profile names that are already added are listed.
7. Select each Profile Name one at a time and click Save.
8. Select the Feature Translation tab from MLPP portlet.
9. Select each Name entry listed one at a time.
10. From Network domain list, select the new network domain that you want to configure.
11. Click Save.
    The row displays the new network domain that you configured.
12. Repeat steps 9 on page 255 through 11 on page 255 for remaining Feature Translation entries.
13. Select the Domain Data tab from MLPP portlet.
14. In the Select domain field, select the domain from the list that will use the new network domain and click >>
15. Click Save to save the domain data.
16. Repeat steps 14 on page 255 and 15 on page 255 for remaining domains that will use the new network domain.

Multiple Call Restriction service configuration

About this task
Use the procedures in this section to configure Multiple Call Restriction service.
- Defining Multiple Call Restriction on page 255
- Assigning Multiple Call Restriction service to a domain on page 256

Defining Multiple Call Restriction
Use this procedure to define the Multiple Call Restriction option to configure the maximum number of simultaneous calls allowed.
Multiple Call Restriction defines whether the multiple call restriction should be enforced on the user or not. If enabled, the number of simultaneous calls that a user is allowed is defined. This is the number of calls that the user can answer/hold (minimum is 1, maximum is 20, and default is 10).

**Before you begin**
- You have Services provisioning rights.

**Procedure**
1. From the Provisioning Client menu bar, select Services > Call Restrictions > Multiple Call Restriction to access the Multiple Call Restriction Service portlet.
2. In the Multiple Call Restriction Service portlet, select the System Profile tab.
3. In the Profile name box, type a name for the profile.
4. In the Number of simultaneous calls field, select the number of simultaneous calls allowed.
5. Click Save.

---

**Assigning Multiple Call Restriction service to a domain**

Use this procedure to configure Direct to Gateway, which determines whether calls must be directed to a predefined gateway.

**Before you begin**
- You have Services provisioning rights.

**Procedure**
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. In the User Services portlet, select the Service Assignment tab.
3. In the Select domain field, select the appropriate domain and click >>.
4. In the User Services portlet, select the Multiple Call Restriction check box.
5. Click Save.

---

**Multiple Register service configuration**

**About this task**
Use the procedures in this section to configure Multiple Register service.

Assigning this service to a user performs the following:
- Enforces the user to register with the proxy before any calls can be made.
• Controls the maximum number of logins allowed.

★ Note:
You can make calls without registering to the proxy, even if this service is not assigned to you. But to receive you must register to the proxy.

• Configuring the Multiple Register service on page 257
• Assigning the Multiple Register service to a domain on page 257
• Assigning the Multiple Register service to a user on page 258

Configuring the Multiple Register service
Use this procedure to configure the Multiple Register service.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Restrictions > Multiple Register to access the Multiple Register Service portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.

Configuring the Multiple Register service job aid
About this task
This job aid describes the parameters for the System Profile tab in the Multiple Register Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Maximum number of logins allowed</td>
<td>This field enables a user to set the maximum number of logons allowed before the user is blocked from registering for a specified time.</td>
</tr>
</tbody>
</table>

Assigning the Multiple Register service to a domain
Use this procedure to configure the Multiple Register service.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
Assigning the Multiple Register service to a user

Use this procedure to configure the Multiple Register service.

**Before you begin**
- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Assign Services** to access the User Services portlet.
2. On the **Services** tab, click **Multiple Register**.
3. On the **User Data** tab, in the **Select user** box, type a user name.
4. Click `>>`.
5. Select a profile from the **User system profile** list.
6. Click **Save**.

Music On Hold service configuration

**About this task**
Use the procedures in this section to configure Music On Hold service.

- [Configuring Music On Hold media](#) on page 258
- [Music on Hold Media Management](#) on page 259

**Configuring Music On Hold media**
Use this procedure to configure access to the Music on Hold (MOH) conferencing logical entity in the domain where you need service.
Before you begin

- Music on Hold must be included in the logical entity. From the Provisioning Client menu bar, select Translations, Logical Entity; ensure that Music on Hold is present in the Selected routable services list.

Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Music on Hold to access the Music On Hold Service portlet.
2. In the Music On Hold Service portlet, select the Create Music Folders tab.
3. From the Select domain list, select a domain to which you want to add Music On Hold service and click >>.
4. In the Select pool field, select a pool and click >>.
5. In the Folder field, type a name for the music folder and click Save.
6. Click Media Management next to the folder you created in 5 on page 259.
7. Click Browse and select the file to add.
8. In the Name field, type the name for the new media file.
9. Click Save.
10. Click the Assign tab.
11. In the Select domain list, select a domain.
12. In the Select folder list, select the folder you created in 5 on page 259.
13. Click Save.

Music on Hold Media Management

About this task

Use the procedures in this section to manage Music on Hold media.

- Adding Music on Hold folders on page 259
- Assigning a music folder to the Music On Hold service on page 260
- Managing Music on Hold folders on page 261
- Adding media files to Music on Hold folders on page 261
- Managing media files in Music on Hold folders on page 262

Adding Music on Hold folders

About this task

Use this procedure to create Music on Hold music folders.
Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Music on Hold to access the Music on Hold Service portlet.
2. In the Music on Hold Service portlet, click Create Music Folders.
3. In the Select domain list, select a domain in which to add the music folder and click >>.
4. In the Select pool list, select a pool in which to add the music folder and click >>.
5. In the Folder field, type the name for the new music folder.
6. Click Save.

Adding Music on Hold folders job aid

About this task

The following job aid describes the parameters for adding music folders.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain in which to add a music folder.</td>
</tr>
<tr>
<td>Select pool</td>
<td>From the list, select a pool in which to add a music folder.</td>
</tr>
<tr>
<td>Folder</td>
<td>Type a descriptive name for the new folder.</td>
</tr>
</tbody>
</table>

Assigning a music folder to the Music On Hold service

About this task

Use this procedure to assign a music folder in the domain where access to the Music on Hold (MOH) service is needed.

Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Music On Hold to access the Music On Hold Service portlet.
2. In the Music On Hold Service portlet, select the Assign Music Folders tab.
3. In the Select domain field, select a domain to which you want to add Music On Hold folders and click >>.
4. In the Select folder field, select a music folder and click Save.

Assigning a music folder to the Music on Hold service job aid

About this task

The following job aid describes the parameters for assigning music folders.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain in which to assign a music folders.</td>
</tr>
<tr>
<td>Select folder</td>
<td>From the list, select a folder to assign.</td>
</tr>
</tbody>
</table>
Managing Music on Hold folders

About this task
Use this procedure to rename or delete Music on Hold music folders.

Procedure
1. From the Provisioning Client menu bar, select Services > Announcements > Music on Hold to access the Music on Hold Service portlet.
2. In the Music on Hold Service portlet, in the Select domain list, select a domain and click >>.
3. In the Select pool list, select a pool and click >>.
4. (Optional) To rename a folder, click the folder name. In the Name field, type a name and click Save.
5. (Optional) To delete a folder, click Delete next to the folder name. Type your password, and click Confirm. Note: You cannot delete a folder if it is assigned to a domain.
6. (Optional) To delete all folders and files, click Remove All. Type your password, and click Confirm.

Managing Music on Hold folders job aid

About this task
The following job aid describes the parameters for managing music folders.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select domain</td>
<td>From the list, select a domain in which to manage music folders.</td>
</tr>
<tr>
<td>Select pool</td>
<td>From the list, select a pool in which to manage music folders.</td>
</tr>
<tr>
<td>Name</td>
<td>Type a name for the music folder.</td>
</tr>
</tbody>
</table>

Adding media files to Music on Hold folders

About this task
Use this procedure to add media files to a Media on Hold music folder.

Procedure
1. From the Provisioning Client menu bar, select Services > Announcements > Music on Hold to access the Music on Hold Service portlet.
2. In the Music on Hold Service portlet, click Media Management next to the folder in which to add the files.
3. Click Browse, and select the file to add.
4. In the Name field, type the name for the new media file.
5. Click Save.
Adding media files to Music on Hold folders job aid

About this task

The following job aid describes the parameters for adding media files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a descriptive name for the new media file.</td>
</tr>
</tbody>
</table>

Managing media files in Music on Hold folders

About this task

Use this procedure to download, rename, or delete media files in Music on Hold music folders.

Procedure

1. From the Provisioning Client menu bar, select Services > Announcements > Music on Hold to access the Music on Hold Service portlet.
2. In the Music on Hold Service portlet, optionally click on a media file name to rename that file. Type a new name in the Name field and click Save.
3. (Optional) To delete a file, click Delete next to the folder name. Type your password and click Confirm.
4. (Optional) To delete all files from the current folder, click Remove All next to the folder name. Type your password and click Confirm.
5. (Optional) To download a file, click Download next to the folder name. Click Browse to select an application to open the file or click OK to save the file to your local PC.

Managing media files in Music on Hold folders job aid

About this task

The following job aid describes the parameters for managing media files.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name for the media file.</td>
</tr>
</tbody>
</table>

Network Call Logs service configuration

About this task

Use the procedures in this section to configure Network Call Logs service.

- Configuring the Network Call Logs service on page 263
- Assigning the Network Call Logs service to a domain on page 263
- Assigning the Network Call Logs service to a user on page 264
Configuring the Network Call Logs service

Use this procedure to configure the Network Call Logs service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Client Interface > Network Call Logs to access the Network Call Logs Service portlet.
2. Configure the parameters in the System Profile tab.
3. Click Save.

Configuring the Network Call Logs service job aid

About this task

This job aid describes the parameters for the System Profile tab of the Network Call Logs Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Maximum Number of Inbox Call Logs</td>
<td>This field enables a user to specify the maximum of call logs users can have in their Inbox.</td>
</tr>
<tr>
<td>Maximum number of outbox call logs</td>
<td>This field enables a user to specify the maximum of call logs users can have in their Outbox.</td>
</tr>
</tbody>
</table>

Assigning the Network Call Logs service to a domain

Use this procedure to configure the Network Call Logs service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click Network Call Logs.
3. On the System Profile tab of the Network Call Logs service portlet, click Assign/Remove for the profile in the Domain table column.
4. From the Available Domains list, select the domain to which you want to assign the profile.
5. Click Copy.
6. Click Save.
7. To remove, select the domain in the Selected Domains box and click Remove.
8. Click Save.

Assigning the Network Call Logs service to a user

Use this procedure to configure the Network Call Logs service.

Before you begin
- You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Network Call Logs.
3. On the User Data tab, in the Select user field, type a user name.
4. Click >>.
5. From the User system profile list, select a profile.
6. Click Save.

Network Call Waiting Disable service configuration

About this task
Use the procedures in this section to configure Network Call Waiting Disable service.

- Configuring the Network Call Waiting Disable service on page 264
- Assigning the Network Call Waiting Disable service to a domain on page 265
- Assigning the Network Call Waiting Disable service to a user on page 265

Configuring the Network Call Waiting Disable service

Use this procedure to configure the Network Call Waiting Disable service.

Before you begin
- You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Network Call Waiting Disable to access the Network Call Waiting Disable Service portlet.
2. Configure the parameters in the System Profile tab.
3. Click Save.

Configuring the Network Call Waiting Disable service job aid

About this task

This job aid describes the parameters for the System Profile tab of the Network Call Waiting Disable Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Network call waiting disable per call via VSC</td>
<td>Allows a user to activate/deactivate and status check of the Network Call Waiting Disable service, using the Vertical Service Code (VSC) option.</td>
</tr>
<tr>
<td>Network call waiting disable permanent via VSC</td>
<td>Allows a user to activate Network Call Waiting Disable service of the subscriber permanently, using the VSC option.</td>
</tr>
</tbody>
</table>

Assigning the Network Call Waiting Disable service to a domain

Use this procedure to configure the Network Call Waiting Disable service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click Network Call Waiting Disable.
3. On the System Profile tab of the Network Call Waiting Disable Service portlet, click Assign/Remove for the profile in the Domain table column.
4. From the Available Domains list, select the domain to which you want to assign the profile.
5. Click Copy.
6. Click Save.
7. To remove, select the domain in the Selected Domains box, and click Remove.
8. Click Save.

Assigning the Network Call Waiting Disable service to a user

Use this procedure to configure the Network Call Waiting Disable service.

Before you begin

• You have Services provisioning rights.
Procedure

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Network Call Waiting Disable.
3. On the User Data tab, in the Select user field, add a user name.
4. Click >>.
5. Select a profile from the User system profile list.
6. Click Save.
7. (Optional) In the User Profile section, configure the Network call waiting disable parameter as required and click Save.

PBX Communicator service configuration

About this task
Avaya Aura® Application Server 5300 does not support the PBX Communicator service.

Personal Ringback Tones service configuration

About this task
Application Server 5300 does not support Personal Ringback Tones/Colorful Ringback Tones.

Presence service configuration

About this task
Use the procedures in this section to configure the Presence service.

• Configuring the Presence service on page 266
• Assigning the Presence service to a domain on page 267
• Assigning the Presence service to a user on page 268

Configuring the Presence service

Use this procedure to configure the Presence service.
Important:
For banning users from seeing your Presence status, see Banning users on page 125.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Services > Presence to access the Presence Service portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.

Configuring the Presence service job aid

About this task
This job aid describes the parameters for the System Profile tab in the Presence Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Maximum friends list</td>
<td>Specifies the number of people in a list of friends. A user can subscribe up to 100 people to view their presence. Although users can log on to numerous devices, the list of friends is a shared resource. For example, if the maximum list of friends size is configured to 10, then each of the client devices can hold 10 friends (the same 10 friends, not 10 per device). The client has the option of sending Presence status to any of the friends.</td>
</tr>
<tr>
<td>Report when inactive</td>
<td>Enables the autopresence (optional) feature that detects when a PC is not in use and updates their Presence status on the network.</td>
</tr>
<tr>
<td>Inactivity timer</td>
<td>Determines the length of time a user’s PC must be idle before their Presence status is updated on the network.</td>
</tr>
<tr>
<td>Report when on the phone</td>
<td>Detects when a user is on an active call and updates the user’s Presence status on the network.</td>
</tr>
</tbody>
</table>

Assigning the Presence service to a domain

Use this procedure to assign the Presence service to a domain.

Before you begin
• You have Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click Presence.
3. On the **System Profile** tab of the Presence Service portlet, click **Assign/Remove** for the profile in the **Domain** table column.

4. From the **Available Domains** list, select the domain to which you want to assign the profile.

5. Click **Copy**.

6. Click **Save**.

7. To remove, select the domain from the **Selected Domains** list and click **Remove**.

8. Click **Save**.

### Assigning the Presence service to a user

Use this procedure to assign the Presence service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Assign Services** to access the User Services portlet.

2. On the **Services** tab, click **Presence**.

3. On the **User Data** tab, in the **Select user** field, type a user name.

4. Click `>>`

5. From the **User system profile** list, select a profile.

6. Click **Save**.

7. Configure the parameters in **User Profile**.

8. Click **Save**.

### Assigning the Presence service to a user job aid

This job aid describes the User Profile check boxes that appear on the **User Data** tab in the Presence Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report when inactive</td>
<td>Enables the autopresence (optional) feature that detects when a PC is not in use and updates their Presence status on the network. Check the box to enable this parameter.</td>
</tr>
<tr>
<td>Inactivity timer</td>
<td>Determines the length of time a user’s PC must be idle before their Presence status is updated on the network. Check the box to enable this parameter.</td>
</tr>
<tr>
<td>Report when on the phone</td>
<td>Detects when a user is on an active call and updates the user’s Presence status on the network. Check the box to enable this parameter.</td>
</tr>
</tbody>
</table>
Provisioning Short Dialing Codes

Use this procedure to provision Short Dialing Codes.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Origination > Short Dial Code to access the Short Dialing Code Service portlet.
2. On the Feature Translation tab, select the domain from the list and click >>.
3. Configure the parameters for this service in the Feature Translation tab.
4. Click Add.

Provisioning Short Dialing Codes job aid

The following job describes the data for the Feature Translation tab in the Short Dialing Codes Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Type a name that specifies the translation record. The name must be unique in a domain and contain 1 to 32 characters.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Type a VSC prefix. The prefix can be from 1 to 32 digits in length, and can begin or end with *, #, or any digit.</td>
</tr>
<tr>
<td></td>
<td>✩ Note: To avoid unexpected results, use each VSC prefix only once in a domain, and ensure that no VSC prefix is a subset of any other. For example, if you provision one VSC to be *1234, do not create another which is a subset of *1234 (*1, *12, *123) or which contains *1234 (such as *12345).</td>
</tr>
<tr>
<td>SDC URI</td>
<td>Type a valid SIP address of a user (for example, user@domain). Both SIP URI and TEL URI are supported.</td>
</tr>
</tbody>
</table>

Quality of Service configuration

About this task

Use the procedures in this section to configure Quality of Service (QoS).

• Configuring the QoS service on page 270
• Assigning the QoS service to a domain on page 270
Configure the QoS service

Use this procedure to configure Quality of Service (QoS).

**Before you begin**
- You have Services provisioning rights.

**Procedure**
1. From the Provisioning Client menu bar, select Services > Media > QoS to access the QoS Service portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.

**Configuring the QoS service job aid**

**About this task**
This job aid describes the parameters for the System Profile tab in the QoS Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>QoS DiffServ Code for Audio</td>
<td>Specifies quality of service for client signaling</td>
</tr>
<tr>
<td>QoS DiffServ Code for Video</td>
<td>Specifies quality of service for client video</td>
</tr>
</tbody>
</table>

Assigning the QoS service to a domain

Use this procedure to assign the QoS service to a domain.

**Before you begin**
- You have Services provisioning rights.

**Procedure**
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click QoS.
3. On the System Profile tab of the QoS Service portlet, click Assign/Remove for the profile in the Domain table column.
4. From the Available Domains list, select the domain to which you want to assign the profile.
5. Click Copy.

The domain that you selected appears in the Selected Domains box.
6. Click **Save**.
7. To remove, select the domain in the **Selected Domains** box and click **Remove**.
8. Click **Save**.

---

**Assigning the QoS service to a user**

Use this procedure to assign the QoS service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Assign Services** to access the User Services portlet.
2. On the **Services** tab, click **QoS**.
3. From the **User Data** tab, in the **Select user** box, type a user name.
4. Click `>>`.
5. Select a profile from the **User system profile** list.
6. Click **Save**.

---

**Routable services information configuration for Meet Me Audio Conferencing**

**About this task**

Use the procedures in this section to configure routable services information for the Meet Me Audio Conferencing service.

The Meet Me Audio Conferencing service provides reservation-less multimedia conferencing based upon the Avaya Media Server platform. Meet Me Audio Conferencing service users have their own private conferencing resource available for meetings at any time. Use of this personal conference resource is controlled by the conference owner, the chairperson, who is provisioned with this service.

- [Configuring access to the logical entity for Meet Me audio conferencing](#) on page 272
- [Creating an alias for Meet Me audio conferencing](#) on page 272
Configuring access to the logical entity for Meet Me audio conferencing

About this task
Use this procedure to configure access to the Meet Me audio conferencing logical entity in the domain where you need service.

Procedure
1. From the Provisioning Client menu bar, select Services > Conferencing > Meet Me Conferencing to access the Meet Me Conferencing Service portlet.
2. In the Meet Me Conferencing portlet, select the Conference Pool tab.
3. In the Select domain field, select a domain to which you want to add routable services for Meet Me Conferencing and click >>.
4. In the Select pool field, select a pool.
5. Click Save.

Creating an alias for Meet Me audio conferencing

About this task
Use this procedure to create an alias for Meet Me audio conferencing. Create an alias in the domain where you need service.

Important:
You can only create aliases for Meet Me at the root domain level.

Procedure
1. From the Provisioning Client menu bar, select Services > Conferencing > Meet Me Conferencing to access the Meet Me Conferencing Service portlet.
2. In the Meet Me Conferencing Service portlet, select the Service Alias tab.
3. In the Select domain field, select a domain to which you want to add a service alias for Meet Me Conferencing and click >>.
4. In the Alias field, enter the alias for the Meet Me Conferencing logical entity (for example, 7736237320).
5. In the Select pool field, select a pool.
6. In the Locale field, select a language associated with the service.
7. Click Save.
Routable services information configuration for the Music on Hold (MOH) feature

About this task

MOH must be assigned to a user. If a user has MOH enabled and then puts a caller on hold (end-user hold, transfer hold, and call park hold), then the caller on hold hears the music or tone files assigned to the domain/subdomain of the user who placed the call on hold.

If MOH is not enabled for a user, and this user places a caller on hold, then the caller on hold does not hear any tone or music.

Use the following procedures to configure routable services information for MOH.

- Configuring Music On Hold media on page 258
- Assigning a music folder to the Music On Hold service on page 260

Configuring Service Capabilities Interaction Manager

About this task

Use this procedure configure Service Capabilities Interaction Manage on the system.

Configure the telephony routes table to remove the access and service digits and route to the appropriate gateway. If the gateway route terminates to the local PSTN gateway, configure the gateway route type as public.

Procedure

1. From the Provisioning Client menu bar, select Services > Applications > Service Capabilities Interaction Manager.
2. In the Service Capabilities Interaction Manager portlet, select the types, services, and mutex services between which to permit interaction.
3. To add additional services, type values in the Service name and Vendor fields.
4. Click Save.

Selective Call Reject service configuration

About this task

Use the procedures in this section to configure the Selective Call Reject service.

- Configuring the Selective Call Reject service on page 274
- Assigning the Selective Call Reject service to a domain on page 274
Configuring the Selective Call Reject service

Use this procedure to configure the Selective Call Reject service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Restrictions > Selective Call Reject to access the Selective Call Reject Service portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.

Configuring the Selective Call Reject service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Selective Call Reject Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The name to identify the system profile.</td>
</tr>
<tr>
<td>Incoming selective call reject</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict incoming calls.</td>
</tr>
<tr>
<td>Outgoing selective call reject</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict outgoing calls.</td>
</tr>
<tr>
<td>Incoming selective call reject via VSC</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict incoming calls through VSC.</td>
</tr>
<tr>
<td>Outgoing selective call reject via VSC</td>
<td>Allows the administrator or user to provision a phone number or SIP address list to restrict outgoing calls through VSC.</td>
</tr>
<tr>
<td>Add incoming call to selective reject list</td>
<td>Allows the administrator or user to add incoming calls to their Selective Reject List.</td>
</tr>
</tbody>
</table>

Assigning the Selective Call Reject service to a domain

Use this procedure to assign the Selective Call Reject service to a domain.

Before you begin

• You have Services provisioning rights.
Procedure

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click Selective Call Reject.
3. On the System Profile tab of the Selective Call Reject Service portlet, click Assign/Remove for the profile in the Domain table column.
4. From the Available Domains list, select the domain to which you want to assign the profile.
5. Click Copy.
6. Click Save.
7. To remove, select the domain in the Selected Domains box, and click Remove.
8. Click Save.

Assigning the Selective Call Reject service to a user

Use this procedure to assign the Selective Call Reject service to a user.

Before you begin

- You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Selective Call Reject.
3. On the User Data tab, in the Select user field, type a user name.
4. Click >>.
5. Select a profile from the User system profile list.
6. Click Save.

Teen Service

Teen Services is not supported in Application Server 5300.
TDM Message Waiting Indicator service configuration

About this task
Use the procedures in this section to configure the Time Division Multiplex (TDM) Message Waiting Indicator (MWI) service.

- Configuring a system profile for the TDM MWI service on page 276
- Assigning a system profile for the TDM MWI service to a domain on page 276
- Assigning a system profile for the TDM MWI service to a user on page 277

Configuring a system profile for the TDM MWI service

About this task
Use the following procedure to configure the system profile, and to specify the terminal server for the TDM Message Waiting Indicator service.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > TDM Message Waiting Indicator.
2. On the System Profile tab, configure the Profile name and SMDI server parameters.
3. Click Save.

Assigning a system profile for the TDM MWI service to a domain

About this task
Use the following procedure to assign the system profile for the TDM Message Waiting Indicator service to a domain.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > TDM Message Waiting Indicator.
2. On the System Profile tab, click Assign/Remove for the profile that you want to assign.
3. From the Available Domains list, select the domain to which you want to assign the profile and then click Copy.
4. (Optional) To remove a domain from the Selected Domains list, select the domain and click Remove.
5. Click Save.
Assigning a system profile for the TDM MWI service to a user

About this task

Use the following procedure to assign the system profile for the TDM Message Waiting Indicator service to a user.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > TDM Message Waiting Indicator.
2. On the User Data tab, in the Select user box, type a user name (in the user@domain format).
3. Click >>.
4. From the User's system profile list, select a user profile.
5. Click Save.

Configuring UCC Short Message Service

About this task

Use this procedure to configure the UCC Short Message service on the system.

Procedure

1. From the Provisioning Client menu bar, select Services > Media > UCC Short Message.
2. In the UCC Short Message Service portlet, configure parameters as required.
3. Click Save.

Configuring UCC Short Message Service job aid

About this task

This job aid describes the parameters that appear on the System Profile tab of the UCC Short Message Service (SMS) portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a descriptive name for the SMS system profile.</td>
</tr>
<tr>
<td>Allow SMS flag</td>
<td>Specify whether to allow SMS flag. Type 1 to allow SMS flag, or 0 to</td>
</tr>
<tr>
<td></td>
<td>disallow SMS flag. Default: 0</td>
</tr>
</tbody>
</table>

Table continues…
### Uniform Call Distribution service

#### About this task

Uniform Call Distribution (UCD) is a feature that can improve call-completion rates by matching incoming calls to available answering locations. UCD service is often used by service industries and catalog sales groups where a number of answering agents serve incoming calls. The service provides even distribution of incoming calls to a specific Listed Directory Number (LDN) or Uniform Resource Indicator (URI) over a group of subscribers, or agents, associated with that LDN or URI. This group of agents is called a Uniform Call Distribution (UCD) group. An agent can be assigned to only one group at a time.

### Routable services information configuration for Unified Communication service

#### About this task

Use the procedures in this section to configure routable services information for Unified Communications.

The Unified Communications service provides users with integrated access to their voice mail messages from a preferred client device, such as a PC, voice over IP (VoIP) phone, wireless phone, or a traditional circuit switched telephone. One single mailbox may be used by these many telephony devices and the messages deposited in this common mailbox may optionally be mailed to a user's email client, offering another convenient access option for voice mail message playback. Users manage their account through a traditional Telephony User Interface (TUI) or through the web-based Avaya Aura® Application Server 5300 Personal Agent, which may be optionally configured for the user.
Navigation

• Configuring access to the logical entity for Unified Communications on page 279
• Creating a message retrieval alias for Unified Communications on page 279
• Creating an express messaging alias for United Communications on page 280

Configuring access to the logical entity for Unified Communications

About this task
Use this procedure to configure access to the Unified Communications logical entity in the domain where routable service is needed.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Unified Communications to access the Unified Communications Services portlet.
2. In the Unified Communications Services portlet, select the Routable Service tab.
3. In the Select domain field, select a domain to which you want to add Unified Communications Services and click ».
4. In the Select pool field, select a pool and click Save.

Creating a message retrieval alias for Unified Communications

About this task
Use this procedure to create a message retrieval alias for the Unified Communications logical entity. The aliases for Unified Communications can be created only at the root domain level.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Unified Communications to access the Unified Communications Services portlet.
2. In the Unified Communications Services portlet, select the Message Retrieval Alias tab.
3. In the Select domain field, select a domain to which you want to Unified Communications Services and click ».
4. In the Alias field, enter a message retrieval alias for the Unified Communications (for example, 45000).
5. In the Select Pool list, select a pool.
6. In the Locale field, select the locale for the services (for example, English).
Creating an express messaging alias for United Communications

About this task
Use this procedure to create an express messaging alias for the Unified Communications logical entity.

Important:
You can create aliases for Unified Communications, only at the root domain level.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Unified Communications to access the Unified Communications Services portlet.
2. In the Unified Communications Services portlet, select the Express Messaging Aliases tab.
3. In the Select domain field, select a domain to which you want to add Unified Communications Services and click >>.
4. In the Alias field, enter an express messaging retrieval alias for the Unified Communications (for example, 46000).
5. In the Select Pool list, select a pool.
6. In the Locale list, select the locale for the logical entity services (for example, English).

Important:
The Locale selection determines the language used for voice prompts and announcements during express messaging sessions on the Unified Communications service logical entity.

7. Click Save.

Video service configuration

About this task
Use the procedures in this section to configure the Video service.

• Configuring the Video service on page 281
Configuring the Video service

Use this procedure to configure the Video service.

Before you begin

• You have Services provisioning rights.

Procedure

1. From the Provisioning Client menu bar, select Services > Media > Video to access the Video Service portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.

Configuring the Video service job aid

About this task

This job aid describes the parameters for the System Profile tab in the Video Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The profile name of this service.</td>
</tr>
<tr>
<td>Available Video Codecs</td>
<td>The list of video codecs configured on the system.</td>
</tr>
<tr>
<td>Selected Video Codecs</td>
<td>The list of video codecs that will be included to selection list box in the Video Configuration dialog in the AS 5300 UC Client.</td>
</tr>
<tr>
<td>Maximum bitrate (in kbps)</td>
<td>The maximum allowed bitrate for video, between 8 and 7000 Kbps. This is a numeric field.</td>
</tr>
<tr>
<td>Maximum video width (in pixels)</td>
<td>The maximum allowed width for video, between 32 and 1280 pixels. Pixel sizes should be multiples of 8. This is a numeric field.</td>
</tr>
<tr>
<td>Maximum video height (in pixels)</td>
<td>The maximum allowed height for video, between 32 and 720 pixels. Pixel sizes should be multiples of 8. This is a numeric field.</td>
</tr>
</tbody>
</table>

Assigning the Video service to a domain

Use this procedure to assign the Video service to a domain.

Before you begin

• You have Services provisioning rights.
**Procedure**

1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click Video.
3. On the System Profile tab of the Video service portlet, click Assign/Remove for the profile in the Domain table column.
4. From the Available Domains list, select the domain to which you want to assign the profile.
5. Click Copy.
6. Click Save.
7. To remove, select the domain in the Selected Domains list, and click Remove.
8. Click Save.

---

**Assigning the Video service to a user**

Use this procedure to assign the Video service to a user.

**Before you begin**

- You have Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Video.
3. On the User Data tab, in the Select user field, type a user name.
4. Click >>.
5. From the User system profile list, select a profile.
6. Click Save.

---

**Assigning the Preferred codec to a user**

**Before you begin**

Ensure that you have the Services provisioning rights.

**Procedure**

1. From the Provisioning Client menu bar, select Services > Assign Services to access the User Services portlet.
2. On the Services tab, click Video.
3. In the **Select user** field on the **User Data** tab, type the username.
4. Click `>>`.
5. From the **Preferred codec** list, select a codec.
6. Click **Save**.

---

**Voice mail configuration**

**About this task**

Configure the voice mail service to provide voice mail functionality for subscribers.

- [Assigning services to a domain](#) on page 192
- [Configuring the voice mail server host](#) on page 283
- [Adding a SIP-based voice mail server](#) on page 284
- [Adding a trunk-based voice mail server](#) on page 285
- [Adding a line-based voice mail server](#) on page 286
- [Adding a prefix-based voice mail server](#) on page 287
- [Configuring the Voicemail service profile](#) on page 288
- [Assigning the Voicemail service profile to a domain](#) on page 289
- [Assigning services to a user](#) on page 303
- [Assigning a voice mail server to a user](#) on page 290
- [Assigning the Voicemail system profile to a user](#) on page 289
- [Listing, modifying, and deleting a voice mail server](#) on page 291

---

**Configuring the voice mail server host**

Use this procedure to configure the voice mail server host.

You (an administrator) can provision a host for voice mail servers. This provisioning helps during upgrade in case an existing voice mail server has a Universal Resource Identifier (URI) provisioned, which translates to a voice mail server instead of the actual server information. Consequently, you can use the existing URI or provision a node to add a voice mail server host.

**Before you begin**

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- You have assigned the Voicemail service to the domain. See [Assigning services to a domain](#) on page 192.
**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Termination > Voicemail** to access the portlet.
2. Configure the parameters on the **VMS Host** tab.
3. Click **Save**.

**Configuring the voice mail server host job aid**

**About this task**

This job aid describes the parameters for the **VMS Host** tab in the Voicemail Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Host name      | Enter the name of the node in this field. The node name cannot be more than 30 characters in length and can only contain the following letters, numbers, and specific symbols:  
  - Letters: a to z and A to Z  
  - Numbers: 0 to 9  
  - Symbols: underscore (_)  |
| Host address   | Select either the Host URL or Address Name.  
  - Host URL: Select this field so that the existing voice mail server configuration works. However, any data available in this field is not validated and cannot be re-IP’ed. You can enter an IP address in this field; however, the data cannot be re-IP’ed.  
  - Address Name: Select the node you want to add from the list. This list shows the nodes and logical entities provisioned on the system.  
  Remember, both Host URL or Address Name fields are mutually exclusive and cannot be selected simultaneously. |

**Adding a SIP-based voice mail server**

Use this procedure to add a SIP-based voice mail server.

**Before you begin**

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- You have assigned the Voicemail service to the domain. See Assigning services to a domain on page 192.
- A configured voice mail server exists.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Termination > Voicemail** to access the Voicemail Service portlet.
2. On the **SIP VMS** tab, configure the **Name**, **Type**, **Client Contact**, **SESM**, **Domains**, and **Voicemail Host** parameters.

3. Click **Save**.

The SIP-based voice mail server you added now appears in a list of voice mail servers.

---

### Adding a SIP-based voice mail server job aid

**About this task**

This job aid lists describes the data for the **SIP VMS** tab in the Voicemail Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name (up to 200 characters) that identifies the line-based voice mail server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies that the voice mail gateway is SIP. Select from the list: SIP_VMS. Default: SIP_VMS</td>
</tr>
<tr>
<td>Client contact</td>
<td>The parameter (up to 400 characters) used to route voice mail. In most cases, you use the default (voice mail). If you require a different client contact, contact your technical support representative.</td>
</tr>
<tr>
<td>SESM</td>
<td>Specifies the AS 5300 Session Manager that hosts the voice-mail server being provisioned. This parameter is used in an N+1 environment. All AS 5300 Session Managers (that are not the home AS 5300 Session Manager) forward requests destined to voice mail to the address specified in this field. Note: From the list, you must select an AS 5300 Session Manager. Default: ServerHome (With this default, each AS 5300 Session Manager ignores this parameter and forward SIP requests to the voice mail server instead of forwarding them to a home Application Server.)</td>
</tr>
<tr>
<td>Domains</td>
<td>The line that uses this trunk-based voice mail server. Use the Ctrl-click key to select multiple domains to use the same voice mail server.</td>
</tr>
<tr>
<td>Voicemail Host</td>
<td>The name of the voice mail server host.</td>
</tr>
</tbody>
</table>

---

### Adding a trunk-based voice mail server

Use this procedure to add a trunk-based voice mail server to configure the AS 5300 Session Manager so that it can communicate with a voice mail server using a PRI or CAS gateway.

**Before you begin**

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- You have assigned the Voicemail service to the domain. See [Assigning services to a domain](#) on page 192.
- A configured voice mail server exists.
Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > Voicemail to access the Voicemail Service portlet.

2. On the Trunk VMS tab, configure the Name, Type, Client Contact, Domains, Address, and Voicemail Host parameters.

3. Click Save.

The trunk-based voice mail server you added now appears in the list of voice mail servers.

Adding a trunk-based voice mail server job aid

About this task

This job aid describes the parameters for the Trunk VMS tab in the Voicemail Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name (up to 200 characters) that identifies the line-based voice mail server.</td>
</tr>
<tr>
<td>Type</td>
<td>Specifies whether the voice mail Gateway is PRI or CAS. Select from the list: PRI_TRUNK or CAS_TRUNK. Default: PRI_TRUNK</td>
</tr>
<tr>
<td>Client contact</td>
<td>The parameter (up to 400 characters) used to route voice mail. In most cases, you use the default (voice mail). If you require a different client contact, contact your technical support representative.</td>
</tr>
<tr>
<td>Domains</td>
<td>The line that uses this trunk-based voice mail server. Use the Ctrl-click key to select multiple domains to use the same voice mail server.</td>
</tr>
<tr>
<td>Address</td>
<td>The Long name of the iTouch terminal configured in element manager.</td>
</tr>
<tr>
<td>SMDI Version</td>
<td>The SMDI version. Only two versions of the SMDI protocol exist: Version 1 and Version 2. (Version 2 is the latest draft and is supported by most voice mail servers.)</td>
</tr>
<tr>
<td>Voicemail Host</td>
<td>The name of the voice mail server host.</td>
</tr>
</tbody>
</table>

Adding a line-based voice mail server

Use this procedure to add a line-based voice mail server.

Before you begin

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- You have assigned the Voicemail service to the domain. See Assigning services to a domain on page 192.
- A configured voice mail server exists.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > Voicemail to access the Voicemail Service portlet.
2. On the **Line VMS** tab, configure the **Name**, **Client Contact**, **Max call duration**, **Domains**, and **Address**, parameters.

3. Click **Save**.

   The line-based voice mail server you added now appears in the list of voice mail servers.

### Adding a line-based voice mail server job aid

**About this task**

This job aid describes the parameters for the **Line VMS** tab in the Voicemail Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Name</strong></td>
<td>The name (up to 200 characters) that identifies the line-based voice mail server.</td>
</tr>
<tr>
<td><strong>Client contact</strong></td>
<td>The parameter (up to 400 characters) used to route voice mail. In most cases, you use the default (voice mail). If you require a different client contact, contact your technical support representative.</td>
</tr>
<tr>
<td><strong>Max Call Duration</strong></td>
<td>The maximum length of the call that routes to the voice mail server. After the call length reaches this limit, it stops and all previous speech is recorded to the voice mail server.</td>
</tr>
<tr>
<td><strong>Domains</strong></td>
<td>The line that uses this trunk-based voice mail server. Use the Ctrl-click key to select multiple domains to use the same voice mail server.</td>
</tr>
<tr>
<td><strong>Address</strong></td>
<td>The Long name of the iTouch terminal configured in element manager.</td>
</tr>
</tbody>
</table>

---

### Adding a prefix-based voice mail server

Provision (add) a prefix-based voice mail server to configure the application so that it can communicate with a voice mail server using prefixes.

**Before you begin**

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- You have assigned the Voicemail service to the domain. See [Assigning services to a domain](#) on page 192.
- A configured voice mail server exists.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Termination > Voicemail** to access the Voicemail Service portlet.

2. On the **Prefix VMS** tab, configure the **Name**, **Client Contact**, **Domains**, and **Prefix** parameters.

3. Click **Save**.

   The prefix-based voice mail server you added now appears in the list of voice mail servers.
Provisioning a prefix-based voice mail server job aid

This job aid describes the parameters for the Prefix VMS tab in the Voicemail Service portlet.

Table 18: Prefix-based voice mail server parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Type</th>
<th>Range</th>
<th>Default</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>String (200)</td>
<td>Up to 200 chars</td>
<td>None</td>
<td>The name that identifies the prefix-based voice mail server.</td>
</tr>
<tr>
<td>Client contact</td>
<td>String (400)</td>
<td>Up to 400 chars</td>
<td>Voicemail</td>
<td>The field used to route voice mail. In most cases, you will use the default (voicemail). If you require a different client contact, contact your technical support representative.</td>
</tr>
<tr>
<td>Domains</td>
<td>String (64)</td>
<td>Up to 64 chars</td>
<td>None</td>
<td>Specify the domains that are supported by the voice mail service.</td>
</tr>
<tr>
<td>Prefix</td>
<td>String (64)</td>
<td>Up to 64 chars</td>
<td>None</td>
<td>The field identifies the prefix digits that will be used when routing to the voice mail server.</td>
</tr>
</tbody>
</table>

Configuring the Voicemail service profile

Use this procedure to configure the Voicemail service profile.

Before you begin

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- The Voicemail service is already assigned to the domain. See Assigning services to a domain on page 192.
- The voice mail server host is already configured. See Configuring the voice mail server host on page 283.
- A configured voice mail server exists.

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > Voicemail to access the portlet.
2. Configure the parameters on the System Profile tab.
3. Click Save.
Configuring the Voicemail service profile job aid

About this task

This job aid describes the parameters for the **System Profile** tab in the Voicemail Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Revertive Call Support</td>
<td>Retrieve voice mail or, for other subscribers, to leave a voice mail message. Voice mail is retrieved from a network server. The user is aware of deposited voice mail since the user’s client’s MWI (message waiting indicator) is enabled.</td>
</tr>
<tr>
<td>Voice mail retrieve via VSC</td>
<td>Retrieve voice mail using the Vertical Service Code.</td>
</tr>
</tbody>
</table>

Assigning the Voicemail service profile to a domain

Use this procedure to assign the Voicemail service profile to a domain.

**Before you begin**

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- The Voicemail service is already assigned to the domain. See [Assigning services to a domain](#) on page 192.
- The voice mail server host is already configured. See [Configuring the voice mail server host](#) on page 283.
- A configured voice mail server exists.
- The Voicemail service profile is already configured. See [Configuring the Voicemail service profile](#) on page 288.

**Procedure**

1. From the Provisioning Client menu bar, select **Services > Call Termination > Voicemail** to access the portlet.
2. Click **Assign/Remove** for the profile you want to assign to a domain from the **Domain** column.
3. From the **Available Domains** list, select a domain and click **Copy**.
4. To remove a domain, select a domain from the **Selected Domains** field, and click **Remove**.
5. Click **Save**.

Assigning the Voicemail system profile to a user

Use this procedure to assign the voice mail system profile to user.

Comments on this document? infodev@avaya.com
Before you begin
• You have Services provisioning rights.
• You have Voice Mail Management provisioning rights.
• The Voicemail service is already assigned to the domain. See Assigning services to a domain on page 192.
• The voice mail server host is already configured. See Configuring the voice mail server host on page 283.
• A configured voice mail server exists.
• The Voicemail service profile is already configured. See Configuring the Voicemail service profile on page 288.
• The Voicemail service profile is already assigned to the domain. See Assigning the Voicemail service profile to a domain on page 289.

Procedure
1. From the Provisioning Client menu bar, select Services > Call Termination > Voicemail to access the portlet.
2. On the User Data tab, in the Select user box, type a user name.
3. Click >>.
4. From the User system profile list, select a profile.
5. Click Save.

Assigning a voice mail server to a user
For a user to have voice mail, you must associate a voice mail server and mail box for that user.

Before you begin
• You have Services provisioning rights.
• You have Voice Mail Management provisioning rights.
• The Voicemail service is already assigned to the domain. See Assigning services to a domain on page 192.
• The voice mail server host is already configured. See Configuring the voice mail server host on page 283.
• A configured voice mail server exists.
• The Voicemail service profile is already configured. See Configuring the Voicemail service profile on page 288.
• The Voicemail service profile is already assigned to the domain. See Assigning the Voicemail service profile to a domain on page 289.
• The Voicemail system profile is already assigned to the user. See Assigning the Voicemail system profile to a user on page 289.
Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > Voicemail to access the Voicemail Service portlet.
2. On the User VMS tab, in the Select user box, type a user name and click >>.
3. Configure the Voicemail server and Voicemail parameters.
4. Click Save.

Assigning a voice mail server to a user job aid

This job aid describes the parameters for the User VMS tab in the Voicemail Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Voicemail server</td>
<td>From the list, select a voice mail server provisioned on the domain to send calls for this user to voice mail.</td>
</tr>
<tr>
<td>Voicemail</td>
<td>Enter the voice mail address (up to 30 characters).</td>
</tr>
</tbody>
</table>

Listing, modifying, and deleting a voice mail server

Use this procedure to list, modify and delete a voice mail server.

Before you begin

- You have Services provisioning rights.
- You have Voice Mail Management provisioning rights.
- Assigning services to a domain on page 192
- Configuring the voice mail server host on page 283

Procedure

1. From the Provisioning Client menu bar, select Services > Call Termination > Voicemail to access the Voicemail Service portlet.
2. Select the VMS Host tab.
3. To view the details of a voice mail server, click the link of the voice mail server in the Name table column.
4. To modify the voice mail server you selected from the Name table column, configure the Hostname and Host address parameters.
5. Click Save.
6. To delete a voice mail server from the system, click Delete for the voice mail server you want to delete.
7. Type a valid administrator's password in the confirmation window to delete the voice mail server.

OR
Click **Cancel** to cancel the delete operation.

After you delete the voice mail server, the users that have this voice mail server provisioned for them have no voice mail server and mailbox.

---

## XMPP Gateway service configuration

Use the procedures in this section to configure XMPP Gateway service:

- [Configuring the XMPP Gateway service](#) on page 292
- [Assigning the XMPP service to a domain](#) on page 293
- [Assigning the XMPP Gateway service to a user](#) on page 293
- [Configuring the XMPP Incoming Connection policy](#) on page 294

---

## Configuring the XMPP Gateway service

**About this task**

Use this procedure to configure the XMPP Gateway service.

**Before you begin**

Ensure that you have the Services provisioning rights to define and assign services to domains.

**Procedure**

1. From the **Provisioning Client** menu bar, select **Services > XMPP Gateway** to access the XMPP Gateway Service portlet.
2. On the **System Profile** tab, configure the parameters as required.
3. Click **Save**.

---

## Configuring the XMPP Gateway service job aid

**About this task**

This job aid describes the parameters for the **System Profile** tab in the XMPP Gateway service portlet.

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>The profile name of the service.</td>
</tr>
<tr>
<td>XMPP domain name</td>
<td>The name of the system XMPP domain.</td>
</tr>
<tr>
<td>Server profile</td>
<td>The Core Services Session Manager system profile to specify the Session Manager that is responsible to serve the system XMPP domain.</td>
</tr>
</tbody>
</table>
Assigning the XMPP service to a domain

Before you begin
Ensure that you have the Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Services to access the User Services portlet.
2. On the Services tab, click XMPP Gateway.
3. On the System Profile tab of the XMPP Gateway Service portlet, click Assign/Remove for the profile in the Domain table column.
4. From the Available Domains list, select the domain to which you want to assign the profile.
5. Click Copy.
6. Click Save.
7. To remove, select the domain from the Selected Domains list and click Remove.
8. Click Save.

Assigning the XMPP Gateway service to a user

Before you begin
Ensure that you have the Services provisioning rights.

Procedure
1. From the Provisioning Client menu bar, select User > Search to access the User portlet.
2. On the Advanced Search tab, enter the appropriate search information about the user to whom you want to assign this feature, and then click Search.
3. On the Services tab of the User portlet scroll down the table and select the XMPP Gateway option.
4. Click Save.
5. On the Services tab, scroll down the table and click XMPP Gateway.
6. On the User Data tab, type the user name in the Select user field.
7. Click >>.
8. From the User system profile list, select a profile.
9. Click Save.
10. Configure the parameters in User Profile.
11. Click **Save**.

### Assigning the XMPP Gateway service to a user job aid

**About this task**

This job aid describes the User Profile fields that appear on the User Data tab in the XMPP Gateway Service portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XMPP name</td>
<td>The XMPP name of the user used as a localpart of JID in XMPP communications.</td>
</tr>
</tbody>
</table>

### Configuring the XMPP Incoming Connection policy

**About this task**

Use this procedure to configure the incoming connection policy to manage the establishing of external XMPP connections.

**Before you begin**

Ensure that you have the Services and the System Layer Management provisioning rights.

**Procedure**

1. From the **Provisioning Client** menu bar, select **Services > XMPP Gateway**.
2. On the **Incoming Connections** tab, choose the policy type according to the needs:
   - **Allow All (Default value)**: No specific conditions for incoming XMPP messages. All XMPP messages from all XMPP domains are allowed.
   - **Allow From White List**: The incoming XMPP messages are allowed only from the list of provisioned XMPP domains.
   - **Deny From Black List**: The incoming XMPP messages are allowed from all XMPP domains except from provisioned domains.
3. For **Allow From White List** and **Deny From Black List** policy types, specify list of external domains:
   a. In the **External domains** field, type the name of the external XMPP domain.
   b. Click **Add**.
   c. To delete the external XMPP domain, select the XMPP domain from the text box and click **Delete**.
   d. Click **Save**.
Chapter 17: Subscriber management procedures

About this task
Use the procedures in this section to manage subscribers in a domain or a subdomain.

- Adding a user to a domain or a subdomain on page 295
- Listing and modifying subscribers on page 299
- Changing user password on page 303
- Assigning services to a user on page 303
- Using the Actions tab to modify a user on page 304
- Configuring the Personal Agent on behalf of a user on page 305
- Adding aliases and directory numbers for a user on page 306
- Moving subscribers between domains on page 307

Adding a user to a domain or a subdomain
Use this procedure to add a user to a domain or subdomain.

Before you begin
- You have domain management rights.

Procedure
1. From the Provisioning Client menu bar, select **User > Add** to access the User portlet.
2. From the **Select domain** list, select the domain (or subdomain) to which you want to add a new user.
3. From the **Type** list, select the type of user you want to add.

<table>
<thead>
<tr>
<th>To add</th>
<th>Choose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Aura subscriber</td>
<td>Aura</td>
</tr>
<tr>
<td>Application Server 5300 subscriber</td>
<td>Standalone</td>
</tr>
</tbody>
</table>

Table continues…
4. Click >>.
5. Configure the parameters for the user.
6. Click Save.

The save operation succeeds only if the maximum number of users that can be added to the domain has not been reached.

## Adding a user to a domain or a subdomain job aid

### About this task

This job aid describes the parameters for adding a user.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>User name of the user. Preferably use lowercase. Does not have to be the same name as the First Name.</td>
</tr>
<tr>
<td></td>
<td><strong>Important:</strong> For the Commercial Cost Avoidance (CCA) feature to work properly, configure the private number for this parameter (for example, 997261135).</td>
</tr>
<tr>
<td></td>
<td>Remember, a user name can only contain letters, numbers, and specific symbols:</td>
</tr>
<tr>
<td></td>
<td>• Letters: a to z, A to Z</td>
</tr>
<tr>
<td></td>
<td>• Numbers: 0 to 9</td>
</tr>
<tr>
<td></td>
<td>• Symbols: period (.), hyphen (-) and underscore (_)</td>
</tr>
<tr>
<td></td>
<td>Type: String (60)</td>
</tr>
<tr>
<td></td>
<td>Range: Up to 60 characters</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the user. Must match the password policy of the domain.</td>
</tr>
<tr>
<td></td>
<td>Type: String (20)</td>
</tr>
<tr>
<td></td>
<td>Range: Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Confirm Password</td>
<td>Password of the user.</td>
</tr>
<tr>
<td></td>
<td>Type: String (20)</td>
</tr>
<tr>
<td></td>
<td>Range: Up to 20 characters</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Service set</td>
<td>The list of service sets assigned to the user's domain or subdomain.</td>
</tr>
<tr>
<td></td>
<td>Type: Select from list</td>
</tr>
<tr>
<td></td>
<td>Range: N/A</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Status Reason</td>
<td>The status value of the user.</td>
</tr>
<tr>
<td></td>
<td>Type: Select from list</td>
</tr>
<tr>
<td></td>
<td>Range: N/A</td>
</tr>
<tr>
<td></td>
<td>Default: ACTIVE</td>
</tr>
<tr>
<td>Location</td>
<td>The location where the user resides.</td>
</tr>
<tr>
<td></td>
<td>Type: Select from list</td>
</tr>
<tr>
<td></td>
<td>Range: Up to 30 characters</td>
</tr>
<tr>
<td></td>
<td>Default: Use Domain Default &quot;Other&quot;</td>
</tr>
<tr>
<td>First Name</td>
<td>First name of the user. Case sensitive. First name cannot contain an apostrophe, a single quotation mark ('), or a double quotation mark (&quot;), The first name combines with the last name to form the display name on the Avaya IP Deskphones. Either first name or last name is a required field. Optionally, and if the LDAP scheme is configured to support it, enter a Title or Rank, followed by a space, followed by a first name. For example, Mister Smith.</td>
</tr>
<tr>
<td></td>
<td>Type: String (30)</td>
</tr>
<tr>
<td></td>
<td>Range: Up to 30 characters</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Last Name</td>
<td>Last name of the user. Case sensitive. Last name cannot contain an apostrophe, a single quotation mark (’), or a double quotation mark (“), The last name combines with the first name to form the display name on the Avaya IP Deskphones. Either first name or last name is a required field.</td>
</tr>
<tr>
<td></td>
<td>Type: String (30)</td>
</tr>
<tr>
<td></td>
<td>Range: Up to 30 characters</td>
</tr>
<tr>
<td></td>
<td>Default: N/A</td>
</tr>
<tr>
<td>Email</td>
<td>The email address of the user.</td>
</tr>
<tr>
<td></td>
<td>Type: String (60)</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Business phone | Business phone number.  
Type: String (60)  
Range: Up to 60 characters  
Default: N/A                                                                                                                                            |
| Home phone  | Home phone number.  
Type: String (30)  
Range: Up to 30 characters  
Default: N/A                                                                                                                                            |
| Cell phone  | Cell phone number, also known as Cellular DN, which acts as a routing alias for the subscriber.  
Type: String (30)  
Range: Up to 30 characters  
Default: N/A                                                                                                                                            |
| Pager       | Pager number of the user.  
Type: String (30)  
Range: Up to 30 characters  
Default: N/A                                                                                                                                            |
| Fax         | Fax number of the user.  
Type: String (30)  
Range: Up to 30 characters  
Default: N/A                                                                                                                                            |
| Time Zone   | The time zone that the user belongs to.  
Type: Select from list  
Range: N/A  
Default: Eastern Standard Time                                                                                                                                 |
| Locale      | Locale of the user.  
Type: Select from list  
Range: N/A  
Default: English                                                                                                                                 |
| Common Names | The common names assigned to the user. When **SIP TLS Identity Checking** is enabled, the common names in this field are compared with the common name in the X.509 client certificate for the SIP TLS connections. |
Listing and modifying subscribers

About this task
Use this procedure to list and modify users.

Procedure
1. From the Provisioning Client menu bar, select User, Search.
2. In the Domain field list, select the domain.
3. In the Search by field list, select the search criteria you want to use to find a user.
4. In the Search for box, optionally type the user name.
5. Click Search
6. To modify a user, click the link in the Username table column.
7. Modify the parameters on the Base data, Password, Services, Links, Extended, and Actions tabs as required.
8. Click Save.
9. Click Save.

Listing and modifying subscribers job aid

About this task
This job aid describes the parameters for the Base data tab in the User Details portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>User name of the user. Avaya recommends that you use lowercase. Does not have to be the same name as the First Name.</td>
</tr>
<tr>
<td>Important:</td>
<td>For the Commercial Cost Avoidance (CCA) feature to work properly, configure the private number for this parameter (for example, 997261135).</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Parameter</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td></td>
<td>Remember, a user name can only contain letters, numbers, and specific symbols: • Letters: a to z, A to Z • Numbers: 0 to 9 • Symbols: period (.), hyphen (-) and underscore (_) Type: String (60) Range: Up to 60 characters Default: N/A</td>
</tr>
<tr>
<td>Password</td>
<td>Password of the user. Must match the password policy of the domain. Type: String (20) Range: Up to 20 characters Default: N/A</td>
</tr>
<tr>
<td>Confirm Password</td>
<td>Password of the user. Type: String (20) Range: Up to 20 characters Default: N/A</td>
</tr>
<tr>
<td>Service set</td>
<td>The list of service sets assigned to the user's domain or subdomain. Type: Select from list Range: N/A Default: N/A</td>
</tr>
<tr>
<td>Status Reason</td>
<td>The status value of the user. Type: Select from list Range: N/A Default: N/A</td>
</tr>
<tr>
<td>Location</td>
<td>The location where the user resides. Type: Select from list Range: Up to 30 characters Default: Use Domain Default &quot;Other&quot;</td>
</tr>
<tr>
<td>First Name</td>
<td>First name of the user. Case sensitive. The first name combines with the Last Name to form the display name on IP Deskphones. You must enter either a First Name, a Last Name, or both. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Name</td>
<td>Last name of the user. Case sensitive. The last name combines with the First Name to form the display name on IP Deskphones. You must enter either a First Name, a Last Name, or both. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
<tr>
<td>Email</td>
<td>Email address of the user. Type: String (60) Range: Up to 60 characters Default: N/A</td>
</tr>
<tr>
<td>Business phone</td>
<td>Business phone number. Type: String (60) Range: Up to 60 characters Default: N/A</td>
</tr>
<tr>
<td>Home phone</td>
<td>Home phone number. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
<tr>
<td>Cell phone</td>
<td>Cell phone number (Cellular DN) which acts as a routing alias for the subscriber. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
<tr>
<td>Pager</td>
<td>Pager number of the user. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
<tr>
<td>Fax</td>
<td>Fax number of the user. Type: String (30) Range: Up to 30 characters Default: N/A</td>
</tr>
<tr>
<td>Time Zone</td>
<td>The time zone to which the user belongs. Type: Select from list Range: N/A</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Default: N/A</td>
<td></td>
</tr>
<tr>
<td>Locale</td>
<td>Locale of the user. Type: Select from list Range: N/A Default: N/A</td>
</tr>
<tr>
<td>Common Names</td>
<td>The common names assigned to the user. When <strong>SIP TLS Identity Checking</strong> is enabled, the common names in this field are compared with the common name in the X.509 client certificate for the SIP TLS connections. Type: String Range: Up to 64 characters for Common Name. Up to 5 Common Names (one per line) Default: N/A</td>
</tr>
<tr>
<td>Password Policy</td>
<td>On this tab, enter a value in the Maximum Password Life field to override the system Password Policy for Maximum Password Life. Leave blank to use the system value. All other fields are read-only.</td>
</tr>
</tbody>
</table>

### Listing and deleting inactive subscribers

**About this task**

Use this procedure to list and delete inactive subscribers.

**Procedure**

1. From the Provisioning Client menu bar, select **User > Search**.
2. Select the **Advanced Search** tab.
3. In the **Domain** field list, select the domain.
4. In the **Search by** field list, select **Status**.
5. In the **Status list** select **Inactive**.
6. Click **Search**. The list of search results displays up to 1000 inactive subscribers.
7. To delete a user, click the link in the **Username** table column.
8. On the **Action** menu, click **Delete**.
9. Click **Save**.
Changing user password

About this task
Use this procedure to change the password of a user.

Procedure
1. From the Provisioning Client menu bar, select User > Search.
2. Select the type of search to perform.
   • Perform a basic search, select the Search tab,
   • Perform an advanced search, select the Advanced Search tab.
3. Configure the search parameters.
   • If you selected to perform a basic search:
     - Type the name of the user in the Select user field.
   • If you selected to perform an advanced search:
     - In the Domain field list, select the domain.
     - In the Search by field list, select the search criteria you want to use to find a user.
     - In the Search for box, type the user name. You can also leave this field blank.
4. Click Search.
5. Click the link for the user in the Username field.
6. On the User Details page, select the Password tab.
7. In the New Password box, type a new password.
8. In the Confirm password box, type the new password again.
9. Click Save.

Assigning services to a user

About this task
Use this procedure to assign services to a user.

Procedure
1. From the Provisioning Client menu bar, select User > Search.
2. Select the type of search to perform.
   • Perform a basic search, select the Search tab,
   • Perform an advanced search, select the Advanced Search tab.
3. Configure the search parameters.
   • If you selected to perform a basic search:
     - Type the name of the user in the Select user field.
   • If you selected to perform an advanced search:
     - In the Domain field list, select the domain.
     - In the Search by field list, select the search criteria you want to use to find a user.
     - In the Search for box, type the user name. You can also leave this field blank.

4. Click Search.

5. Click the link for the user in the Username field.

6. From the User Details page of the User portlet, select the Services tab.

7. Check the Assign all services box if you want to assign all services to the user.

8. Configure services for the user.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable a service for the user</td>
<td>Select the corresponding check box.</td>
</tr>
<tr>
<td>Disable a service for the user</td>
<td>Clear the corresponding check box.</td>
</tr>
</tbody>
</table>

9. Click Save.

---

**Using the Actions tab to modify a user**

**About this task**

On the Action tab in a User Details page, you can:

- log off the user’s registered contacts
- clear lockout for a user
- access the user’s Personal Agent

**Procedure**

1. From the Provisioning Client menu bar, select User > Search.

2. Select the type of search to perform.
   • Perform a basic search, select the Search tab,
   • Perform an advanced search, select the Advanced Search tab.

3. Configure the search parameters.
   • If you selected to perform a basic search:
     - Type the name of the user in the Select user field.
• If you selected to perform an advanced search:
  - In the **Domain** field list, select the domain.
  - In the **Search by** field list, select the search criteria you want to use to find a user.
  - In the **Search for** box, type the user name. You can also leave this field blank.

4. Click **Search**.
5. Click the link for the user in the Username field.
6. From the User Details page of the **User** portlet, select the **Actions** tab.
7. To log off the user’s registered contacts, click **Logout Contacts**.
8. Enter a valid administrator password in the confirmation window to log out contacts.
9. To clear lockout for the user, click **Clear lockout**.
10. To access the Personal Agent, click **Personal Agent**.

---

**Configuring the Personal Agent on behalf of a user**

**About this task**

An administrator can access the Personal Agent on behalf of a user by overriding the user password.

⚠️ **Important:**

After an administrator accesses the Personal Agent of a user, the system is preconfigured to time out. The time-out interval is defined by a value in the engineering parameter of the Personal Agent.

**Procedure**

1. From the Provisioning Client menu bar, select **User > Search**.
2. Select the type of search to perform.
   • Perform a basic search, select the **Search** tab,
   • Perform an advanced search, select the **Advanced Search** tab.
3. Configure the search parameters.
   • If you selected to perform a basic search:
     - Type the name of the user in the Select user field.
   • If you selected to perform an advanced search:
     - In the **Domain** field list, select the domain.
     - In the **Search by** field list, select the search criteria you want to use to find a user.
     - In the **Search for** box, type the user name. You can also leave this field blank.
4. Click **Search**.
5. Click the link for the user in the **Username** field.
6. From the User Details page of the **User** portlet, select the **Actions** tab.
7. Click **Personal Agent**.
   The Personal Agent opens in a browser, at which time the administrator is logged on automatically.

   **Important:**
   Only one Personal Agent logon is supported at a time. If an administrator logs on to a second Personal Agent account, a new Personal Agent window opens in the same browser window.

8. Make the required configuration changes.
   The administrator has the same privileges as a user and can perform any operation, including deletion of a route.

---

## Adding aliases and directory numbers for a user

**About this task**

Use this procedure to add aliases and directory numbers for a user. For the Commercial Cost Avoidance (CCA) feature to work, you must configure the alias for users.

**Procedure**

1. From the Provisioning Client menu bar, select **User > Search**.
2. Select the type of search to perform.
   - Perform a basic search, select the **Search** tab,
   - Perform an advanced search, select the **Advanced Search** tab.
3. Configure the search parameters.
   - If you selected to perform a basic search:
     - Type the name of the user in the Select user field.
   - If you selected to perform an advanced search:
     - In the **Domain** field list, select the domain.
     - In the **Search by** field list, select the search criteria you want to use to find a user.
     - In the **Search for** box, type the user name. You can also leave this field blank.
4. Click **Search**.
5. If you used the **Advanced Search** tab, click the link for the user in the **Username** field.
6. On the User Details page of the User portlet, select the Extended data tab.
7. In the Aliases box, type the alias for the user.
8. In the Directory number box, type the directory number associated with the user.
9. Click Save.

---

### Adding aliases and directory numbers of a user job aid

**About this task**

This job aid describes the parameters for the Extended data tab in the User Details portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Aliases           | The list of aliases for the user. Aliases associate a PSTN phone number with a username.  
                  | **Important:** For the Commercial Cost Avoidance (CCA) feature to work, you must specify the fully qualified international public number (for example, 17181234567) for this parameter. Aliases of an Equal Access user must be defined with his or her 18-digit equal access prefixes.  
                  | Type: String (40)  
                  | Range: N/A  
                  | Default: N/A |
| Directory Number  | The number that identifies a communication server user. The system uses the directory number for call termination attempts. The directory number of the user must be unique in the whole system.  
                  | Type: Number  
                  | Range: Up to 64 characters  
                  | Default: N/A |

---

### Moving subscribers between domains

Use this procedure to move subscribers from one domain to another.

**Before you begin**

- You have domain management rights.
- All user data (for example, services or profiles) assigned to the user to be moved, is already assigned to the destination domain.
Procedure

1. From the Provisioning Client menu bar, select **User > Search** to access the User portlet.
2. Select the **Advanced Search** tab.
3. From the **Domain** list, select the domain for the user.
4. From the **Search by** list, select the search criteria.
5. **(Optional)** In the **Search for** box, type the search string.
6. Click **Search**.
7. To copy a single user, or multiple users, select the corresponding check box for each user.
   
   **OR**
   
   To copy all users, select the **Select** check box.
8. From the **Action** list, select **Move user(s)** and click **>>**.
9. On the **Move user(s)** tab, from the **To domain** list, select the destination domain.
10. In the **New password** box, type a new password for the users.
11. In the **Confirm password** box, type the password for the users again.
12. Click **Save**.

---

**Moving subscribers between domains job aid**

The following points apply to the procedure to move a subscriber to a new domain or enclave:

- The move operation fails if the destination domain (To domain) does not have all of the user's data assigned to it. For example, you want to move a user from domainA to domainB. If the user has profileA assigned to him, the move fails if profileA is not assigned to domainB. The same rule applies to any service or profile assigned to the user.
- The move operation fails if any of the unique information is already in use in the destination domain. The data that falls into this category includes the username, alias, converged alias, directory number, voicemail id, SIP end point ID and any other data that must be unique in a domain.
- The move operation adds the user to the destination domain and deletes the user from the source (From domain). If the move tool cannot delete the user from the source domain, the move operation fails.
- For multisite domains, a move operation fails if the configured SLR LDAP server is down.
- After you move a user (from one domain to another, or within the same domain), the user must log off and log on with the new credentials, to receive calls.
- If a same root domain move fails (for example, the operation to add a user to the destination subdomain fails) the operation adds the user to the source subdomain (From subdomain). Therefore, like a new user, the user must log off and back on to receive calls. This is the standard behavior for calls and other services. If you delete and then add back this same user,
the user must log off and back on to receive calls. If the user does not log out, they can still originate calls, and send Instant Messages, but cannot receive anything.

• After you move a user who is assigned the Meetme Service and Meetme ChairPin or the Unified Communications Service and Unified Communications Pin, you must regenerate the PIN for the user in the destination domain.

• After you move a user of voicemail or unified communications capabilities, you must assign to the user, a voicemail server that is hosted on the target domain. Ideally, the host for that server has an address that identifies the target domain.

• When you move a user between domains, the user’s password history is preserved.
Chapter 18: Avaya Media Server application management procedures

About this task
Use the procedures in this chapter to locate Avaya Media Server Meet Me users and conferences.

- You must belong to the Meet Me Operator role.

For more information about Application Server 5300 Administrator roles, see Understanding provisioning roles and rights on page 25.

Navigation

- Finding a Meet Me user by access code on page 310
- Finding an active Meet Me conference by access code on page 311
- Finding an active Meet Me conference by domain on page 311

Finding a Meet Me user by access code

About this task
Use the following procedure to locate a particular Meet Me user by access code.

Procedure
1. From the Provisioning Client menu bar, choose Services > Conferencing > Meet Me Conferencing.
2. Select the Lookup Users tab.
3. Type the access code for the user and then click Search.

If you leave the Access Code blank, the search returns all users. Enter a string (for example, 445) to locate all matching users.
Finding an active Meet Me conference by access code

About this task
Use the following procedure to locate a particular Meet Me conference by access code.

Procedure
1. From the Provisioning Client menu bar, choose Services > Conferencing > Meet Me Conferencing.
2. Select the Active Conferences tab.
3. From the Search by list, select Access Code.
4. Type the access code for the user, and then click Search.
   If you leave the Access Code blank, the search returns all users. Enter a string (for example, 445) to locate all matching users.

Finding an active Meet Me conference by domain

About this task
Use the following procedure to locate a particular Meet Me conference by domain.

Procedure
1. From the Provisioning Client menu bar, choose Services > Conferencing > Meet Me Conferencing.
2. Select the Active Conferences tab.
3. From the Search by list, select Domain Name.
4. Type the name for the domain, and then click Search.
Chapter 19: Translations configuration procedures

About this task
Use the procedures in this section to configure translations.

- Configuring telephony routes class of service information on page 312
- Adding a telephony route on page 313
- Listing a telephony route on page 315
- Adding a route list on page 315
- Listing, modifying, and deleting a route list on page 316
- Assigning a number qualifier for a domain on page 317
- Using the Translation Tool on page 317
- Assigning pretranslations for a domain on page 318

For more information and examples about telephony routing and translation plans, see Provisioning for telephony routing and translations on page 65.

Telephony route configuration
Use the procedures in this section to configure telephony routes for translations.

Configuring telephony routes class of service information

About this task
Class of Service (COS) is assigned to users, domains, and routing lists. It is an integer value, and the lower the number, the greater, or higher, the COS value. For example, if a user has a COS value of 1, and a route list has a COS of 3, then the user with a COS of 1 can use all the routes in that route list (that is, the user has a higher COS). The lower the number, the higher the access to making calls.

Adding a COS to gateway translations allows the administrator to control which user can make calls through which gateway and to control the dialing plans allowed.

Use this procedure to add COS information.
Procedure
1. From the Provisioning Client menu bar, select Translations > Class of Service to access the Class of Service portlet.
2. In the Class of Service portlet, select the Domain tab.
3. In the Select domain field, select the domain for which you want to add COS information, and click >>.
4. In the Class of service name field, enter the name for the COS.
5. In the Class of service description field, enter a description for the COS.
6. Click Save.
7. Use the corresponding UP and DOWN links to change the order of appearance in the table that lists existing COS entries.
8. To delete a COS from the table, click Delete for that entry.

Adding a telephony route

About this task
Use this procedure to add Private, SIP or Gateway telephony routes on the system.
Configure the telephony routes table to remove the access and service digits and route to the appropriate gateway. If the gateway route terminates to the local PSTN gateway, configure the gateway route type as public.

Procedure
1. From the Provisioning Client menu bar, select Translations > Telephony Routes.
2. In the Telephony Route portlet, select the tab associated with the type of route that you want to add.
3. In the Select domain box, type the name of the domain for which you want to add a new telephony route, and then click >>.
4. Configure the telephony route parameters as required.
5. Click Save.

Adding a telephony route job aid

About this task
This job aid describes the parameters on the tabs of the Telephony Route page.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>A description of the route. Range: 0–100</td>
</tr>
</tbody>
</table>

Table continues…
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>From Digit</td>
<td>Digits on which translation is carried out and should be the same as To Digits. Range: 0–20</td>
</tr>
<tr>
<td>Gateway route</td>
<td></td>
</tr>
<tr>
<td>Gateway route type</td>
<td></td>
</tr>
<tr>
<td>Interop profile</td>
<td></td>
</tr>
<tr>
<td>Max Number of Digit</td>
<td>Maximum number of digits that translation will be performed on. Should be the same as Min Digits</td>
</tr>
<tr>
<td>Min Number of Digit</td>
<td>Minimum number of digits that translation will be performed on. Should be the same as Max Digits</td>
</tr>
<tr>
<td>Name</td>
<td>The name of the route. Range: 0-120</td>
</tr>
<tr>
<td>Number qualifier</td>
<td></td>
</tr>
<tr>
<td>Off Net</td>
<td></td>
</tr>
<tr>
<td>Override charge ID</td>
<td></td>
</tr>
<tr>
<td>Override charge value</td>
<td></td>
</tr>
<tr>
<td>Override name value</td>
<td></td>
</tr>
<tr>
<td>Prefix</td>
<td>The digits to prefix the dialed digits, if any.</td>
</tr>
<tr>
<td>Recursive</td>
<td>Select from the list: yes or no.</td>
</tr>
<tr>
<td>Remove</td>
<td>The number of digits, if any, to remove during translation.</td>
</tr>
<tr>
<td>Route List</td>
<td>The list of routes.</td>
</tr>
<tr>
<td>Route Type</td>
<td>Select route type from the list: Private, SIP, or Gateway</td>
</tr>
<tr>
<td>SIP route</td>
<td></td>
</tr>
<tr>
<td>SIP route type</td>
<td></td>
</tr>
<tr>
<td>Subscriber not found</td>
<td></td>
</tr>
<tr>
<td>To Digit</td>
<td>Digits on which translation is carried out and should be the same as From Digits. Range: 0–20</td>
</tr>
</tbody>
</table>

**Recommended telephony route entries**

This job aid provides the recommended entries for telephony routes that process the service digit.

<table>
<thead>
<tr>
<th>From Digit</th>
<th>To Digit</th>
<th>Number of Digits</th>
<th>Route Type</th>
<th>Remove</th>
<th>Gateway Route</th>
<th>Gateway Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>95</td>
<td>95</td>
<td>9</td>
<td>Gateway</td>
<td>2</td>
<td>Off-net 700</td>
<td>Private</td>
</tr>
<tr>
<td>97</td>
<td>97</td>
<td>9</td>
<td>Gateway</td>
<td>2</td>
<td>DSN CONUS</td>
<td>Private</td>
</tr>
<tr>
<td>99</td>
<td>99</td>
<td>9</td>
<td>Gateway</td>
<td>2</td>
<td>Local public telephone</td>
<td>Public</td>
</tr>
<tr>
<td>95</td>
<td>95</td>
<td>12</td>
<td>Gateway</td>
<td>2</td>
<td>Off-net 700</td>
<td>Private</td>
</tr>
<tr>
<td>97</td>
<td>97</td>
<td>12</td>
<td>Gateway</td>
<td>2</td>
<td>DSN CONUS</td>
<td>Private</td>
</tr>
<tr>
<td>99</td>
<td>99</td>
<td>12</td>
<td>Gateway</td>
<td>2</td>
<td>Local public telephone</td>
<td>Public</td>
</tr>
</tbody>
</table>
Listing a telephony route

About this task
Use this procedure to view details about a telephony route.

Procedure
1. From the Provisioning Client menu bar, select Translations > Telephony Routes.
2. In the Telephony Route portlet, select the tab associated with the type of route that you want to list.
3. From the Select domain list, select a domain where you want to view telephony route details and click >>.

Adding a route list

Use this procedure to add a route list.

Before you begin
• Ensure that Class of Service (COS) information is defined.

Procedure
1. From the Provisioning Client menu bar, select Translations > Telephony Routes to access the Telephony Route portlet.
2. In the Telephony Route portlet, select the Add New Route List tab.
3. From the Select domain list, select the name of the domain for which you want to add a new telephony route list, and click >>.
4. Configure the telephony route parameters as required.
5. In the Available Telephony route(s) window, select the routes to add to the list.

<table>
<thead>
<tr>
<th>To</th>
<th>Do this</th>
</tr>
</thead>
<tbody>
<tr>
<td>Add selected routes</td>
<td>Click Copy.</td>
</tr>
<tr>
<td>Add all of the routes</td>
<td>Click Copy all.</td>
</tr>
</tbody>
</table>

6. Click Save.
Adding a route list job aid

About this task

This job aid describes the parameters for the Add New Route List tab in the Telephony Route portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>A unique name to identify the route list.</td>
</tr>
<tr>
<td>Description</td>
<td>A description for the route list. Range: Up to 50 characters.</td>
</tr>
<tr>
<td>Incoming Other Domain Tree Call Routing</td>
<td>Specify how the system handles calls from foreign domains. Select from the list: ALLOW, BLOCK, or REDIRECT.</td>
</tr>
<tr>
<td>Incoming Same Domain Tree Call Routing</td>
<td>Specify how the system handles calls from local domains. Select from the list: ALLOW, BLOCK, or REDIRECT.</td>
</tr>
<tr>
<td>Class of Service</td>
<td>Specify the Class of Service. Select from the list: Gold, Silver, or Bronze.</td>
</tr>
<tr>
<td>Telephony Route(s)</td>
<td>Select the routes to include.</td>
</tr>
</tbody>
</table>

Listing, modifying, and deleting a route list

About this task

Use this procedure to view details about a route list. You can also modify or delete a route list.

Procedure

1. From the Provisioning Client menu bar, select Translations > Telephony Routes to access the Telephony Route portlet.
2. In the Telephony Route portlet, select the List RouteLists tab.
3. From the Select domain list, select a domain for which you want to view route list details and click >>.
4. In the route list that appears, click the link for the route list to modify.
5. Modify route list information and click Save.
6. To delete an existing route list, click the Delete link in the Delete column of the row containing the route list you want to delete.
7. In the pop-up that appears, click Confirm to proceed with the deletion.
Assigning a number qualifier for a domain

About this task
Use this procedure to assign a number qualifier for a domain.

Procedure
1. From the Provisioning Client menu bar, select Translations > Number Qualifiers.
2. In the Number Qualifier portlet, from the Select domain list, select a domain to which you want to assign a number qualifier, and then click > >.
3. In the Number Qualifier portlet, configure the parameters as required.
4. Click Save.

Assigning a number qualifier job aid
This job aid describes the parameters for the Number Qualifier tab in the Number Qualifier portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone context</td>
<td>Provide a phone context. It should match the type of number you select for the TON field.</td>
</tr>
<tr>
<td>NPI</td>
<td>Select the Numbering Plan Identifier (NPI) from the list.</td>
</tr>
<tr>
<td>TON</td>
<td>Select the Type of Number (TON) from the list.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description for the number qualifier. For example, if you selected NPI as public and TON as national, the description can be NPI=public, TON=National</td>
</tr>
</tbody>
</table>

Using the Translation Tool

About this task
Use this procedure to use the translation verification tool.

The translation tool allows you to verify that a call is provisioned correctly.

Procedure
1. From the Provisioning Client menu bar, select Translations > Translation Tool.
2. In the Translation Tool portlet, configure the parameter information and values for Translation Tool and then click > >.
Using the Translation Tool job aid

This job aid describes the data for the **Translation Tool** tab in the Translation Tool portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request URI</td>
<td>In this field, enter a number to call using the following format: <code>&lt;number&gt;@&lt;domain_or_subdomain_name&gt;.com</code></td>
</tr>
<tr>
<td>TO</td>
<td>In this field, enter the same name as in the Request URL field, or leave blank.</td>
</tr>
<tr>
<td>From</td>
<td>In this field, enter the number of the caller using one of the following formats: <code>&lt;name&gt;@&lt;domain_or_subdomain_name&gt;.com&lt;number&gt;@&lt;domain_or_subdomain_name&gt;.com</code></td>
</tr>
</tbody>
</table>

Assigning pretranslations for a domain

**About this task**

Use this procedure to assign pretranslations for a domain.

**Procedure**

1. From the Provisioning Client menu bar, select **Translations > Pretranslations** to access the Pre Translation portlet.
2. In the **Select domain** field of the Pre Translation portlet, select a domain where you want to assign pretranslations and click `>>`.
3. In the Pre Translation portlet, enter the parameter information and values for Pretranslations.
4. Click `Save`.

Assigning pretranslations for a domain job aid

This job aid describes the data for the **Pre Translations** tab in the Pre Translation portlet.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Number Qualifier</td>
<td>Select the number qualifier from the list.</td>
</tr>
<tr>
<td>Length</td>
<td>Specify the length of the number qualifier.</td>
</tr>
<tr>
<td>Prefix</td>
<td>Specify the prefix. This is the number that would be prefixed to the number coming in for translation.</td>
</tr>
</tbody>
</table>
Chapter 20: Time zone management procedures

About this task
Use the procedures in this section to add, select, modify, and delete time zones.

- Creating a new time zone on page 319
- Selecting a time zone on page 319
- Modifying or deleting a time zone on page 321

Creating a new time zone

About this task
Use this procedure to create a new time zone.

Procedure
1. From the Provisioning Client menu bar, select System > Timezone to access the Time Zone portlet.
2. In the Name box, type a meaningful name for the time zone.
   (This field is visible to subscribers.) Both the name and the time zone must be unique.
3. From the Select time zone list, select a time zone.
4. Click Save.

Selecting a time zone

About this task
Use this procedure to select a time zone.

Procedure
1. From the Provisioning Client menu bar, select System > Timezone.
2. In the Time Zone portlet, from the list, select a time zone.
3. Click **Save**.

---

**Selecting a time zone job aid**

The Provisioning Client allows you to define and manage as many time zones as you require to meet your needs and to create your own time zones for easy reference. Time zones define the time zone from which a subscriber normally accesses the system (that is, the subscribers's local time zone). Time zones are used in the Avaya Aura® Application Server 5300 Personal Agent Call Manager function to set a screening rule that applies during a certain time. This time is dependent on the time zone selected.

Make certain that for time zones with matching language (for example, French), an in-French time zone must be created, even though it is the same time zone as in English. User Locale does not accommodate language differences for time zones.

The Provisioning Client is initially set up with the standard 24 time zones, plus or minus 12 hours from the Greenwich Mean Time (GMT) format. However, there are more than 300+ time zones. What defines a time zone is not just the offset from the GMT. It is also whether or not the time zone uses Daylight Saving Time, when Daylight Saving Time occurs, and what the offset is.

---

**Configuring times zones in the United States**

**About this task**

As an example, the time zones you would configure across the United States from East to West are listed in the following table:

**Table 19: Time zones**

<table>
<thead>
<tr>
<th>Zone</th>
<th>Standard Time</th>
<th>Daylight Saving Time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Atlantic</td>
<td>AST</td>
<td>ADT</td>
</tr>
<tr>
<td>Eastern</td>
<td>EST</td>
<td>EDT</td>
</tr>
<tr>
<td>Central</td>
<td>CST</td>
<td>CDT</td>
</tr>
<tr>
<td>Mountain</td>
<td>MST</td>
<td>MDT</td>
</tr>
<tr>
<td>Pacific</td>
<td>PST</td>
<td>PDT</td>
</tr>
<tr>
<td>Alaska</td>
<td>AKST</td>
<td>AKDT</td>
</tr>
<tr>
<td>Hawaii</td>
<td>HST</td>
<td>Not Observed</td>
</tr>
</tbody>
</table>
Modifying or deleting a time zone

About this task
Use this procedure to modify or delete a time zone.

The Provisioning Client is preloaded with a number of default time zones. You may want to modify or delete a time zone to prevent the time zone from showing up in the list that is available when creating or modifying a user.

Procedure

1. From the Provisioning Client menu bar, select System > Timezone to access the Time Zone portlet.
2. On the Time Zone tab, in the time zone list, click the name of the time zone that you want to modify.
3. In the Name box, type a meaningful name for the time zone.
   (This field is visible to subscribers.) Both the name and the time zone must be unique.
4. In the Select time zone field, select a time zone.
5. Click Save.
6. To delete a time zone, click the Delete link next to any time zone that you do not need.

   Important:
   You cannot modify or delete a time zone that is currently in use.

7. Enter your administrator password in the confirmation dialog to permanently delete the time zone.
Chapter 21: Example of Configuring the Presence service

The following procedure provides an overview of how to provision a service, by using the Presence service as an example.

⚠️ Important:
Clients do not receive notification about changes to their service sets. Any changes (such as Presence preferences) take effect after the next log on.

📌 Note:
Disabling the XMPP gateway service for a user will delete XMPP User Profile of the user. When re-enabling the XMPP User Profile for a user, XMPP User Profile for the user must also be re-configured. For more information on configuring the XMPP User Profile, see XMPP Gateway service configuration on page 292.

Before you begin
• You have Services provisioning rights.
• You can access the Provisioning Client. For more information, see Starting the Provisioning Client on page 79.
• The domain to which you want to assign the service already exists. For more information, see Domain management procedures on page 88.
• The users to whom you want to assign the service already exist and have configured service sets. For more information, see Subscriber management procedures on page 295 and Service set procedures on page 180.

Procedure
1. From the Provisioning Client menu bar, select Domain > Domain Steps > Assign Resources to access the Resource Management portlet.
2. On the Domain resources tab, from the Select domain list, select an existing domain and click >>.
3. In the Assign column, Presence subscribers row, assign the required number of units.

⚠️ Important:
The Presence service is tagged as a resource; there is a limit on the number of units for the service that can be assigned to the domain.
4. Click **Save**.
   The units requested are validated against the remaining units for that resource in the system. The system saves the allocations if the validation passes.

5. From the Provisioning Client menu bar, select **Domain > Domain Steps > Assign Services** to access the User Services portlet.

6. On the **Services** tab, click **Presence**.

7. On the **System Profile** tab of the Presence Service portlet, click **Assign/Remove** for the profile in the **Domain** table column.

8. From the **Available Domains** list, select the domain to which you want to assign the profile.

9. Click **Copy**.

10. Click **Save**.

11. From the Provisioning Client menu bar, select **Services > Service Set** to access the Service Set portal.

12. On the **List** tab, from the **Select domain** list, choose a domain and click **>>**.

13. In the **Name** column of the table, click the service set that you want to modify.

14. Select the **Presence** service.

15. From the list, select the system profile for the **Presence** service.

16. Click **Save**.

17. From the Provisioning Client menu bar, select **Services > Presence** to access the Presence Service portlet.

   The Presence Service portlet controls all the service data for the Presence service. The **System Profile** tab is the default selection, and is used for creating, modifying, or deleting service profiles for the service.

18. On the **System Profile** tab, configure the **Profile name**, **Maximum friends list**, **Report when inactive**, **Inactivity timer**, and **Report when on the phone** parameters on the tab.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profile name</td>
<td>Type a profile name for this service.</td>
</tr>
<tr>
<td>Maximum friends list</td>
<td>Specifies the number of people in a list of friends. A user can subscribe up to 100 people to view their presence. Although users can log on to numerous devices, the list of friends is a shared resource. For example, if the maximum list of friends size is configured to 10, then each of the client devices can hold 10 friends (the same 10 friends, not 10 per device). The client has the option of sending Presence status to any of the friends.</td>
</tr>
<tr>
<td>Report when inactive</td>
<td>Enables the autopresence (optional) feature that detects when a PC is not in use and updates their Presence status on the network.</td>
</tr>
</tbody>
</table>
Example of Configuring the Presence service

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Inactivity timer</td>
<td>Determines the length of time a user’s PC must be idle before their Presence status is updated on the network.</td>
</tr>
<tr>
<td>Report when on the phone</td>
<td>Detects when a user is on an active call and updates the user’s Presence status on the network.</td>
</tr>
</tbody>
</table>

19. Click **Save**.

20. On the **Domain Data** tab, from the **Select domain** list, choose a domain and click **>>**

21. Configure the maximum number of presence subscriptions and then click **Save**.

22. On the **User Data** tab, in the **Select user (user@domain)** box, type the name of a user (in the @domain format), and then click **>>**.

23. From the **User's system profile** list, select the system profile for the user and click **Save**.

24. In the **User profile** section, configure the **Report when inactive**, **Inactivity timer**, and **Report when on the phone** parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report when inactive</td>
<td>Enables the autopresence (optional) feature that detects when a PC is not in use and updates their Presence status on the network.</td>
</tr>
<tr>
<td>Inactivity timer</td>
<td>Determines the length of time a user’s PC must be idle before their Presence status is updated on the network.</td>
</tr>
<tr>
<td>Report when on the phone</td>
<td>Detects when a user is on an active call and updates the user’s Presence status on the network.</td>
</tr>
</tbody>
</table>

25. Click **Save**.
Chapter 22: World Wide Numbering and Dial Plan reference

About this task

This section explains the World Wide Numbering and Dialing Plan (WWNDP), defines associated terminology, and provides configuration recommendations.

🚨 Important:

The sample and recommended telephony route entries tables assume the use of 9 for the access digit.

- Digit format on page 325
- Four-digit dialing on page 327
- Seven-digit dialing on page 328
- 10-digit dialing on page 328
- PSTN dialing from within DSN on page 328
- Class of Service on page 329

Digit format

The Application Server 5300 requires the world wide number dialing plan (WWNDP) within the userinfo of the SIP URL:

```
INVITE sips:<userinfo>@<hostname>
```

| <userinfo> | This value is a SIP alias or a world wide number. |
| <hostname> | This value is the domain on which the terminator is homed. |

For dialed digits, the userinfo must be in WWNDP format to prevent E.164 and WWNDP overlap. Users can have a SIP alias and must have a 10–digit numeric alias, which identifies the users area code, switch code, and line number.
Table 20: WWNDP digit format

<table>
<thead>
<tr>
<th>Access code</th>
<th>Route code</th>
<th>Area code</th>
<th>Switch code</th>
<th>Line number</th>
</tr>
</thead>
<tbody>
<tr>
<td>(N P or S)</td>
<td>(1X)</td>
<td>(KXX)</td>
<td>KXX</td>
<td>XXXX</td>
</tr>
</tbody>
</table>

N = Access digit—any digit 2–9
P = Precedence digit—any digit 0–4
S = Service digit—any digit 5–9
X = Any digit 0–9
K = Any digit 2–8

Items enclosed in brackets () have default values and are not always dialed.

**Access code**

The access code consists of the access digit, followed by either the precedence or service digit. The access digit provides the indication to the switch that the following digit is a precedence or service digit. Avaya recommends that you configure 9 as the access digit.

**Precedence digit**

With the precedence digit, users can dial an authorized precedence level. The precedence digit must follow the access digit.

The originating switch performs the authorization of the precedence digits and generation of the SIP resource-priority header because the originating switch can determine the homed user’s maximum authorized precedence value.

**Table 21: Precedence digit to SIP resource-priority r-value mapping**

<table>
<thead>
<tr>
<th>Precedence digit</th>
<th>Precedence level</th>
<th>SIP resource-priority r-value</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>Flash Override</td>
<td>uc-000000.8</td>
</tr>
<tr>
<td>1</td>
<td>Flash</td>
<td>uc-000000.6</td>
</tr>
<tr>
<td>2</td>
<td>Immediate</td>
<td>uc-000000.4</td>
</tr>
<tr>
<td>3</td>
<td>Priority</td>
<td>uc-000000.2</td>
</tr>
<tr>
<td>4</td>
<td>Routine</td>
<td>uc-000000.0</td>
</tr>
</tbody>
</table>

After the precedence level is determined, the system authenticates the requester and determines whether the requester is authorized to employ the precedence level. After authorization the system forwards the SIP message with the generated SIP ‘resource-priority’ header. If the requestor is not authorized to use the requested precedence level, the call terminates with unauthorized precedence announcements (UPA).

The following rules apply to precedence:

- Ingress calls from the PRI Gateway do not have the precedence digit. The originating switch removes the precedence digit and uses T1.619a to pass the precedence level through PRI and SIP messaging.
- If the system receives the precedence digit, and the originating user is not homed on the system, the call terminates with an unauthorized precedence announcements (UPA).
• If the system receives the precedence digit, and the SIP resource-priority header is present within the SIP request message, the highest precedence applies for the call. If the precedence digit has a higher precedence level, the system updates the SIP resource-priority header with the precedence digit-mapped value.

• If the system receives the precedence digit, but the MLPP user is not part of the DSN group, the system removes the access code and precedence digit, and the DSN SIP resource-priority header is not included. If the incoming SIP message includes the resource-priority option tag in the SIP requirement, the system rejects the request with a 417 (Unknown Resource-Priority).

• If the system receives the precedence digit, and the user does not have the MLPP service, the call bypasses the feature translation trigger table. The access code and precedence digit are included for terminating route determination.

**Service digit**

With the service digit, users can connect to other networks, such as government or public networks. The service digit must follow the access digit.

**Area code**

The area code indicates the geographical part of the world or tactical unit where the user is assigned. The area code is a 3-digit code (format KXX). The area code is required to address a user outside of the originator’s own numbering plan area. An Application Server 5300 for an enclave must reside in only one area code.

**Switch code**

The switch code indicates the location of a switching center within a numbering plan. The switch code is 3-digit code (format KXX). The switch code is required to address another switch in the same numbering plan area. A subdomain is expected must reside in only one switch center.

**Line number**

The line number is the switch-unique user station identification (format XXXX). You can configure the Application Server 5300 to support 4-digit dialing to address a user on the same switching center.

---

**Four-digit dialing**

With four-digit dialing, the user dials the four-digit line number. The Application Server 5300 appends the area code and switch code of the originator’s Application Server 5300 enclave to the four digits. This combination of area code, switch code, and the four-digit line number must match the terminator’s alias.

**Table 22: Telephony route entries for four-digit dialing**

<table>
<thead>
<tr>
<th>From digit</th>
<th>To digit</th>
<th>Number of digits</th>
<th>Prefix</th>
<th>Route type</th>
<th>Gateway route</th>
<th>Gateway type</th>
<th>Subscriber not found</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>9</td>
<td>4</td>
<td>(Area code) (Switch code)</td>
<td>Private</td>
<td></td>
<td></td>
<td>Pre-translate</td>
</tr>
</tbody>
</table>
Seven-digit dialing

With seven-digit dialing, the user dials the three-digit switch code and the four-digit line number. The Application Server 5300 appends the area code of the originator’s Application Server 5300 enclave to these seven digits. This combination of area code, switch code, and the four-digit line number can match the terminator’s alias, or be routed out the PRI Gateway.

Table 23: Telephony route entries for seven-digit dialing

<table>
<thead>
<tr>
<th>From digit</th>
<th>To digit</th>
<th>Number of digits</th>
<th>Prefix</th>
<th>Route type</th>
<th>Gateway route</th>
<th>Gateway type</th>
<th>Subscriber not found</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>8</td>
<td>7</td>
<td>(Area code)</td>
<td>Private</td>
<td></td>
<td></td>
<td>Pre-translate</td>
</tr>
</tbody>
</table>

10-digit dialing

With 10-digit dialing, the user dials the three-digit area code, the three-digit switch code, and the four-digit line number. This 10-digit number can match the terminator’s alias, or be routed out the PRI Gateway.

Table 24: Telephony route entries for 10-digit dialing

<table>
<thead>
<tr>
<th>From digit</th>
<th>To digit</th>
<th>Number of digits</th>
<th>Route type</th>
<th>Gateway route</th>
<th>Gateway type</th>
<th>Subscriber not found</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>(Area code)</td>
<td>10</td>
<td>Gateway</td>
<td>KXX Enclave</td>
<td>Private</td>
<td></td>
</tr>
<tr>
<td>(Switch code)</td>
<td>-1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>(Area code)</td>
<td>(Switch code)</td>
<td>10</td>
<td>Private</td>
<td></td>
<td></td>
<td>Block</td>
</tr>
<tr>
<td>(Switch code)</td>
<td>+1</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>(Area code)</td>
<td>10</td>
<td>Gateway</td>
<td>KXX Enclave</td>
<td>Private</td>
<td></td>
</tr>
<tr>
<td>(Switch code)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>0</td>
<td>8</td>
<td>10</td>
<td>Gateway</td>
<td>KXX Enclave</td>
<td>Private</td>
<td></td>
</tr>
</tbody>
</table>

⚠ Important:

The system performs the 10-digit subscriber lookup before routing to the KXX Enclave. If the area code and switch code matches the enclave, but the subscriber is not found, the system blocks the call with a vacant treatment.

PSTN dialing from within DSN

For PSTN dialing, the user must append the access digit and the Local PSTN service digit to the E. 164 number.
Table 25: Telephony route entries for PSTN dialing

<table>
<thead>
<tr>
<th>From digit</th>
<th>To digit</th>
<th>Number of digits</th>
<th>Route type</th>
<th>Remove</th>
<th>Gateway route</th>
<th>Gateway type</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>99</td>
<td>9</td>
<td>Gateway</td>
<td>2</td>
<td>Local public telephone</td>
<td>Public</td>
</tr>
<tr>
<td>99</td>
<td>99</td>
<td>12</td>
<td>Gateway</td>
<td>2</td>
<td>Local public telephone</td>
<td>Public</td>
</tr>
</tbody>
</table>

To specify a route code, the user must also append another two digits for the route code. An administrator must provision translation triggers for both Table 25: Telephony route entries for PSTN dialing on page 329 and Table 25: Telephony route entries for PSTN dialing on page 329.

Table 26: Telephony route entries for PSTN dialing with route codes

<table>
<thead>
<tr>
<th>From digit</th>
<th>To digit</th>
<th>Number of digits</th>
<th>Route type</th>
<th>Remove</th>
<th>Gateway route</th>
<th>Gateway type</th>
</tr>
</thead>
<tbody>
<tr>
<td>99</td>
<td>99</td>
<td>11</td>
<td>Gateway</td>
<td>2</td>
<td>Local public telephone</td>
<td>Public</td>
</tr>
<tr>
<td>99</td>
<td>99</td>
<td>14</td>
<td>Gateway</td>
<td>2</td>
<td>Local public telephone</td>
<td>Public</td>
</tr>
</tbody>
</table>

Class of Service

Incoming calls from the gateway must have a lower Class of Service (CoS) than calls that originate from the IP-PBX. Table 27: CoS entries for enclave routing on page 329 provides an example of CoS order.

Table 27: CoS entries for enclave routing

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Public routable</td>
</tr>
<tr>
<td>Inter-enclave</td>
<td>Inter-enclave routable</td>
</tr>
<tr>
<td>Enclave</td>
<td>Enclave routable</td>
</tr>
</tbody>
</table>

The following rules apply to CoS:

- The CoS assigned to the domain applies to calls received from the PRI gateway. Avaya recommends that you configure the COS for the domain as Enclave or lower.
- The CoS assigned to subscribers applies to subscriber-originated calls. Avaya recommends that you configure the COS for subscribers as Inter-enclave or higher.
- The telephony route list marks the COS against routes. A call must have a class of service equal to or greater than the class of service assigned to a route; otherwise, the system ignores the route. Avaya recommends the following route list entries.
### Table 28: Telephony route list entries for CoS

<table>
<thead>
<tr>
<th>Same domain</th>
<th>Other domain</th>
<th>CoS</th>
<th>Route name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Allow</td>
<td>Allow</td>
<td>Enclave</td>
<td>DSN 4-digit</td>
</tr>
<tr>
<td>Allow</td>
<td>Allow</td>
<td>Enclave</td>
<td>DSN 7-digit</td>
</tr>
<tr>
<td>Allow</td>
<td>Allow</td>
<td>Inter-enclave</td>
<td>Enclave GW</td>
</tr>
<tr>
<td>Allow</td>
<td>Allow</td>
<td>Public</td>
<td>Public GW</td>
</tr>
</tbody>
</table>

### Route Code Usage

The route code is a special purpose DSN code that allows the customer to inform the switch of special routing or termination requirements. According to the route codes, the system configures tgrp and trunk group parameters to the user portion of Request URI at origin.
## Index

### A
- Adding
  - call pickup feature translation triggers ........................................... 214
  - Call Pickup group members .............................................................. 212
- Administration
  - overview ............................................................................................ 78
- ANI ............................................................................................................ 224, 237
- Assigning
  - call pickup service ............................................................................... 210
  - group administrator for Call Pickup group ........................................ 213
  - session manager for call pickup service group ................................... 212

### C
- Call pickup ................................................................................................. 208
  - call pickup configuration
    - job aid ............................................................................................... 211
  - call pickup feature translation triggers
    - adding ................................................................................................... 214
  - call pickup feature translation triggers in a domain
    - job aid .................................................................................................. 214
  - call pickup group
    - modification .......................................................................................... 212
    - searching ............................................................................................... 212
  - Call pickup group
    - adding members .................................................................................. 212
  - call pickup group service to a domain
    - assigning ............................................................................................... 209
  - call pickup service
    - job aid .................................................................................................. 209
  - call pick up service assignment
    - job aid .................................................................................................. 210
  - call pickup service group
    - assigning session manager .................................................................. 212
    - configuring ............................................................................................. 211
  - call pickup service profile
    - configuring ............................................................................................. 208
  - Call pickup VSC ..................................................................................... 213
  - Call Pickup VSC ..................................................................................... 215
- Configuring
  - call pickup service group ..................................................................... 211
  - call pickup service profile ..................................................................... 208

### D
- Document changes ...................................................................................... 17
  - create a default location ......................................................................... 59
  - default ....................................................................................................... 36
  - foreign ....................................................................................................... 39
  - listing ......................................................................................................... 100
  - modifying .................................................................................................. 100

- Domain (continued)
  - modifying a default location .................................................................. 149
  - multisite .................................................................................................... 39
  - root ............................................................................................................ 38

### F
- Foreign domain
  - deleting .................................................................................................... 101
  - example .................................................................................................... 39
  - modifying .................................................................................................. 100

### G
- Gateway
  - CAS .......................................................................................................... 56

### I
- IM Chat
  - routable services .................................................................................... 228

### L
- LDAP
  - query test tool ....................................................................................... 53
  - schema config .......................................................................................... 50
  - syncing scheduler .................................................................................... 52
  - user defaults ............................................................................................. 52
  - Lightweight Directory Access Protocol see LDAP .................................... 47, 132
  - line-based voice mail server .................................................................... 286
  - location
    - add ......................................................................................................... 60
    - associate a user ..................................................................................... 60
    - modifying ............................................................................................... 151

### P
- Password
  - changing the admin ................................................................................ 81
  - complexity rules ...................................................................................... 33
- Password policy ........................................................................................... 41
- Prefix-based voice mail server
  - adding ...................................................................................................... 287
  - description ............................................................................................... 56
- Provisioning
  - creating a new role .................................................................................. 28
  - listing roles ............................................................................................... 32
  - provisioning rights
    - examples ............................................................................................... 25
    - understanding ......................................................................................... 25
# Index

### User Defaults
- LDAP: 52

### User Parameters
- Business Phone: 296, 299
- Cell Phone: 296, 299
- Confirm Password: 296, 299
- Email: 296, 299
- Fax: 296, 299
- First Name: 296, 299
- Home Phone: 296, 299
- Last Name: 296, 299
- Locale: 296, 299
- Pager: 296, 299
- Password: 296, 299
- Service Set: 296, 299
- Status Reason: 296, 299
- Time Zone: 296, 299
- User Name: 296, 299

### Time Zone
- Creating a New Time Zone: 319
- Deleting: 321
- Modifying: 321
- Overview: 320

### TR87: Assigning Resources for TR87
- Assigning TR87 Client Control to a Domain: 164
- Assigning TR87 Client Control to Users: 164
- Assigning TR87 Profile to a Domain: 162
- Configuring TR87 Client Control: 161
- Setting up the TR87 Client Control Profile: 163
- Setting up TR87 Client Control Profile: 162
- Translation Tool: 317
- Trunk-Based Voice Mail Server: 285

### SIP-Based Voice Mail Server
- Definition: 38
- Example: 38
- Modifying a Default Location: 150

### System Scheduler (LDAP)
- Assignment: 52

### Telephony Route
- Associating COS and the Route: 76
- Concepts
  - Class of Service (COS): 66
  - Subdomains: 65
- Definition: 312
- Dial Plan Description: 76
- Example Dial Plan Assignments: 76
- Listing a Route List: 316
- Modifying: 315
- Redirection Between Subdomains: 72
- Route Lists: 71
- Routes: 73
- Sample Dial Plan: 73
- Telephony Redirect Example: 72
- Terminology: 71

### Telephony Redirection Example
- Overview: 73

### Telephone Line
- Creating a New Time Zone: 319
- Deleting: 321
- Modifying: 321
- Overview: 320

### Unified Communications
- Routable Services: 279