



Administering Avaya Call Management System

Release 21.0.2
Issue 3
July 2025

Notices

© 2026 Avaya LLC. All Rights Reserved.

You may, at your own risk, assemble a MyDocs collection solely for your own internal business purposes, which constitutes a modification to the original published version of the publications. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of publications. You agree to defend, 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, your modifications, additions or deletions to the publications.

A single topic or a collection of topics may come from multiple Avaya publications. All of the content in your collection is subject to the legal notices and disclaimers in the publications from which you assembled the collection. For information on licenses and license types, trademarks, and regulatory statements, see the original publications from which you copied the topics in your collection.

Except where expressly stated by Avaya otherwise, no use should be made of materials provided by Avaya on this site. All content on this site and the publications provided by Avaya including the selection, arrangement and design of the content is owned by Avaya and/or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. Avaya owns all right, title and interest to any modifications, additions or deletions to the content in the Avaya publications.

Notice

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

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, 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. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: <https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided 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](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE

TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website <https://www.avaya.com/en/legal-license-terms/> or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, 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. Unless otherwise stated, 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

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](http://www.mpegla.com).

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE 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 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](http://www.mpegla.com).

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply 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, please contact your Avaya Sales Representative.

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>).

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 LLC.

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.

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 Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud 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.

Contents

Chapter 1: Introduction	21
Purpose	21
Change history	21
Chapter 2: CMS overview	23
Logical storage of ACD data	23
Real-time databases	23
Historical databases	23
Data summarizing	24
Data storage	24
Structure of data in the database	26
DbSPACE	26
Chunks	26
ACD data tracking	27
CMS call tracking	27
Events that start or stop data collection	27
Chapter 3: Getting started with the CMS Supervisor client	29
Logging in to the CMS Supervisor Web Client	29
Changing your password in the Web Client	29
Setting preferences	30
Preferences tabs field descriptions	30
Common operational features of the PC Client	31
Before using the Options window	31
Controller features	32
Chapter 4: Administering Dictionary names for call center entities	38
Dictionary permissions	39
Dictionary rules	39
Dictionary search options in the PC Client	40
Permissions required to search the Dictionary	40
Searching the Dictionary	40
Dictionary global search results	40
Administering ACD names in the Dictionary	41
Adding an ACD name in the Web Client	41
Modifying an ACD name in the Web Client	41
Deleting an ACD name in the Web Client	42
Adding an ACD name using the PC Client	42
Modifying an ACD name using the PC Client	43
Deleting an ACD name using the PC Client	43
Viewing ACD group information in the Dictionary	44
Considerations for ACD groups	44

Viewing the contents of an ACD group in the Web Client.....	44
Listing all ACD Groups using the PC Client.....	45
Viewing the contents of an ACD Group using the PC Client.....	45
Administering agent groups in the Dictionary.....	45
Agent group considerations.....	46
Adding an agent group in the Web Client.....	46
Adding agents to an agent group in the Web Client.....	46
Removing an individual agent from an agent group in the Web Client.....	47
Deleting multiple agents from an agent group in the Web Client.....	47
Copying an agent group in the Web Client.....	48
Deleting an agent group in the Web Client.....	48
Adding an agent group using the PC Client.....	49
Copying an agent group using the PC Client.....	49
Deleting an agent group using the PC Client.....	49
Listing agents in an agent group using the PC Client.....	50
Adding agents to an agent group using the PC Client.....	50
Deleting agents from an agent group using the PC Client.....	51
Administering agent string values in the Dictionary.....	51
Modifying agent string value descriptions in the Web Client.....	51
Modifying agent string value descriptions using the PC Client.....	52
Agent string value descriptions.....	52
Administering announcements in the Dictionary.....	54
Adding an announcement name in the Web Client.....	54
Modifying an announcement name in the Web Client.....	55
Deleting an announcement name in the Web Client.....	56
Viewing an announcement name using the PC Client.....	56
Listing all announcement names for an ACD using the PC Client.....	56
Adding an announcement name using the PC Client.....	57
Modifying an announcement name using the PC Client.....	57
Deleting an announcement name using the PC Client.....	58
Administering AUX reason codes in the Dictionary.....	58
Considerations for administering AUX reason codes.....	58
Adding an AUX reason code name in the Web Client.....	59
Modifying an AUX reason code name in the Web Client.....	59
Deleting an AUX reason code name in the Web Client.....	60
Viewing an AUX reason code name using the PC Client.....	60
Listing all AUX reason code names using the PC Client.....	60
Adding an AUX reason code name using the PC Client.....	61
Modifying an AUX reason code name using the PC Client.....	61
Deleting an AUX reason code name using the PC Client.....	62
Administering calculations in the Dictionary.....	62
Considerations for administering calculations.....	63
Adding a custom calculation in the Web Client.....	63

Modifying a custom calculation in the Web Client.....	64
Deleting a custom calculation in the Web Client.....	64
Viewing calculations using the PC Client.....	65
Listing all calculations using the PC Client.....	65
Adding a custom calculation using the PC Client.....	66
Modifying a custom calculation using the PC Client.....	66
Deleting a custom calculation using the PC Client.....	67
Administering call work codes in the Dictionary.....	68
Considerations for call work codes.....	68
Adding a name to a call work code in the Web Client.....	68
Modifying a call work code name in the Web Client.....	69
Deleting a call work code name in the Web Client.....	69
Viewing a call work code name using the PC Client.....	69
Listing all call work code names using the PC Client.....	70
Adding a name to a call work code using the PC Client.....	70
Modifying a call work code name using the PC Client.....	71
Deleting a call work code name using the PC Client.....	71
Administering constants in the Dictionary.....	72
Adding a constant in the Web Client.....	72
Modifying a constant in the Web Client.....	72
Deleting a constant in the Web Client.....	73
Viewing a constant using the PC Client.....	73
Listing all constants using the PC Client.....	73
Adding a constant using the PC Client.....	74
Modifying a constant using the PC Client.....	74
Deleting a constant using the PC Client.....	75
Administering custom database items in the Dictionary.....	75
Adding a custom database item in the Web Client.....	75
Modifying a custom database item in the Web Client.....	76
Deleting a custom database item in the Web Client.....	76
Viewing a custom database item using the PC Client.....	76
Listing all custom database items using the PC Client.....	77
Adding a custom database item using the PC Client.....	77
Modifying a custom database item using the PC Client.....	78
Deleting a custom database item using the PC Client.....	78
Generic string value synonyms in the Dictionary.....	79
Modifying generic string values in the Web Client.....	79
Viewing generic string values using the PC Client.....	79
Modifying generic string values using the PC Client.....	79
Administering location IDs in the Dictionary.....	80
Adding a location ID in the Web Client.....	80
Modifying a location ID in the Web Client.....	80
Deleting a location ID in the Web Client.....	81

Viewing a location ID using the PC Client.....	81
Listing all location IDs using the PC Client.....	81
Adding a location ID using the PC Client.....	82
Modifying a location ID using the PC Client.....	82
Deleting a location ID using the PC Client.....	83
Administering login ID names in the Dictionary.....	83
Considerations for using login ID names.....	83
Adding a login ID name in the Web Client.....	84
Modifying a login ID name in the Web Client.....	84
Deleting a login ID name in the Web Client.....	85
Adding a name to a login ID using the PC Client.....	85
Listing all login ID names using the PC Client.....	85
Adding a name to a login ID using the PC Client.....	86
Modifying a login ID name using the PC Client.....	86
Deleting a login ID name using the PC Client.....	87
Administering logout reason code names in the Dictionary.....	87
Adding a logout reason code name in the Web Client.....	87
Modifying a logout reason code name in the Web Client.....	88
Deleting a logout reason code name in the Web Client.....	88
Viewing a logout reason code name using the PC Client.....	89
Listing all logout reason code names using the PC Client.....	89
Adding a logout reason code name using the PC Client.....	90
Modifying a logout reason code name using the PC Client.....	90
Deleting a logout reason code name using the PC Client.....	91
Administering split/skill names in the Dictionary.....	91
Considerations for split/skill names.....	92
Adding a skill name in the Web Client.....	92
Modifying a skill name in the Web Client.....	92
Deleting a skill name in the Web Client.....	93
Viewing a split/skill name using the PC Client.....	93
Listing all split/skill names using the PC Client.....	93
Adding a split/skill name using the PC Client.....	94
Modifying a split/skill name using the PC Client.....	94
Deleting a split/skill name using the PC Client.....	95
Administering split/skill string values in the Dictionary.....	95
Considerations for split/skill string values.....	96
Modifying split/skill string values in the Web Client.....	96
Viewing split/skill string values using the PC Client.....	96
Modifying split/skill string values using the PC Client.....	96
Split/skill string value descriptions.....	97
Standard CMS database items in the Dictionary.....	98
Viewing standard CMS database items in the Web Client.....	99
Viewing a standard CMS database item using the PC Client.....	99

Viewing all standard CMS database items alphabetically using the PC Client.....	99
Administering tenants in the Dictionary.....	100
Before using tenant names.....	100
Adding a tenant name in the Web Client.....	100
Modifying a tenant name in the Web Client.....	101
Deleting a tenant name in the Web Client.....	101
Viewing a tenant name using the PC Client.....	101
Listing all tenant names using the PC Client.....	102
Adding a tenant name using the PC Client.....	102
Modifying a tenant name using the PC Client.....	102
Deleting a tenant name using the PC Client.....	103
Administering trunk group names in the Dictionary.....	103
Considerations for trunk group names.....	104
Adding a trunk group name in the Web Client.....	104
Modifying a trunk group name in the Web Client.....	104
Deleting a trunk group name in the Web Client.....	105
Viewing a trunk group name using the PC Client.....	105
Listing all trunk group names using the PC Client.....	105
Adding a trunk group name using the PC Client.....	106
Modifying a trunk group name using the PC Client.....	106
Deleting a trunk group name using the PC Client.....	107
Administering trunk string values in the Dictionary.....	107
Administering trunk string values in the Web Client.....	107
Administering trunk string values using the PC Client.....	108
Trunk string value descriptions.....	108
Administering VDN names in the Dictionary.....	110
Considerations for VDN naming.....	110
Adding a VDN name in the Web Client.....	110
Modifying a VDN name in the Web Client.....	110
Removing a VDN name in the Web Client.....	111
Viewing a VDN name using the PC Client.....	111
Listing all VDN names.....	112
Adding a VDN name using the PC Client.....	112
Modifying a VDN name using the PC Client.....	112
Deleting a VDN name using the PC Client.....	113
Administering vector names in the Dictionary.....	113
Considerations for vector names.....	114
Adding a vector name in the Web Client.....	114
Modifying a vector name in the Web Client.....	114
Deleting a vector name in the Web Client.....	115
Viewing a vector name using the PC Client.....	115
Listing all vector names using the PC Client.....	115
Adding a vector name using the PC Client.....	116

Modifying a vector name using the PC Client.....	116
Deleting a vector name using the PC Client.....	117
Chapter 5: Administering call center features.....	118
ACD group administration.....	118
Considerations for administering ACD groups.....	118
Benefits of using ACD groups.....	119
Adding an ACD group in the Web Client.....	120
Adding an ACD to an ACD group in the Web Client.....	120
Deleting an ACD from an ACD group in the Web Client.....	120
Deleting an ACD group in the Web Client.....	121
Listing ACD groups using the PC Client.....	121
Viewing the contents of an ACD group using the PC Client.....	121
Adding an ACD group using the PC Client.....	122
Adding an ACD to an ACD group using the PC Client.....	123
Modifying an ACD group name using the PC Client.....	124
Deleting an ACD from an ACD group using the PC Client.....	125
Deleting an ACD group using the PC Client.....	126
Call work code administration.....	126
Considerations for call work codes.....	126
Adding call work codes in the Web Client.....	127
Removing a single call work code in the Web Client.....	127
Removing multiple call work codes in the Web Client.....	127
Viewing call work codes using the PC Client.....	128
Listing all call work codes using the PC Client.....	128
Adding call work codes using the PC Client.....	129
Deleting call work codes using the PC Client.....	129
Administration of VDN skill preferences.....	130
Considerations for working with VDN skill preferences.....	130
Changing VDN skill preferences in the Web Client.....	130
Viewing VDN skill preferences using the PC Client.....	131
Listing all VDN skill preferences using the PC Client.....	131
Changing VDN skill preferences using the PC Client.....	131
Split/skill call profile administration.....	132
Considerations for split/skill call profiles.....	132
Adding split/skill call profiles in the Web Client.....	133
Modifying a split/skill call profile in the Web Client.....	133
Removing a single split/skill profile in the Web client.....	134
Removing multiple split/skill profiles in the Web client	134
Viewing split/skill call profiles using the PC Client.....	135
Adding split/skill call profiles using the PC Client.....	135
Modifying a split/skill call profile using the PC Client.....	136
Deleting a split/skill call profile using the PC Client.....	137
About viewing trunk group assignments.....	138

Considerations for trunk group assignments.....	138
Viewing trunk group assignments using the Web Client.....	139
Viewing all trunk group assignments using the PC Client.....	139
Viewing a single trunk group assignment using the PC Client.....	139
Viewing a trunk group assignment by VDN or split using the PC Client.....	140
Administration of VDN assignments.....	140
Considerations for VDN assignments.....	141
Managing VDN assignments in the Web Client.....	141
Viewing VDN assignments using the PC Client.....	141
Listing VDNs associated with a vector using the PC Client.....	142
Administration of VDN call profiles.....	142
Considerations for administering VDN call profiles.....	143
Adding a VDN call profile in the Web Client.....	143
Removing an individual VDN call profile in the Web Client.....	144
Removing multiple VDN call profiles in the Web Client	144
Viewing a VDN call profile using the PC Client.....	145
Adding a VDN call profile using the PC Client.....	145
Modifying a VDN call profile using the PC Client.....	147
Deleting a VDN call profile using the PC Client.....	148
Administering a data summarization time zone using the PC Client.....	149
Data summarization time zone fields.....	150
Chapter 6: Administering call center agents.....	151
Permissions for agent administration.....	151
Agent skill changes.....	151
Requirements and considerations for changing agent skills.....	152
Adding agent skills in the Web Client.....	152
Changing agent skills in the Web Client.....	153
Deleting agent skills in the Web Client.....	154
About changing agent skills using the PC Client.....	155
Multi-agent skill changes.....	160
Considerations for multi-agent skill changes.....	160
Assigning a skill to multiple agents in the Web Client.....	160
Moving agents from one skill to another in the Web Client.....	161
Removing agents from a skill in the Web Client.....	161
Changing skills for multiple agents using the PC Client.....	162
Agent tracing.....	163
Viewing current agent trace states using the Web Client.....	163
Viewing current agent trace states using the PC Client.....	164
Activating agent tracing.....	164
Listing of traced agents.....	166
About administering splits using the PC Client.....	167
About changing extension split assignments.....	167
Move extensions between splits.....	168

About running a split members report.....	170
Chapter 7: Administering users and user permissions.....	172
Considerations for the User Permissions subsystem.....	172
Required permissions and example.....	172
User administration.....	173
Viewing CMS users.....	173
Adding a CMS user.....	174
Modifying CMS users.....	177
Deleting CMS users.....	178
Password management in the Web Client.....	179
CMS feature access.....	180
Considerations for administering access to CMS features.....	181
Managing feature access permissions in the Web Client.....	181
Viewing feature access permissions in the PC Client.....	182
Listing all feature access permissions in the PC Client.....	182
Modifying feature access permissions in the PC Client.....	183
Custom menu item assignments and access.....	183
Considerations for access permissions to custom menu items.....	184
Adding custom menu item access permissions in the Web Client.....	184
Modifying custom menu item access permissions in the Web Client.....	184
Viewing custom menu item access permissions in the PC Client.....	185
Listing all custom menu item access permissions in the PC Client.....	185
Assigning or modifying custom menu item access permissions in the PC Client.....	185
Access administration for splits and skills.....	186
Considerations for administering access to splits/skills.....	186
Adding split/skill permissions in the Web Client.....	187
Modifying split/skill permissions in the Web Client.....	188
Deleting split/skill permissions in the Web Client.....	188
Viewing split/skill permissions in the PC Client.....	188
Listing all split/skill user permissions in the PC Client.....	189
Adding split/skill permissions in the PC Client.....	189
Modifying split/skill permissions in the PC Client.....	190
Deleting split/skill permissions in the PC Client.....	191
Access administration for trunk group data.....	191
Considerations for administering access to trunk group data.....	191
Adding trunk group data permissions in the Web Client.....	192
Modifying trunk group data permissions in the Web Client.....	193
Deleting trunk group data permissions in the Web Client.....	193
Viewing trunk group data permissions in the PC Client.....	194
Listing all trunk group data permissions in the PC Client.....	194
Adding trunk group data permissions in the PC Client.....	194
Modifying trunk group data permissions in the PC Client.....	195
Deleting trunk group data permissions in the PC Client.....	196

ACD access permissions.....	196
Considerations for administering access to ACDs.....	196
Adding ACD access permissions in the Web Client.....	197
Modifying ACD access permissions in the Web Client.....	197
Deleting ACD access permissions in the Web Client.....	198
Viewing ACD permissions in the PC Client.....	198
Listing all ACD permissions in the PC Client.....	199
Adding ACD permissions in the PC Client.....	199
Modifying ACD permissions in the PC Client.....	200
Deleting ACD permissions in the PC Client.....	200
Vector access administration.....	201
Considerations for administering access to vector data.....	201
Adding vector access permissions in the Web Client.....	201
Modifying vector permissions in the Web Client.....	202
Deleting vector permissions in the Web Client.....	202
Viewing vector permissions in the PC Client.....	203
Listing all vector permissions in the PC Client.....	203
Adding vector permissions in the PC Client.....	204
Modifying vector permissions in the PC Client.....	204
Deleting vector permissions in the PC Client.....	205
VDN access administration.....	205
Considerations for administering access to VDN data.....	206
Adding VDN data user permissions using the Web Client.....	206
Modifying VDN permissions in the Web Client.....	207
Deleting VDN permissions in the Web Client.....	207
Viewing VDN permissions in the PC Client.....	208
Listing all VDN permissions in the PC Client.....	208
Adding VDN permissions in the PC Client.....	209
Modifying VDN permissions in the PC Client.....	209
Deleting VDN permissions in the PC Client.....	210
Access to tenant data.....	210
Considerations for administering access to tenant data.....	211
Adding tenant permissions in the Web Client.....	211
Modifying tenant permissions in the Web Client.....	212
Deleting tenant permissions in the Web Client.....	212
Administering access to tenant data using the PC Client.....	213
Tenant access operations using the PC Client.....	213
Chapter 8: Administering exceptions.....	215
Types of exceptions.....	215
Exception capacities.....	216
Considerations for exception thresholds.....	217
Permissions for administering exceptions.....	217
About administering exception notification using the PC Client.....	218

Changing exception notification using the PC Client.....	218
Agent exceptions.....	219
Considerations for administering agent exceptions.....	219
Permissions required to administer agent exceptions.....	219
Administering agent exceptions in the Web Client.....	219
Adding agent exceptions using the PC Client.....	220
Modifying agent exceptions using the PC Client.....	221
Deleting agent exceptions using the PC Client.....	222
Agent exception descriptions.....	223
Split/skill exceptions.....	226
Considerations for split/skill exceptions.....	226
Permissions required to administer split/skill exceptions.....	226
Administering split/skill exceptions in the Web Client.....	226
Adding split/skill exceptions in the PC Client.....	227
Modifying split/skill exceptions in the PC Client.....	228
Deleting split/skill exceptions in the PC Client.....	229
Split/skill exception descriptions.....	229
Trunk group exceptions.....	230
Permissions required to administer trunk group exceptions.....	231
Administering trunk group exceptions in the Web Client.....	231
Adding trunk group exceptions in the PC Client.....	232
Modifying trunk group exceptions in the PC Client.....	233
Deleting trunk group exceptions in the PC Client.....	233
Trunk group exception descriptions.....	234
VDN exceptions.....	235
Considerations for administering VDN exceptions.....	235
Permissions required to administer VDN exceptions.....	235
Administering VDN exceptions in the Web Client.....	235
Adding VDN exceptions in the PC Client.....	236
Modifying VDN exceptions in the PC Client.....	237
Deleting VDN exceptions in the PC Client.....	238
VDN exception descriptions.....	238
Vector exceptions.....	240
Considerations for administering vector exceptions.....	240
Permissions required to administer vector exceptions.....	240
Administering vector exceptions in the Web Client.....	240
Adding vector exceptions in the PC Client.....	241
Modifying vector exceptions in the PC Client.....	242
Deleting vector exceptions using the PC Client.....	243
Vector exception definitions.....	244
Real-time exceptions log.....	244
Considerations for the real-time exceptions log.....	245
Viewing the real-time exceptions log using the Web Client.....	245

Viewing the real-time exceptions log using the PC Client.....	245
Chapter 9: Managing tenant access.....	246
Tenancy examples.....	246
Prerequisite tasks for tenancy administration.....	247
Tenant user access restrictions.....	247
Working with tenant features in the Web Client.....	248
Adding agents to a tenant in the Web Client.....	248
Removing an individual agent from a tenant in the Web Client.....	248
Removing multiple agents from a tenant in the Web Client.....	249
Creating a tenant agent group in the Web Client.....	249
Adding agents to a tenant agent group in the Web Client.....	250
Removing an individual agent from a tenant agent group in the Web Client.....	250
Removing multiple agents from a tenant agent group in the Web Client.....	251
Copying a tenant agent group in the Web Client.....	251
Deleting a tenant agent group in the Web Client.....	252
Adding call work codes to a tenant in the Web Client.....	252
Removing an individual call work code from a tenant in the Web Client.....	253
Removing multiple call work codes from a tenant in the Web Client.....	253
Adding splits/skills to a tenant in the Web Client.....	254
Removing an individual split/skill from a tenant in the Web Client.....	254
Removing multiple splits/skills from a tenant in the Web Client.....	255
Adding trunk groups to a tenant in the Web Client.....	255
Removing an individual trunk group from a tenant in the Web Client.....	256
Removing multiple trunk groups from a tenant in the Web Client.....	256
Adding VDNs to a tenant in the Web Client.....	257
Removing an individual VDN from a tenant in the Web Client.....	257
Removing multiple VDNs from a tenant in the Web Client.....	258
Adding vectors to a tenant in the Web Client.....	258
Removing a vector from a tenant.....	259
Removing multiple vectors from a tenant in the Web Client.....	259
PC Client tenant administration sub-menus.....	260
Tenant Agent Assignment administrative operations.....	260
Tenant Agent Groups administrative operations.....	261
Tenant Call Work Code Assignment administrative operations.....	262
Tenant split/skill assignment.....	263
Tenant Trunk Group Assignment administrative operations.....	264
Tenant VDN Assignment administrative operations.....	264
Tenant Vector Assignment administrative operations.....	265
Chapter 10: Configuring CMS system settings.....	267
Switch setup data.....	267
Considerations for viewing switch setup data.....	267
Viewing switch setup data in the Web Client.....	268
Viewing Switch Setup data using the PC Client.....	268

Listing all Switch Setup data using the PC Client.....	268
Pseudo-ACD administration.....	269
Considerations for administering pseudo-ACDs.....	269
Adding a pseudo-ACD in the Web Client.....	270
Deleting a pseudo-ACD in the Web Client.....	270
Viewing pseudo-ACDs using the PC Client.....	270
Adding a pseudo-ACD using the PC Client.....	271
Deleting a pseudo-ACD using the PC Client.....	273
About backing up data from a real ACD to load on a pseudo-ACD.....	274
Considerations for backing up data from a real ACD to load on a pseudo-ACD.....	274
Scenario for backing up data from a real ACD to load on a pseudo-ACD.....	274
About loading pseudo-ACD data.....	275
Considerations for loading pseudo-ACD data.....	275
Verifying that backup data can be read.....	275
Loading pseudo-ACD data in the Web Client.....	276
Loading pseudo-ACD data in the PC Client.....	277
Data storage allocation.....	278
Data storage allocation considerations.....	278
Viewing data storage allocation in the Web Client.....	279
Viewing Data Storage Allocation using the PC Client.....	279
Guidelines for modifying data storage allocation settings.....	280
About viewing free space allocation.....	282
Free space allocation considerations.....	282
Permissions required to view Free Space Allocation.....	283
Viewing free space allocation information in the Web Client.....	283
Viewing Free Space Allocation using the PC Client.....	284
Viewing Free Space Allocation detailed values using the PC Client.....	285
Storage interval administration.....	285
Considerations for administering storage intervals.....	286
Modifying storage interval settings in the Web Client.....	286
Managing storage interval settings in the PC Client.....	288
Administration of custom menu items.....	291
Adding a custom menu item from the Web Client.....	292
Modifying custom menu items using the Web Client.....	292
Deleting custom menu items using the Web Client.....	292
CMS operational states.....	293
Considerations for changing the CMS operational state.....	293
Changing the CMS operational state and master ACD in the Web Client.....	293
Changing the CMS operational state using the PC Client.....	294
Changing the master ACD using the PC Client.....	294
About turning data collection on and off.....	295
Before turning data collection on and off.....	295
Turning data collection on and off in the Web Client.....	296

Turning data collection on and off using the PC Client.....	296
About running data summarizing.....	297
Before running data summarizing.....	297
Running data summarizing using the Web Client.....	298
Running data summarizing using the PC Client.....	298
Administering a data summarization time zone in the Web Client.....	299
Administering a data summarization time zone using the PC Client.....	300
About External Application Status.....	301
Before using External Application Status.....	301
Permissions for External Application Status.....	302
Enabling or disabling the External Application Status feature.....	302
Viewing the states of external applications.....	302
Starting or stopping external applications.....	303
Data migration.....	304
Before migrating data.....	304
Migrating data from the Web Client.....	305
Migrating data using the PC Client.....	306
Migrate Data page descriptions.....	307
Chapter 11: Maintaining CMS	309
Periodic reboot best practices.....	309
Data backups.....	310
CMSADM backups.....	310
Maintenance backups.....	312
Considerations when backing up or restoring data.....	317
Backup file used to restore data.....	319
Performing a binary database backup to a network device.....	320
Adding a full maintenance backup timetable for an ACD in the PC Client.....	320
Options for restoring data.....	322
Before restoring data.....	322
Automatically restoring data in the Web Client.....	323
Manually restoring data in the Web Client.....	323
Doing an automatic restore using the PC Client.....	324
Doing a manual restore using the PC Client.....	325
Restoring the database from a binary backup.....	326
Backup and restore devices.....	327
Adding a backup and restore storage device in the Web Client.....	327
Modifying a backup and restore storage device in the Web Client.....	327
Deleting a backup/restore storage device in the Web Client.....	328
Viewing backup or restore devices using the PC Client.....	329
Listing all backup and restore devices using the PC Client.....	329
Adding a backup or restore device using the PC Client.....	329
Modifying a backup or restore device using the PC Client.....	330
Deleting a backup or restore device using the PC Client.....	330

Printer administration.....	331
Considerations for administering a printer.....	331
Adding a printer in the Web Client.....	332
Modifying printer options using the Web Client.....	332
Deleting a printer using the Web Client.....	333
Listing all printers using the PC Client.....	333
Adding a printer using the PC Client.....	333
Modifying printer options using the PC Client.....	334
Deleting a printer using the PC Client.....	335
Report properties.....	335
Before administering report properties.....	336
Modifying report properties using the Web Client.....	336
Modifying report properties from the command line interface.....	336
ACD connection status.....	337
Viewing connection status in the Web Client.....	337
Viewing connection status of an ACD using the PC Client.....	337
Listing connection status of all ACDs using the PC Client.....	338
Connection status descriptions.....	338
About viewing ACD status.....	340
Prerequisites for viewing ACD status.....	340
Viewing ACD status using the Web Client.....	340
Viewing ACD status using the PC Client.....	340
Listing ACD status using the PC Client.....	341
ACD status field descriptions.....	341
About viewing archiving status.....	342
Viewing archiving status using the Web Client.....	342
Viewing archiving status of a single ACD using the PC Client.....	342
Viewing archiving status of all ACDs using the PC Client.....	343
Archiving status field descriptions.....	343
Viewing firewall status information in the Web Client.....	344
Viewing CMS licensing information in the Web Client.....	345
Support for LDAP integration.....	346
Configuring LDAP in the command line interface.....	347
Chapter 12: Using administration and maintenance reports.....	349
About Dictionary reports.....	349
Permissions required to run Dictionary reports.....	350
Types of Dictionary reports.....	350
Printing dictionary reports.....	351
Running an agent group members report.....	352
About exception reports.....	352
Running the Agent Exceptions by Location report using the Web Client.....	352
Running the Data Collection Exceptions report using the Web Client.....	354
Running the Malicious Call Trace report using the Web Client.....	354

Running the Split or Skill Exceptions report using the Web Client.....	355
Running the Trunk Group by Location Exceptions report using the Web Client.....	356
Running the VDN Exceptions report using the Web Client.....	357
Running the Vector Exceptions report using the Web Client.....	358
Running the Agent Exceptions by Location report using the PC Client.....	359
Running the Data Collection Exceptions report using the PC Client.....	361
Running the Malicious Call Trace report using the PC Client.....	362
Running the Splits/Skills Exceptions report using the PC Client.....	363
Running the Trunk Group by Location Exceptions report using the PC Client.....	365
Running the VDN Exceptions report using the PC Client.....	366
Running the Vector Exceptions report using the PC Client.....	368
About Trunk Group Members reports.....	369
Before using the Trunk Group Members report.....	369
Permissions required to use the Trunk Group Members report.....	370
Running the Trunk Group Members report using the Web Client.....	370
Running the Trunk Group Members report using the PC Client.....	370
About Vector Configuration reports.....	371
Before using the Vector Configuration report.....	371
Permissions required to use the Vector Configuration report.....	371
Running the Vector Configuration report using the Web Client.....	371
Running the Vector Configuration report using the PC Client.....	372
About tenant administration reports.....	372
Running the Tenant Agent Group Members report using the Web Client.....	373
Running the Tenant Agent Group Members report using the PC Client.....	373
Running the Tenant Agent Groups report using the PC Client.....	373
About maintenance reports.....	374
About the ACD Administration Log report.....	374
About the Maintenance Error Log report.....	376
Chapter 13: Scheduling for administration jobs.....	403
Setting up scheduling.....	403
Scheduler page descriptions.....	405
Customizing the maximum retention settings.....	407
Chapter 14: Scripting CMS operations.....	409
Scripting CMS operations.....	409
Before you begin scripting CMS operations.....	409
Tasks scripts can automate.....	409
Interactive and automatic scripts.....	410
Script creation.....	410
Scripting options description.....	411
Setting user ID and password.....	412
Setting users procedure.....	412
Scripting reports.....	412
Creating an interactive report script.....	412

Creating an automatic report script.....	413
Creating a script to export report data.....	413
Creating a script to export report data as HTML.....	414
Scripting operational tasks.....	415
About scripting an input window.....	415
Scripting an action.....	416
Organizing scripts.....	417
Error and warning messages.....	418
Chapter 15: Using the operating system to access CMS and manage passwords.....	419
CMS server login.....	419
Logging in to CMS from the remote console.....	419
Logging in to the CMS server from the virtual console.....	420
Administering passwords.....	420
Considerations for password management.....	420
Changing a user's password through the command line interface.....	421
Enabling password aging.....	421
Chapter 16: Using timetables and shortcuts.....	423
Timetables.....	423
Before using timetables.....	423
Permissions for timetables.....	424
Creating and scheduling a timetable.....	425
Adding tasks to a timetable.....	428
Listing all timetables.....	430
Copying a timetable.....	431
Copying timetable tasks.....	433
Modifying timetable tasks.....	435
Editing timetables globally.....	437
Globally editing tasks in a timetable.....	439
Deleting tasks from a timetable.....	443
Deleting a timetable.....	444
Shortcuts.....	446
Before using shortcuts.....	446
Permissions for shortcuts.....	446
Creating a shortcut.....	447
Adding tasks to a shortcut.....	448
Running a shortcut.....	449
Modifying a shortcut description.....	450
Copying a shortcut.....	451
Copying shortcut tasks.....	452
Modifying shortcut tasks.....	454
Deleting shortcut tasks.....	455
Deleting a shortcut.....	456
Chapter 17: Resources.....	458

Documentation.....	458
Finding documents on the Avaya Support website.....	460
Avaya Documentation Center navigation.....	460
Viewing Avaya Mentor videos.....	462
Support.....	462
Using the Avaya InSite Knowledge Base.....	462
Appendix A: Updating time zones	464
Updating time zones displayed to users.....	464
Glossary	466

Chapter 1: Introduction

Purpose

This document describes how to administer call center features of Avaya Call Management System (CMS) using CMS Supervisor.

CMS Supervisor is available in two client interfaces:

- Web Client, where you access CMS using a web browser.
- PC Client, where you access CMS using a software package installed on a user's personal computer (PC).

Most administrative tasks are available using either client, but some tasks are only available using one client or the other. Procedures in this document identify which tasks are available from the Web Client or the PC Client.

This document is intended for:

- CMS administrators.
- Supervisors with access to CMS.

Change history

The following table outlines the key changes in this document for Release 21.x:

Issue	Date	Summary of changes
3	June 2025	• Added information about scheduling an administration job from the Back Up Data screen. • Added information about enabling or disabling data collection for all ACDs from the Data Collection screen. • Added information about entering the enterprise ID on the User data screen.

Table continues...

Issue	Date	Summary of changes
2	November 2024	• Revised CMS Supervisor administration procedures throughout the document for clarity and accuracy. • Added information about the new administration scheduling feature. • Revised outdated hardware information throughout the document. There are major content updates in some sections. • Removed hardware RAID data storage information. CMS is supported in a virtual environment. • Removed Solaris references and other outdated references. • Revised Logging in to the CMS server from the virtual console on page 420. • Cleaned up structural issues and rephrased various content for clarity.
1	June 2024	Revised Informix information and outdated references.

Chapter 2: CMS overview

Avaya Call Management System (CMS) is a software product for businesses and organizations that receive a large volume of telephone calls processed through the Automatic Call Distribution (ACD) feature of the Avaya Aura® Communication Manager system.

CMS runs on the Red Hat Enterprise Linux (RHEL) operating system and uses various operating system utilities to communicate with terminals and printers, log errors, and run processes. The Informix database management system provides an interface to the CMS historical database.

As an administrator or supervisor, you can use CMS Supervisor to access the CMS database, generate reports, administer ACD parameters, and monitor call activities to determine the most efficient service for customers calling the contact center. The Tenancy feature enables you to restrict user access to CMS reporting data and functionality within the call center.

Logical storage of ACD data

Logical storage refers to how CMS organizes data for processing. It affects how CMS users access and work with ACD data. CMS stores all ACD data received from the communication server in the real-time and historical databases.

Real-time databases

Real-time databases include tables for the current intrahour interval data and the previous intrahour interval data. The storage interval can be 15, 30, or 60 minutes.

Historical databases

Historical databases include tables for the intrahour, daily, weekly, and monthly data. The following table shows all historical database tables and the maximum time that the data can be stored in a particular table:

Historical database tables	Maximum time for data storage
Intrahour historical data	370 days
Daily historical data	5 years (1825 days)

Table continues...

Historical database tables	Maximum time for data storage
Weekly historical data	10 years (520 weeks)
Monthly historical data	10 years (120 months)

Data summarizing

When CMS collects data from the ACD, the real-time database stores the data for the current interval. At the end of the current interval, the following events occur:

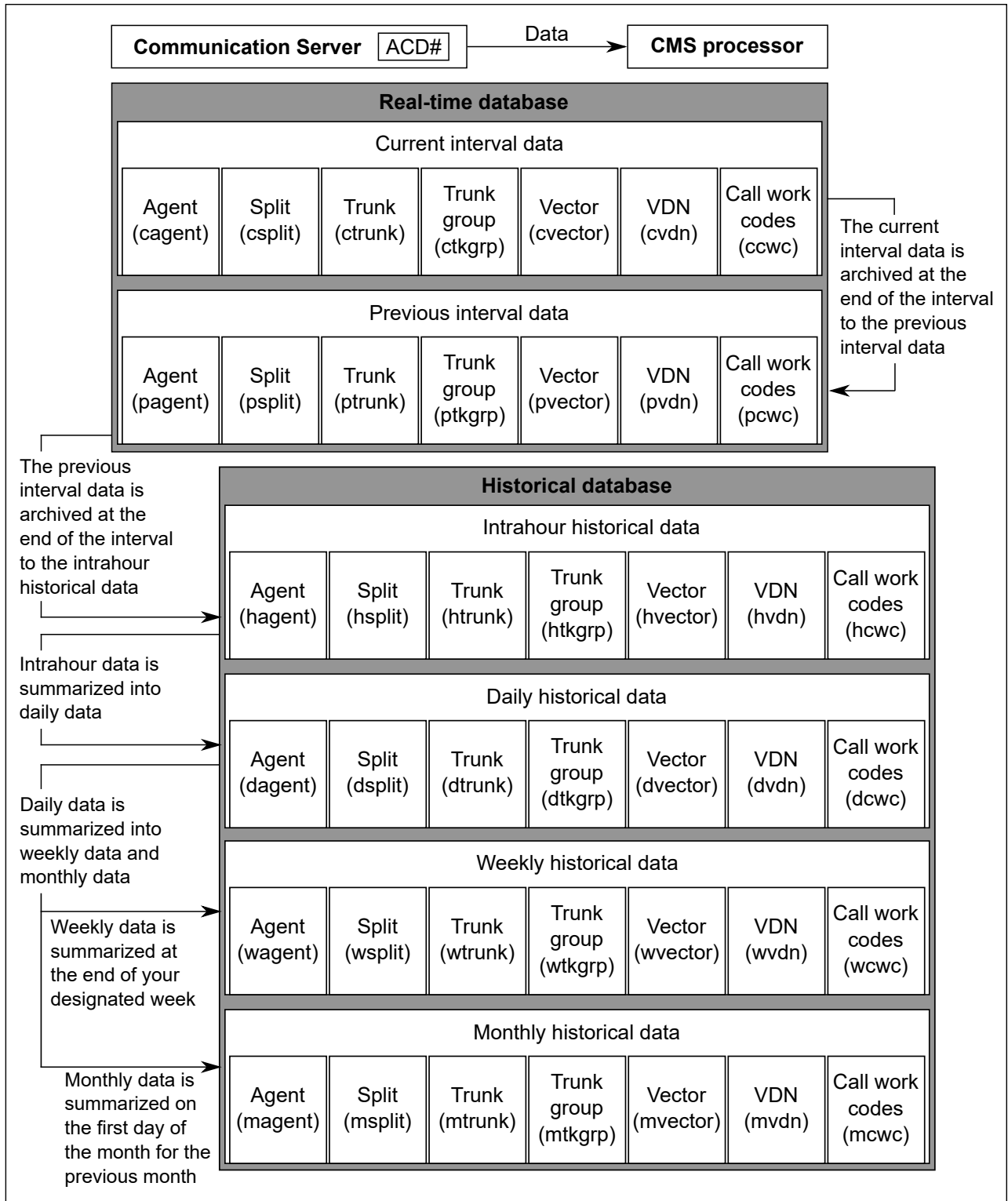
- The data that was in the current interval database table is archived to the previous interval database table.
- The data that was in the previous interval database table is archived in the historical database as intrahour historical data.

The data remains in the historical database as intrahour historical data for a maximum of 370 days. At your designated data summarizing time, the intrahour historical data is summarized into daily historical data.

The daily historical data is summarized on a weekly and monthly basis. At the end of your designated week, the daily historical data is summarized into weekly historical data. On the first day of a new month, the daily historical data is summarized into monthly historical data for the previous month.

Data storage

The following figure shows how CMS stores data.



Structure of data in the database

CMS uses the Informix Dynamic Server (IDS) as a relational database. IDS manages CMS data in specific dbspaces.

Dbospace

A dbospace is a logical database that consists of one or more chunks. Dbspaces can exist across multiple disks. A CMS system contains the following dbspaces:

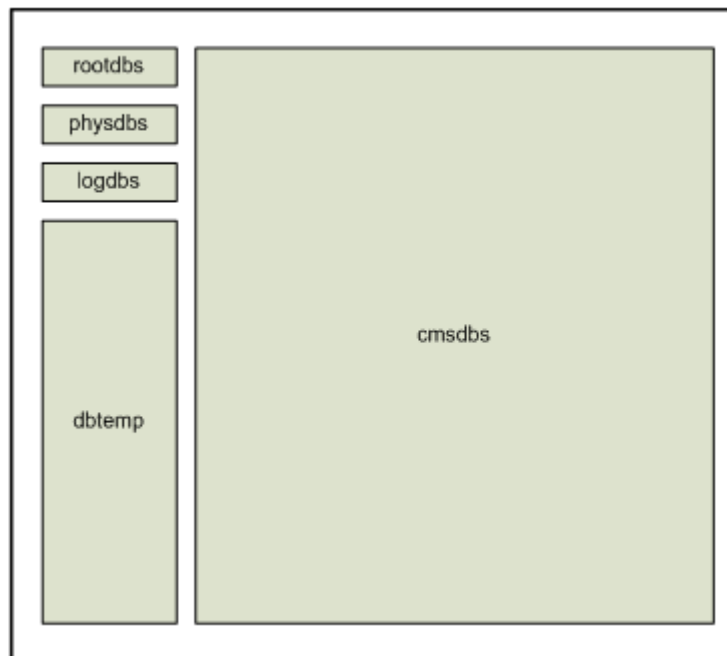
- rootdbs
- physdbs
- logdbs
- dbtemp
- cmsdbs

! **Important:**

Do not try to alter rootdbs, physdbs, logdbs, dbtemp, or cmsdbs.

Chunks

A chunk is a unit of disk space used to store database data that IDS manages. For CMS, each dbospace contains one chunk. The size of each chunk depends on the data requirement specification of CMS. The following figure shows an example of chunk sizing. IDS requires the rootdbs, physdb, and logdbs dbspaces, but these databases store minimal data. Dbospace dbtemp is larger and is used for temporary data space. Dbospace cmsdbs is the location that stores all CMS data and it contains the largest chunk of data.



ACD data tracking

CMS uses the data in the real-time and historical databases to generate standard reports that help you monitor your call center activities. Various agents, split/skill, trunk, trunk group, vector, and VDN activities are tracked at different points in the call process.

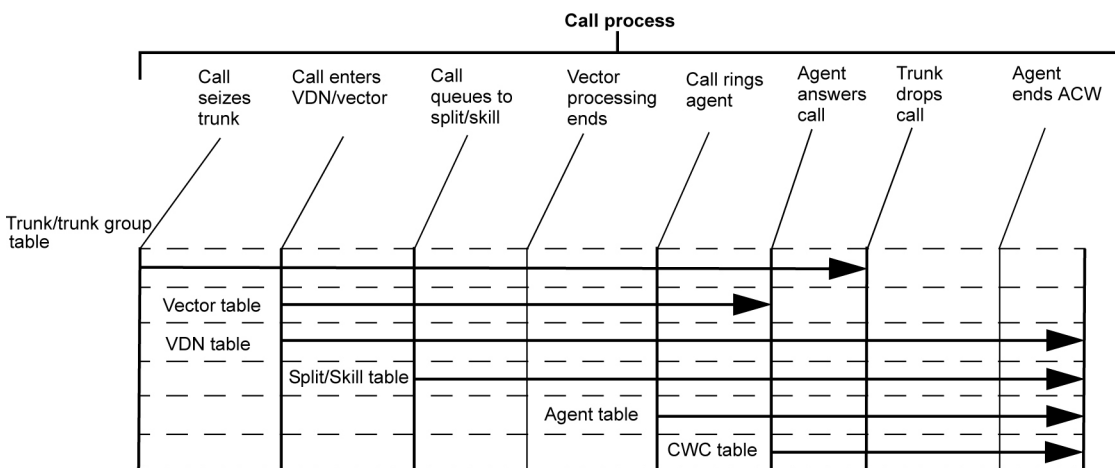
CMS call tracking

The following diagram shows how CMS tracks a call from the time the call seizes a trunk until an agent ends After Call Work (ACW) activities.

The trunk table, trunk group table, vector table, VDN table, split/skill table, agent table, and Call Work Code (CWC) table are CMS database tables that store call data. In the following image, the CMS database table positions identify the points where CMS begins to collect call data. The arrowheads identify the points where data collection ends. CMS does not record the data in the tables until the call and any ACW is complete.

* Note:

With vectoring, the **stop** command stops the processing of vector commands.



Events that start or stop data collection

Data collection starts or stops when one of these events occur:

- The Agent table starts collecting data on non-ACD calls when the agent answers or completes dialing.
- The Split/Skill table stops collecting data when:
 - The ACW for an ACD call ends
 - The call leaves the split queue and is forwarded to another destination . For example, intraflow.
 - The caller abandons the call

- The Vector table stops collecting data for the current vector when the call is:
 - Sent to an ACD agent
 - Connected to a station or trunk
 - Routed to a VDN or vector
 - Abandoned by the caller

 Note:

Time in the vector stops, but the vector tracks the call disposition to determine if the call is answered or abandoned.

- The VDN table stops collecting data for the current VDN when:
 - The ACW for an ACD call ends
 - The call is routed to a trunk or VDN
 - The call is transferred
 - The caller abandons the call

Chapter 3: Getting started with the CMS Supervisor client

This chapter provides general information about accessing and getting started with CMS Supervisor, which is available as a Web Client or PC Client.

- The Web Client is a browser-based tool that runs on the CMS server.
- The PC Client is a software program you install on your computer.

Logging in to the CMS Supervisor Web Client

Procedure

1. In the address bar of your browser, enter the CMS Supervisor URL.
2. In the **User ID** field, type your username.
3. In the **Password** field, type your password.
4. Click **Sign In**.
5. On the CMS Supervisor Web home page, click **Reports**.

The page displays three categories of reports: Realtime, Historical, and Integrated. Each of the categories includes a Designer category, which is only visible in the report lists if there are reports in the Designer folder.

Changing your password in the Web Client

About this task

You can change your CMS password from the Web Client. You might need to do this after logging in for the first time.

Procedure

1. From the top menu bar, click your username and then click **Change password**.

For example, if the username you used to log in is cms, navigate to **cms > Change password**.

2. In the **Old password** field, enter your old password.
3. In the **New password** and **Confirm new password** fields, enter the new password.
4. Click **OK** to save your changes.

Setting preferences

About this task

Use the Preferences option to set color schemes for charts and text strings in reports. You can also adjust tracing settings with this option.

Procedure

1. Log in to the CMS Supervisor Web.
2. On the CMS Supervisor Web home page, select **Reports**.
3. On the menu bar, click your username and then click **Preferences**.
4. On each of the four tabs, set the appropriate preferences.

For information about the color and tracing settings on the Preferences tabs, see [Preferences tabs field descriptions](#) on page 30.

5. To save your settings, click **Apply**.

Preferences tabs field descriptions

Tab	Description
Chart Threshold Colors tab	Use the color palette to change the color of each of the following chart thresholds: • Chart Warning Low Color • Chart Caution Low Color • Chart Insufficient Sample Size Color • Chart Caution High Color • Chart Warning High Color

Table continues...

Tab	Description
Text Threshold Colors tab	Use the background and text color palettes to change the color of each of the following text thresholds: • Warning Low Color • Caution Low Color • Insufficient Sample Size Color • Caution High Color • Warning High Color
Report Chart Colors tab	Select a report chart color theme from the Color Scheme list. To change any color in a theme, select the Customize check box. You cannot change the theme colors if you do not select the Customize option.
Tracing tab	Change the following values to adjust tracing settings: • Trace level: Select one of the following values: Off, Fatal, Error, Warning, Info, Debug, Trace, All • Number of trace files: Select a value between 2 and 8 from the list. • Rollover file size: Select a file-size value between 50 kb and 450 kb. File sizes are listed in multiples of 50.

Common operational features of the PC Client

This section contains information about how to configure the CMS Supervisor PC Client through the Options window.

The Options window allows you to adjust and control the following types of settings:

- The default ACD for all operations and reports windows
- Scripting defaults
- Colors used in CMS Supervisor reports
- Formatting of the different types of fields displayed in CMS Supervisor reports

Before using the Options window

Except for the CMS Servers tab, all other tabs of the Options window are only available after a successful login to a CMS server. The CMS Servers tab is disabled when you are logged in to a CMS server.

Controller features

Overview of the Controller

When you are logged in to the CMS server, the toolbar, status bar, and menu bar have more functions. Your CMS user permissions determines which of the menu items and toolbar buttons are available to you.

Toolbar

The toolbar contains buttons for quick access to specific features of the application. When you move your cursor over a toolbar button, a tooltip displays with a brief description of the command the button performs and a tooltip. For more information, see the specific sections on these features.

Status indicators

These indicators on the status bar indicate the state of CMS.

Name	Description
Login status	A green light if you are connected to the CMS server, and a gray light if you are not connected.
Exception counter	An exception count of the ACDs for which you have exception permissions. The count is zero at the beginning of an interval.
ACD Status	Icons for the ACDs that are supported by the CMS. If the link to an ACD is not working, the icon is crossed out. If the CMS server is connected to the ACD through a TCP/IP connection and the connection is in a transient (stalled) state, the icon changes to a straight line. If you put your mouse over an indicator, a tooltip displays the name of the ACD.
Date and time	The current date and time of the CMS server that you are logged in to.

Status messages

The status bar of the Controller window and other Avaya CMS Supervisor windows might display any of the following Avaya CMS status messages.

Name	Description
Working	An action is incomplete. The window is locked during this time.
Successful	An action completes without errors.
Error	A syntactical error is identified in a field. An error message with field help also displays.
Failed	An action request cannot complete. An Acknowledgement window explains why the request failed.
Does not exist	A record that you are trying to change, delete, or a record for which you are searching is not in the database.

Table continues...

Name	Description
Already exists	A record you are trying to add is in the database. This message also displays when you try to add a range of items, some of which exist and some of which do not. You can add the records that do not exist to the database. The record that already exist remain unchanged.
Cancelled	You cancel a potentially destructive action in an Acknowledgement window.
No matches found	A Find one action completes.
[Number] matches found; permitted ones displayed	A List all action completes, reminding you that you might not have permission to view or change all matches.
No permission	You do not have read permission for the match or matches identified in the search. This issue might occur on the first match identified doing a Find one or on any match identified doing a Next or Previous .
See status window	A status window displays to further explain the condition.

Menu bar

This section identifies the five menus that are available after you log in to the CMS server: **Commands**, **Connect**, **Tools**, **Script**, and **Help**. For more information, see the specific sections on these features.

General tab

Use the General tab to set your first calendar day, default ACD, and other interface usage options.

This tab of the Options dialog box contains the following controls:

Name	Description
First Day of Week	This option affects only how the calendar displays. For example, if you browse for a date, the calendar starts the week based on the day that you choose. This action does not change the Start of Week day for weekly data collection that displays through the System Setup-Storage Intervals window.
Default ACD	Select the ACD that is used as the default ACD for operations and reports windows. Note that an ACD Group can also be set as the default.
Synchronize PC and CMS Time at Login	Select this check box to change the internal clock of the computer to match the current time on the CMS server. This option does not affect the time on the CMS server.
Use Sound	Select this check box to receive an audible alert when the Exceptions Indicator box is updated. The Exceptions Indicator box is located on the Controller status bar. The sound that you hear is the sound that you chose for the exclamation event in Windows. Threshold Highlighting does not use sound and uses color only as an indicator of a threshold being met.
Use Tooltips	Select this check box to make tooltips visible for the controls in the CMS Supervisor interface. For example, when you are working in the CMS Supervisor Controller window, you can put your mouse pointer over a toolbar button. The system displays a yellow box that provides a brief description of that button.

Table continues...

Name	Description
Use Taskbar Icon	Select this check box to have CMS Supervisor put an icon in the notification area.
Window Menu Sort Order	Use this option group to determine how items that are displayed in the menu for notification area icon are arranged: • Start Order: Select this option to display the items in the notification area icon menu where the last item used displays at the top of the menu. • Alphabetical: Select this option to display the items in the notification area icon menu in alphabetical order.

Scripting tab

Use the Scripting tab to set the user ID used to run scripts, adjust the logging level, and set the file used for logging.

This tab of the Options dialog box contains the following controls:

Name	Description
User ID	The login ID for a CMS user.
Set User	Select this button to open the Save as Script - User Information dialog box.
Logging Level	This option group facilitates the following logging levels in configuring the amount of information that is recorded during scripting: • Minimum: The only activities that are logged are errors and messages from Supervisor that is displayed in the window. These messages are displayed as if the user performed the scripted activity manually. • Normal: All activities are logged, plus the start and stop time of each task in the script. This control also includes the script name. • Maximum: All activities are logged, plus more information that might be useful for debugging a script. Any message that displays as the script runs is logged.
Log File Path	Enter the path and the file name of the log file in this field. You might also use the Browse button to the right of this field to select a file on the PC.
Log File Size	This field determines how large the script log file can get before the log file begins replacing the oldest data. The field defaults to a value of 200KB.
View Log	Select this button to view the script log file.

Report Colors tab

Use the Report Colors tab to set the colors in your graphical reports.

This tab of the **Options** dialog box contains the following controls:

Name	Description
Scheme	This field contains all available color schemes.
Save As	Selecting this button saves any changes made in the color bar window as a new scheme. See Creating a new report color scheme on page 35 for instructions on creating report color schemes.

Table continues...

Name	Description
Remove	Selecting this button deletes the displayed scheme.
Color window	This display of 16 bars lets you change the color and pattern of each bar by performing a right-click on that bar.
Background	The background color of reports provides two choices: • White : Select this option to display a white background for all reports. • Automatic : Select this option to have the background of all reports use the color scheme configured through Windows.

Creating a new report color scheme

Procedure

1. From the menu bar of the Controller window, select **Tools > Options**.
CMS Supervisor displays the Options window.
2. Select the **Report Colors** tab.
3. From the **Scheme** drop-down list, select the color scheme you want to use as a basis for the new color scheme.
CMS Supervisor displays the configuration of the scheme in the color bar window.
4. From the **Background** options, select **White** or **Automatic**.
5. Click the color bar (1 through 16) that you want to change.
6. If you want to change the color, select the **Change Color** button and select the color through the Change Color dialog box that the system displays .
7. If you want to change the pattern, select the **Change Pattern** button and select the pattern from the resulting list.
8. Repeat Step [5](#) on page 35 through Step [7](#) on page 35 until you have updated all color bars that you want to change.
9. When you finish modifying color bars, select the **Scheme** button.

 Note:

If you do not save the new color scheme using the **Save As** button, the changes that you make overwrites the default color scheme that you change.

CMS Supervisor displays the Save Scheme As window.

10. Enter a name for this new color scheme in the relevant field.
11. Select **OK** to save this scheme.

To view the changes that you made to a color scheme at any point, select the **Apply** button. The current color scheme is then applied to any reports that are running.

Threshold Colors tab

Use the Threshold Colors tab to set the colors that are used in reports to notify you when exceptions thresholds are reached.

This tab of the **Options** dialog contains the following controls:

Name	Description
Options	This drop-down list box contains all of the existing color schemes available.
Scheme	Selecting this button saves any changes made in the color bar window as a new scheme. See Creating a new threshold color scheme on page 36 for instructions on creating new color schemes.
Remove	Selecting this button deletes the currently displayed scheme.
View/set colors for report threshold indicators	This list box displays the states used for exception thresholds. A graphical representation of the selected state is displayed in the area to the right.
Color	Use the button to the right of this field to change the color for the selected exception threshold state.
Pattern	Use the button to the right of this field to change the graphical pattern applied for the selected exception threshold state.

Creating a new threshold color scheme

Procedure

1. From the menu bar of the Controller window, select **Tools > Options**.

CMS Supervisor displays the Options window.

2. Select the **Threshold Colors** tab.

3. From the **Scheme** drop-down list, select the color scheme you want to use as a basis for the new color scheme.

CMS Supervisor displays the view of the scheme.

4. In the **View/set colors for report threshold indicators** list, select the item you want to change.

Supervisor displays the current setting for the selected item in the area to the right of the list box. The **Color** and **Pattern/Background** fields display the respective settings for the current item.

5. If you want to change the color of the selected item, select the **Change Color** button at the right of the **Color** field.

CMS Supervisor displays the standard Color window from Windows allowing you to select the new color.

6. If you want to change the pattern/background color for the selected item, select the button at the right of the **Pattern/Background** field.

Depending on the item selected, Supervisor will display either the pattern list or the Color window which allows you to select a new pattern or background color.

7. Repeat Steps [4](#) on page 36 through [6](#) on page 36 until you have updated all of the threshold element colors that you want to modify.
8. When you are done modifying the threshold element colors, select the **Save As** button.
Supervisor displays the Save Scheme As window.
9. In the text box, enter a name for this new threshold color scheme you have just created.
10. Select the **OK** button to save this new color scheme.

To view the changes that you made to a color scheme at any point in the modification, select the **Apply** button.

The current color scheme is then applied to any reports that are running.

Name Format tab

Use the Name Format tab to choose or create formats for how CMS entities, for example, splits/skills, ACDs, VDNs, vectors, trunks, trunk groups, call work codes, and AUX codes, are displayed in CMS. Supervisor. The display can be set to any one or a combination of **{name}** for Dictionary Name, **{entity}** for entity type, and **{number}** for entity number.

Choose or create a name format using **{name}** for entity name, as entered in the Dictionary, **{entity}** for entity type, and **{number}** for entity number. These formats determine how items are displayed in reports. For example, if you select the name format of **{entity}{number}**, all entities that can be named in the Dictionary are displayed as the entity type and number instead of the name defined in the Dictionary. If you selected **{name}** as the name format, the names that are assigned to the entities in the Dictionary are displayed.

Defining entity formats

Procedure

1. From the **Entity** field, select the item for which you want to change the format.
2. In the **Format** field, use one of the following methods to select a format for the specified entity type:
 - Manually enter the format that you want using the three possible types: **{name}**, **{entity}**, and **{number}**. Using a separator character between formats is unnecessary unless you want the separator to appear in the report. For example, if you want to display agent names and extension numbers on reports, enter **{name} {number}** in the **Format** box.
 - Use the drop-down list to choose from a set of preformatted options.

The **Example** field provides an example of what the format resembles based on your current definition.

If you entered a nonstandard name format, this format not saved in the **Format** list.

3. Select **OK** to save your changes.

Chapter 4: Administering Dictionary names for call center entities

You can use the Dictionary to assign names or synonyms to the following call center entities:

- ACDs
- Agent groups
- Agent string values
- Announcements
- AUX reason codes
- Call work codes
- Generic string values
- Location IDs
- Login IDs
- Logout reason codes
- Splits/skills
- Split/Skill string values
- Tenants
- Trunk groups
- Trunk string values
- VDNs
- Vectors

You can also use the Dictionary to work with items in the database. The tasks you can perform include the following:

- Viewing ACD groups
- Creating and administering custom calculations
- Creating and administering constants
- Creating and administering custom database items
- Viewing standard database items

- Viewing standard calculations

The names assigned through the Dictionary are displayed in reports. The Dictionary also enables you to create agent groups, change agent splits/skills, and change trunk string values for reporting purposes.

*** Note:**

Changes to the Dictionary should occur during off hours when there are the fewest database updates. Otherwise, you will need to constantly query the database to update the cache on the computer where CMS Supervisor is running. This causes the real-time reports to hang and access to CMS Supervisor might be denied.

Dictionary permissions

You need permissions for the Dictionary subsystem.

- To view items in the Dictionary, you require Read permissions.
- To add, change, or delete items in the Dictionary, you require Write permissions.

You might also need permissions for the entity you are managing.

- When working with ACD names, you need permissions for the Dictionary subsystem and for the ACD.
- To view ACD groups, you need Read permissions for the Dictionary subsystems and for the ACD group. Tenant users can only view the ACD groups to which they are assigned.

Dictionary rules

The following rules apply when assigning names in the Dictionary:

- First character must be A-Z or a-z.
- Remaining characters can be A-Z, a-z, 0-9, underscores, periods, and commas.
- Spaces are allowed in all Dictionary names except calculation names and constant names.
- Names must be unique within each section of the Dictionary for an ACD. For example:
 - You can name trunk group 1 as “sales”, and skill 1 as “sales”, but you cannot name skill 1 as “sales” and skill 2 as “sales” on the same ACD.
 - Similarly, no two agents can have the same synonyms within the same ACD.

The following rules apply to the descriptions assigned in the Dictionary:

- Descriptions in the Dictionary can have from 0 to 50 characters.
- Descriptions can include all printable characters except semicolon (;), double quotes ("), and the pipe symbol (|).

Dictionary search options in the PC Client

The Dictionary contains a global search feature that you can use to find a variety of information. Some examples of the types of information that you can search for in the dictionary are:

- A login ID or a group of login IDs
- A split, skill, or trunk group
- ACD names
- Database items
- Calculations
- Agent names

Consider the following:

- You can search any pattern.
- You can include an asterisk (*) or question mark (?) in your pattern.
- The search is case sensitive.

Permissions required to search the Dictionary

To do a global search in the dictionary, you need the *write* permissions for the Dictionary subsystem.

Searching the Dictionary

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Global Search**.
3. In the **Search for** field, enter the item name or pattern.
4. From the **Actions** menu, select **Run**.

CMS displays the Dictionary Global Search Results.

Dictionary global search results

Field	Contents
Value matched	Displays the matches for your pattern.
Field matched	Displays the name of the field in the Dictionary that corresponds to value matched.

Table continues...

Field	Contents
In submenu	The Dictionary submenu that contains your search pattern.
Name	The name that corresponds to the value matched.

Administering ACD names in the Dictionary

Use the Dictionary subsystem to assign names to ACDs. ACD names are displayed in reports. You can add, delete, or change an ACD name regardless of which ACD you are logged in to.

For example, you can be logged in to ACD 1 and change the name for ACD 3.

For tenant users, the Dictionary menu options are read only. A tenant user can search the database for matching ACD numbers and ACD names.

Adding an ACD name in the Web Client

About this task

Use this procedure to create a name for an ACD. You must specify an existing ACD. An error is displayed if you enter an invalid ACD number.

Procedure

1. Navigate to **Administration > Dictionary > ACDs**.
CMS Supervisor displays the list of administered ACD names.
2. Click **Add ACD**.
3. In the **ACD Number** field, enter the number corresponding to the ACD for which you want to define a name.
You can enter a number from 1 to 26. You must enter the number of an existing ACD. If you enter a number that does not correspond to an ACD, an error message is displayed.
4. In the **ACD Name** field, enter the name of the ACD or ACD group.
5. In the **Description** field, add additional information about the ACD.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
6. Click **OK** to save your changes.

Modifying an ACD name in the Web Client

About this task

You can change an ACD name and its associated description. The ACD number is read only.

Procedure

1. Navigate to **Administration > Dictionary > ACDs**.
CMS Supervisor displays the list of administered ACD names.
2. Click  next to the item you want to modify.
The Modify Item window is displayed.
3. In the **ACD Name** field, update the name of the ACD or ACD group.
4. **(Optional)** Revise the information in the **Description** field.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
5. Click **OK** to save your changes.

Deleting an ACD name in the Web Client

About this task

This procedure only removes the name of an ACD and not the ACD itself. When you remove an ACD name in the Dictionary, the ACD is displayed as `unnamed_acdn`, where *n* is the ACD number. Do not perform this procedure unless you are certain that you want to delete the ACD name.

Procedure

1. Navigate to **Administration > Dictionary > ACDs**.
CMS Supervisor displays the list of administered ACD names.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. Click **Yes** to complete the change.

Adding an ACD name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **ACDs**.
3. Click **OK**.
CMS Supervisor displays the Dictionary ACDs window.
4. In the **ACD Name** field, enter the name of the ACD or ACD Group that you want to add, delete, or change.

The name you assign to an ACD, pseudo ACD, or ACD Group in the Dictionary is displayed on all reports and window titles that are associated with that ACD.

5. In the **ACD Number** field, enter a number from 1 to 26 to correspond with the new ACD name. Numbers 1 through 8 is reserved for real ACDs and 9 through 26 is reserved for pseudo-ACDs.
6. To add your changes to the Dictionary, select **Actions > Add**.

Modifying an ACD name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **ACDs**.
3. Click **OK**.
CMS Supervisor displays the Dictionary ACDs window.
4. In the **ACD Number** field, enter the number of the ACD, pseudo-ACD, or ACD Group that you want to change.
5. From the **Actions** menu, select **Find one**.
6. In the **ACD Name** field, enter the new name for the selected ACD.
7. To add your changes to the Dictionary, select **Actions > Modify**.

Deleting an ACD name using the PC Client

About this task

Important:

Deleting an ACD name from the Dictionary only removes the name of the ACD. The ACD is then displayed as `unnamed_acdn` where *n* is the number of the ACD. No warnings are given during the process of deleting an ACD. This procedure should not be performed unless you are certain that you want to delete the ACD.

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **ACDs**.
3. Click **OK**.
CMS Supervisor displays the Dictionary ACDs window.
4. In the **ACD Number** field, enter the number of the ACD, pseudo-ACD, or ACD Group for which you want to delete the name.

5. From the **Actions** menu, select **Find one**.

The name of the ACD is displayed in the **ACD Name** field.

6. Select **Actions > Delete** to remove the ACD from the Dictionary.

Viewing ACD group information in the Dictionary

Before you can view ACD groups in the Dictionary, you must first configure them in the Call Center Administration subsystem. The Dictionary displays the configured ACD groups and their corresponding members. The option to view ACD groups in the Dictionary enables users who run reports in the call center to see which ACDs are defined within each ACD group. This is useful for determining which ACD groups should be used when running reports.

ACD group information is not displayed in standard CMS reports. You must create custom reports through the CMS ASCII interface.

Considerations for ACD groups

Consider the following when working with ACD groups:

- After adding an ACD group, you must log out of CMS Supervisor to see it.
- An ACD group cannot serve as the CMS master ACD.
- Synonym conflicts can occur if you have overlapping ACD groups with common member ACDs. To prevent problems, ensure that the entity IDs in overlapping ACD groups are mutually exclusive.
- Entity synonyms must be unique for an ACD group and across all ACDs that are members of the ACD group.
- User permissions are administered separately for an ACD group and its member ACDs.
- CMS real-time custom reports are only displayed if data collection is enabled and the ACD link status is up for at least one member ACD in the specified ACD group. An error message is displayed if these conditions are not met.
- Custom reports that you create with the Single ACD Only option enabled cannot be run for an ACD group and vice versa.

Viewing the contents of an ACD group in the Web Client

About this task

You can view ACD groups in the Dictionary in read-only format.

Before you begin

Use the Call Center Administration subsystem to create an ACD group and assign ACDs to it.

Procedure

1. Navigate to **Administration > Dictionary > ACD Groups**.
CMS Supervisor displays the configured ACD groups.
2. Click  next to an ACD group to view the ACDs assigned to the group.
3. **(Optional)** To return to the main list of ACD groups, click **Back to Group List**.

Listing all ACD Groups using the PC Client**Procedure**

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.
CMS Supervisor displays the Dictionary ACD Groups window.
4. From the menu bar, select **Actions > List all**.
CMS Supervisor displays the Dictionary ACD Groups List all window listing all ACD Groups defined on this CMS server.

Viewing the contents of an ACD Group using the PC Client**Procedure**

1. From the Controller window, select **Commands > Dictionary**.
2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.
CMS Supervisor displays the Dictionary ACD Groups window.
4. In the **ACD Group Name** field, enter the name of the ACD Group that you want to view.
5. From the menu bar, select **Actions > Find one**.
CMS Supervisor retrieves the information for the specified ACD Group, if valid.
6. From the menu bar, select **Actions > Get contents**.
CMS Supervisor displays the Dictionary ACD Groups Get contents window which lists all ACDs assigned to this ACD Group.

Administering agent groups in the Dictionary

Use the following procedures to manage agent groups in the Dictionary.

Agents can be grouped for reporting purposes, without regard to the split/skill assignment for the agent. For example, you can create a group for new employees or a group for employees with special skills.

Agent group considerations

Consider the following when creating agent groups:

- Limit the size of agent groups to approximately 99 agents. Larger agent groups can affect system performance.
- You can add or remove up to 32 agents at a time.
- When possible, report on consecutive Agent IDs in the same report.
- When possible, limit agent group reports and use skill-based reports.
- Tenant users must have permissions for the agent group they want to modify.

Adding an agent group in the Web Client

About this task

You can add an agent group in the Dictionary and define a name for it.

Procedure

1. Navigate to **Administration > Dictionary > Agent Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent groups.
CMS Supervisor displays the agent groups administered for the selected ACD.
3. Click **Add Agent Group**.
4. In the **Agent Group Name** field, enter a name for the new agent group.
5. Click **OK** to save your changes.

Adding agents to an agent group in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Agent Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent groups.
CMS Supervisor displays the agent groups administered for the selected ACD.
3. Click  next to the agent group you want to modify.
4. Click **Add Agent** to add an agent to the agent group.
CMS Supervisor displays the Agent Groups: Contents window.
5. In the **Add Agent** field, enter agent names or IDs.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

6. Click **+** to move agents from the Search Results area to the Selected Agents area.

The agents in the Selected Agents area are added to the agent group.

7. Click **OK** to save your changes.

Removing an individual agent from an agent group in the Web Client

About this task

Use this procedure to remove an individual agent from an agent group or to remove a few agents one at a time.

Procedure

1. Navigate to **Administration > Dictionary > Agent Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent groups.

CMS Supervisor displays the agent groups administered for the selected ACD.

3. Click  next to the agent group you want to modify.

4. Click  next to the agent you want to remove.

The Confirm Delete dialog box is displayed.

5. Click **Yes** to complete the change.

Deleting multiple agents from an agent group in the Web Client

About this task

Use this procedure to remove agents from an agent group in bulk. Specify which agents no longer need to be in the agent group and then remove them.

Procedure

1. Navigate to **Administration > Dictionary > Agent Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent groups.

CMS Supervisor displays the agent groups administered for the selected ACD.

3. Click  next to the agent group you want to modify.

4. Click **Remove Agent**.

CMS Supervisor displays the Agent Groups: Contents window.

5. In the **Remove Agent** field, enter the names or IDs of agents that are currently in the agent group but no longer need to be there.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

6. Click **+** to move agents from the Search Results area to the Selected Agents area.

The agents in the Selected Agents area will be removed from the agent group.

7. Click **OK** to save your changes.

Copying an agent group in the Web Client

About this task

Use this procedure to copy the contents from one agent group to a new agent group. Under the “to” heading, you can enter a name for the new agent group.

Procedure

1. Navigate to **Administration > Dictionary > Agent Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent groups.
CMS Supervisor displays the agent groups administered for the selected ACD.
3. Click  next to the agent group you want to copy.
The Copy Agent Group window displays the name of the agent group you are copying from.
4. In the **Agent Group Name** field under the “to” heading, enter a name for the new agent group.
5. Click **OK** to save your changes.

Deleting an agent group in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Agent Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent groups.
CMS Supervisor displays the agent groups administered for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Adding an agent group using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD group on which the agent group resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Agent Groups window.
5. In the **Agent group name** field, enter the name of the new agent group.
6. To add the agent group to the Dictionary, select **Actions > Add**.
7. To add the Login IDs for this agent group, select **Actions > Get contents**.
CMS Supervisor displays the Agent Groups-Get Contents window.
8. Enter the Login IDs for the new group.
9. To add the Login IDs to the Dictionary for this agent group, select **Actions > Add**.

Copying an agent group using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD group on which the agent group resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Agent Groups window.
5. In the **Agent group name** field, enter the name of the new agent group.
6. From the **Actions** menu, select **Copy Group**.
CMS Supervisor displays the Dictionary Agent Groups window.
7. In the **Copy from** field, enter the name of the agent group that you want to copy.
8. From the **Actions** menu, select **Copy Group**.
The new agent group is automatically populated with all agents from the copied group.

Deleting an agent group using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD group on which the agent group resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Agent Groups window.

5. In the **Agent group name** field, enter the name of the agent group to delete.
6. From the **Actions** menu, select **Delete**.

The selected agent group name is removed from the Dictionary.

Listing agents in an agent group using the PC Client Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD group on which the agent group resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Agent Groups window.

5. In the **Agent group name** field, enter the name of the agent group.
6. From the **Actions** menu, select **Get contents**.

CMS Supervisor displays the Agent Groups-Get Contents window.

7. From the **Actions** menu, select **List all**.

CMS Supervisor displays the Dictionary Agent Groups-Get Contents-List All window listing the agents in the group.

Adding agents to an agent group using the PC Client Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD group on which the agent group resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Agent Groups window.

5. In the **Agent group name** field, enter the name of the agent group to which you want to add agents.

6. From the **Actions** menu, select **Get contents**.

CMS Supervisor displays the Dictionary ACD Groups Get contents window.

7. Enter the Login IDs that you want to add to this group. You can add up to 32 agents at a time.
8. From the **Actions** menu, select **Add**.

Deleting agents from an agent group using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD group on which the agent group resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Agent Groups window.

5. In the **Agent group name** field, enter the name of the agent group from which you want to delete agents.
6. From the **Actions** menu, select **Get contents**.
- CMS Supervisor displays the Agent Groups-Get Contents window.
7. Enter the Login IDs to delete from this group. You can delete up to 32 agents at a time.
8. From the **Actions** menu, select **Delete**.

Administering agent string values in the Dictionary

Agent string values are descriptive words in reports that correspond to agent states. Words such as ACD, ACW, or AUX, describe the value for the data. Strings are changed to the values you set when they are displayed as data in a report. The report heading is not affected.

Modifying agent string value descriptions in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Agent String Values**.
2. In the **Current ACD** drop-down list, select the active ACD for which you want to change agent string values.

CMS Supervisor displays the list of agent string values administered for the selected ACD.

3. Enter a new descriptive word in the fields you want to change.

For a description of the available agent string values, see [Agent string value descriptions](#) on page 52.

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

Modifying agent string value descriptions using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Agent String Values**.
3. In the **ACD** field, select the ACD or ACD Group that you want to change.
4. Click **OK**.

CMS Supervisor displays the Dictionary Agent String Values window.

5. Enter a new descriptive word in the fields you want to change.

For a description of the available agent string values, see [Agent string value descriptions](#) on page 52.

6. Click **Actions > Modify**.

CMS Supervisor saves the changed agent string values.

Agent string value descriptions

You can modify the default string values on the Agent String Values page. The following table describes the options available under each area:

Area	Description
Work Mode	• ACD: The agent is on an ACD call. • ACW: The agent is in the After Call Work mode. • AUX: The agent is in the auxiliary work mode and is not available to take calls. • AVAIL: The agent is available to take an ACD call. • DACD: The agent is on a direct agent ACD call. • DACW: The agent is in the ACW mode for a direct agent ACD call. • OTHER: The agent has just logged in and CMS has not yet been notified of the agent's state. This mode is also used if: - An agent is dialing an extension or has an extension call ringing while in auto-in/manual-in (AI/MI). - An agent puts a call on hold and does not perform any other call-related actions. • RINGING: An ACD call is ringing at the agent's voice terminal and the agent is not doing anything else. • UNKNOWN: CMS does not recognize the current state. • UNSTAFF: The agent is not logged in or is not staffed yet.
Agent Trace Work Mode	• LOGON: An agent is logged in. • LOGOFF: An agent is logged out and is not available to take ACD calls.
Call Direction	• IN: The agent is on an incoming call. • OUT: The agent is on an outbound call.
Call Origination	• PHONE: The agent dialed an outbound call using the voice terminal dialpad. • KEYBOARD: The agent dialed an outbound call using the computer keyboard.
Call Destination	• PBX: Internal to the switch. • Off: External to the switch.
Reserve Level	• Rsv1: The agent begins answering calls when the skill's first threshold is crossed. • Rsv2: The agent begins answering calls when the skill's second threshold is crossed.
Call Handling Preference	• Level: The agent's call-handling preference is by skill level. • NEED: The agent's call-handling preference is by greatest need. • PERCENT: The agent's call-handling preference is based on an assigned percentage of time allocated to each skill.

Table continues...

Area	Description
Agent Role	• TOP: The agent can be counted on to answer the skill's calls, unless their other skills go into overload. • ALLOCATED: The agent has time allocated to answering the skill's calls. • BACKUP: The agent helps answer the skill's calls when their top skill is not busy. • ROVING: The agent answers a skill's calls when this skill has the greatest need. • RESERVE: The agent helps answer the skill's calls when the skill is over threshold. These roles vary according to call handling preferences.
Interrupt Type	• NA: No interruptions when the agent is in the auxiliary state. • AUTO-IN: While in the auxiliary state, the agent can automatically be put into the Available state to receive calls when the number of available agents is insufficient. • MANUAL-IN: When interrupted, the agent presses a button to manually indicate that they are available. • NOTIFY: The agent is notified and can choose to accept or reject the interruption.
Interrupt Status	• NA: The agent is not in the interruptible auxiliary state. • NOTIFYING: The agent is notified of an interruption while in the interruptible auxiliary state. • INTRRPTED: The agent is interrupted in the interruptible auxiliary state and is handling a call. • INTRRPTBLE: The agent is in the interruptible auxiliary state.

Administering announcements in the Dictionary

Announcements are recorded messages that are played for callers. You can record an announcement in the ACD system.

Use the Dictionary in CMS Supervisor to administer announcement names. These announcement names are synonyms, which are assigned to the recorded messages. When administering announcement names, note the following:

- Use unique announcement names.
- Do not use multiple values for announcement names or numbers.

Adding an announcement name in the Web Client

About this task

You can record an announcement in the ACD system. In the Dictionary, enter an extension number, name, and description for the announcement.

Procedure

1. Navigate to **Administration > Dictionary > Announcements**.
2. In the **Current ACD** list, select the active ACD for which you want to administer announcement names.
CMS Supervisor displays the announcement names administered for the selected ACD.
3. Click **Add Announcement**.
4. In the **Announcement Extension** field, enter an extension number for the announcement.
The extension can contain 3 to 7 numbers. When callers enter this extension, they hear the announcement.
5. In the **Announcement Name** field, enter a name for the announcement.
6. In the **Description** field, enter a brief description with additional information about the announcement.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
7. Click **OK** to save your changes.

Modifying an announcement name in the Web Client

About this task

You can modify the name and description for an announcement. The extension number for the announcement is read only.

Procedure

1. Navigate to **Administration > Dictionary > Announcements**.
2. In the **Current ACD** list, select the active ACD for which you want to administer announcement names.
CMS Supervisor displays the announcement names administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. In the **Announcement Name** field, update the formula of the calculation.
5. **(Optional)** Revise the information in the **Description** field.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
6. Click **OK** to save your changes.

Deleting an announcement name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Announcements**.
2. In the **Current ACD** list, select the active ACD for which you want to administer announcement names.
CMS Supervisor displays the announcement names administered for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing an announcement name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Announcements window.
5. To find an announcement name to view, only one of the fields requires that you specify an announcement. Perform one of the following actions to specify an announcement in the Dictionary:
 - In the **Announcement Name** field, enter the synonym name of the announcement.
 - In the **Announcement Number** field, enter the number of the announcement.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the data for the specified announcement, if valid.

Listing all announcement names for an ACD using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Announcements window.

5. From the **Actions** menu, select **List all**.

Adding an announcement name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Announcements window.

5. In the **Announcement Name** field, enter the name that you want to assign to the announcement.
6. In the **Announcement Number** field, enter a number that corresponds with the announcement name.

You can enter any other information about the announcement in the **Description** field. You can enter only 50 or fewer characters in this field.

7. From the **Actions** menu, select **Add**.

Modifying an announcement name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Announcements window.

5. To find an announcement name to change , you must specify an announcement in only one of the fields. Perform one of the following actions to specify an announcement in the Dictionary:

- In the **Announcement Name** field, enter the name of the announcement.
- In the **Announcement Number** field, enter the number of the announcement.

6. From the **Actions** menu, select **Find one**.

Supervisor retrieves and displays the data for the specified announcement, if valid.

7. In the **Announcement Name** field, enter the new announcement name.
8. From the **Actions** menu, select **Modify**.

Deleting an announcement name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Announcements window.

5. To find an announcement name to delete, you must specify an announcement in only one of the fields. Perform one of the following actions to specify an announcement in the Dictionary:
 - In the **Announcement Name** field, enter the name of the announcement.
 - In the **Announcement Number** field, enter the number of the announcement.
6. From the **Actions** menu, select **Find one**.

Supervisor retrieves and displays the data for the specified announcement, if valid.
7. From the **Actions** menu, select **Delete**.

Administering AUX reason codes in the Dictionary

Agents can select a configured AUX reason code to specify why they are in the AUX state. AUX refers to the auxiliary time during which agents are not available to take calls. For example, during lunch or meetings. You can add, change, or delete AUX reason code names from the Dictionary.

Considerations for administering AUX reason codes

Consider the following before administering AUX reason codes in the Dictionary:

- The supported digits for AUX reason codes are 0 to 99.
- AUX reason code names can be up to 20 characters long.
- AUX reason code 0 is used for cases in which the switch automatically puts an agent into AUX work mode. You can change the name.
- Names must be unique within an ACD. No two AUX reason codes in the same ACD can have the same name.
- If you make changes to the AUX reason code names, you must restart any report that uses AUX reason codes to see the changes.

Adding an AUX reason code name in the Web Client

About this task

In the Dictionary, you can add a name and description for a reason code. AUX reason code 0 is used for cases where the ACD automatically puts an agent into AUX work mode. You can still assign a name for this reason code.

Procedure

1. Navigate to **Administration > Dictionary > AUX Reason Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to manage AUX reason code names.

CMS Supervisor displays the existing AUX reason code names for the selected ACD.

3. Click **Add AUX Reason Code**.
4. In the **AUX Reason Code** field, enter a value between 0 and 99.
5. In the **AUX Reason Code Name** field, enter a name for the reason code.
6. In the **Description** field, enter a brief description with additional information about the reason code.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

7. Click **OK** to save your changes.

Modifying an AUX reason code name in the Web Client

About this task

You can modify the name and description for an AUX reason code. However, the number assigned to a reason code is read-only.

Procedure

1. Navigate to **Administration > Dictionary > AUX Reason Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to manage AUX reason code names.

CMS Supervisor displays the existing AUX reason code names for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. In the **AUX Reason Code Name** field, update the name of the reason code.
5. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Deleting an AUX reason code name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > AUX Reason Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to manage AUX reason code names.
CMS Supervisor displays the existing AUX reason code names for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing an AUX reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD group on which the AUX Reason Codes reside.
4. Click **OK**.
CMS Supervisor displays the Dictionary AUX Reason Codes window.
5. To find an AUX reason code name to view, only one of the fields requires that you specify an AUX reason code . Perform one of the following actions to specify an AUX reason code in the Dictionary:
 - In the **AUX Reason Code Name** field, enter the name for the AUX reason code.
 - In the **AUX Reason Code** field, enter an AUX reason code number from 0 to 99.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified AUX reason code, if valid.

Listing all AUX reason code names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **AUX Reason Codes**.

3. In the **ACD** field, enter the ACD or ACD group on which the AUX Reason Codes reside.
4. Click **OK**.

CMS Supervisor displays the Dictionary AUX Reason Codes window.

5. From the **Actions** menu, select **List all**.

CMS Supervisor displays the Dictionary AUX Reason Codes — List All window.

Adding an AUX reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD group on which the AUX Reason Codes reside.
4. Click **OK**.

CMS Supervisor displays the Dictionary AUX Reason Codes window.

5. In the **AUX Reason Code Name** field, enter the name for the AUX reason code.
 6. In the **AUX Reason Code** field, enter an AUX reason code number from 0 to 99.
- You can enter any other information about the AUX reason code in the **Description** field.
You can enter only 50 or fewer characters in this field.
7. From the Actions menu, select **Add**

Modifying an AUX reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD group on which the AUX Reason Codes reside.
4. Click **OK**.

CMS Supervisor displays the Dictionary AUX Reason Codes window.

5. To find an AUX reason code name to modify, only one of the fields requires an AUX reason code name to be specified. Perform one of the following actions to specify an existing AUX reason code name in the Dictionary:
 - In the **AUX Reason Code Name** field, enter the name for the AUX reason code.
 - In the **AUX Reason Code** field, enter an AUX reason code number from 0 to 99.
6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified AUX reason code, if valid.

7. In the **AUX Reason Code Name** field, enter the new name for the AUX reason code.
8. From the **Actions** menu, select **Modify**.

CMS Supervisor updates the name for the AUX reason code in the database.

Deleting an AUX reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD group on which the AUX Reason Codes reside.
4. Click **OK**.

CMS Supervisor displays the Dictionary AUX Reason Codes window.

5. To find an AUX reason code name to delete, you must specify an AUX reason code in only one of the fields. Perform one of the following actions to specify an AUX reason code in the Dictionary:

- In the **AUX Reason Code Name** field, enter the name for the AUX reason code.
- In the **AUX Reason Code** field, enter an AUX reason code number from 0 to 99.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified AUX reason code, if valid.

7. From the **Actions** menu, select **Delete**.

CMS Supervisor removes the specified AUX reason code from the Dictionary.

Administering calculations in the Dictionary

Calculation names are abbreviated names for the calculations in the database. These calculations are used to create reports. You can view standard calculations or create your own custom calculations to use in custom reports. The names for the calculations used in standard reports already exist in the Dictionary.

Considerations for administering calculations

Consider the following before changing calculation names in the Dictionary:

- Calculation names must be one word with no spaces.
- Reports do not run if you embed calculations more than three levels deep.
- You cannot delete standard calculation names. For information about standard CMS calculations, see *Avaya Call Management System Database Items and Calculations*.
- You can identify your own calculation names in all lowercase letters to distinguish them from the standard CMS Supervisor calculation names. The standard calculation names are in all uppercase letters.
- If you delete a custom calculation from the Dictionary, any report with that calculation does not run.
- You can adversely affect standard reports if you change a standard CMS Supervisor calculation. Reports might run, but the results could be unpredictable.
- Reports do not run if you create calculations that reference each other in a circular way. For example, assume that CALC_1 uses CALC_2 in processing. If CALC_2 then uses CALC_1, this creates a circular pattern where the processing cannot be completed.

Adding a custom calculation in the Web Client

About this task

You can create a custom calculation in the Dictionary. The formula for the calculation can have up to three levels of nesting. It can include database items, constants, and the following arithmetic operators:

- + (add)
- – (subtract)
- * (multiply)
- / (divide)
- () (do first, as in standard mathematical operations)

Important:

Calculations that refer to another calculation should enclose the referenced calculation within parentheses. For example, if Calculation 1 (C1) is $A + B + C$ and Calculation 2 (C2) is C1 divided by D, type $(C1) / D$ for Calculation 2.

Procedure

1. Navigate to **Administration > Dictionary > Calculations**.
CMS Supervisor displays the calculations administered for the system.
2. Click **Add Calculation** to add a new custom calculation.
3. In the **Calculation Name** field, enter a name for the custom calculation.

Use lowercase letters in the name to distinguish this custom calculation from a standard CMS calculation.

4. In the **Calculation** field, enter the formula for the calculation.

You can enter up to 70 characters in this field.

5. In the **Description** field, enter a brief description with additional information about the calculation.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Modifying a custom calculation in the Web Client

About this task

You can modify custom calculations that you created. The calculation name is read only and cannot be changed.

Caution:

Do not modify standard CMS calculations. If you change a standard calculation, its meaning changes in every report that uses the calculation. Even if you can successfully run the affected reports, the results could be inaccurate and unpredictable.

Procedure

1. Navigate to **Administration > Dictionary > Calculations**.

CMS Supervisor displays the calculations administered for the system.

2. Click  next to the item you want to modify.

The Modify Item window is displayed.

3. In the **Calculation** field, update the formula for the calculation.

4. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

5. Click **OK** to save your changes.

Related links

[Adding a custom calculation in the Web Client](#) on page 63

Deleting a custom calculation in the Web Client

About this task

You can delete a custom calculation that you created.

 Caution:

Do not delete standard CMS calculations. If you delete a standard calculation, every report that uses the calculation will be invalid.

Procedure

1. Navigate to **Administration > Dictionary > Calculations**.
CMS Supervisor displays the calculations administered for the system.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. Click **Yes** to complete the change.

Viewing calculations using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Calculations**.
3. Click **OK**.
CMS Supervisor displays the Dictionary Calculations window.
4. To find a calculation to view, only one of the fields requires that you specify a calculation. Perform one of the following actions to specify an existing database calculation in the Dictionary:
 - If you know the name of the calculation, enter the calculation in the **Calculation Name** field.
 - If you do not know the name of the calculation, Leave all the fields in the Dictionary Calculations window blank, and from the **Actions** menu, select **Find one**. Use the **Next** or **Previous** buttons to move through the list of calculations.

Listing all calculations using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Calculations**.
3. Click **OK**.
CMS Supervisor displays the Dictionary Calculations window.
4. From the **Actions** menu, select **List all**.

Adding a custom calculation using the PC Client

About this task

You can create a custom calculation in the Dictionary. The formula for the calculation can have up to three levels of nesting. It can include database items, constants, and the following arithmetic operators:

- + (add)
- – (subtract)
- * (multiply)
- / (divide)
- () (do first, as in standard mathematical operations)

Important:

Calculations that refer to another calculation should enclose the referenced calculation within parentheses. For example, if Calculation 1 (C1) is $A + B + C$ and Calculation 2 (C2) is C1 divided by D, type $(C1) / D$ for Calculation 2.

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Calculations**.

3. Click **OK**.

CMS Supervisor displays the Dictionary Calculations window.

4. Enter the name of the calculation in the **Calculation Name** field.

Use lowercase letters in the name to distinguish this custom calculation from a standard CMS calculation.

5. In the **Calculations** field, enter the formula for the calculation.

6. Add any other information about the calculation in the **Description** field.

You can enter up to 50 characters in this field.

7. From the **Actions** menu, click **Add**.

The custom calculation is added to the Dictionary.

Modifying a custom calculation using the PC Client

About this task

You can modify custom calculations that you created.

 Caution:

Do not modify standard CMS calculations. If you change a standard calculation, its meaning changes in every report that uses the calculation. Even if the affected reports run, the results could be inaccurate and unpredictable.

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Calculations**.
3. Click **OK**.
CMS Supervisor displays the Dictionary Calculations window.
4. Enter the name of the custom calculation in the **Calculation Name** field.
5. From the **Actions** menu, select **Find one**.
6. In the **Calculation** field, enter the new formula.
7. Update the information in the **Description** field if required.
8. From the **Actions** menu, click **Modify**.

Deleting a custom calculation using the PC Client

About this task

You can delete a custom calculation that you created.

 Caution:

Do not delete standard CMS calculations. If you delete a standard calculation, every report that uses the calculation will be invalid.

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Calculations**.
3. Click **OK**.
CMS Supervisor displays the Dictionary Calculations window.
4. Enter the name of the custom calculation in the **Calculation Name** field.
5. From the **Actions** menu, click **Find one**.
CMS Supervisor retrieves and displays the information for the specified calculation.
6. From the **Actions** menu, click **Delete**.
The specified calculation is removed from the Dictionary.

Administering call work codes in the Dictionary

Call work codes (also known as CWCs) are numeric sequences for categorizing the calls agents have received or are handling. By entering call work codes, agents can assign one of many defined categories to calls. Call work codes are defined in the Dictionary and can represent any kind of tracked call, including complaints, special sales, and promotional events. You can assign up to five call work codes to each call.

The names you define in the Dictionary are displayed in the standard CWC historical report.

Considerations for call work codes

Consider the following before changing call work codes in the Dictionary:

- Call work codes must be activated on the ACD before you can perform any administration tasks.
- Call work codes require storage space on the CMS file system. For information about configuring CMS settings, see [Configuring CMS system settings](#) on page 267.
- Call Work Code 0 is reserved for unadministered work codes so summary data can be collected. The default name for Call Work Code 0 is “Unadministered codes”, but this name can be changed.
- Even though call work codes can be up to 16 digits long, a Dictionary name can only be assigned to a call work code that is 9 digits long.
- Tenant users must have permissions for the call work codes they need to manage.

Adding a name to a call work code in the Web Client

About this task

Use the Dictionary to define a call work code and add a name for it.

Procedure

1. Navigate to **Administration > Dictionary > Call Work Code**.
2. In the **Current ACD** list, select the active ACD for which you want to administer call work codes.

CMS Supervisor displays the call work codes administered for the selected ACD.

3. Click **Add Call Work Code**.
4. In the **Call Work Code** field, enter the numeric call work code.

The call work code can contain 1 to 16 numbers.

5. In the **Call Work Code Name** field, enter a name to represent the call work code.
6. In the **Description** field, enter a brief description with additional information.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

7. Click **OK** to save your changes.

Modifying a call work code name in the Web Client

About this task

You can modify the name of a call work code and its description. The call work code itself is read only.

Procedure

1. Navigate to **Administration > Dictionary > Call Work Code**.
2. In the **Current ACD** list, select the active ACD for which you want to administer call work codes.

CMS Supervisor displays the call work codes administered for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. In the **Call Work Code Name** field, update the name of the call work code.
5. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Deleting a call work code name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Call Work Code**.
2. In the **Current ACD** list, select the active ACD for which you want to administer call work codes.

CMS Supervisor displays the call work codes administered for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the change.

Viewing a call work code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Call Work Code**.

3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Call Work Codes window.

5. To find a call work code name to view, only one of the fields requires that you specify a call work code. Perform one of the following actions to specify a call work code in the Dictionary:
 - In the **Call Work Code Name** field, enter the name of the call work code.
 - In the **Call work code** field, enter the number of the of the call work code.
6. From the **Call Work Code Name** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified call work code, if valid.

Listing all call work code names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Call Work Code**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Call Work Codes window.
5. From the **Actions** menu, select **List all**.

Adding a name to a call work code using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Call Work Code**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Call Work Codes window.
5. In the **Call Work Code Name** field, enter the name of the of the new call work code.
6. In the **Call work code** field, enter the number of the of the new call work code.
7. From the **Actions** menu, select **Add**.

The specified call work code and the associated name is added to the Dictionary.

Modifying a call work code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Call Work Code**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Call Work Codes window.

5. To find a call work code name to change , only one of the fields requires that you specify a call work code. Perform one of the following actions to specify a call work code in the Dictionary:

- In the **Call Work Code Name** field, enter the name of the call work code.
- In the **Call work code** field, enter the number of the of the call work code.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified call work code, if valid.

7. In the **Call Work Code Name** field, enter the new name of the call work code.
8. From the **Actions** menu, select **Modify**.

The specified call work code entry is changed in the Dictionary.

Deleting a call work code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Call Work Code**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Call Work Codes window.

5. To find a call work code name to delete, only one of the fields requires that you specify a call work code. Perform one of the following actions to specify a call work code in the Dictionary:

- In the **Call Work Code Name** field, enter the name of the of the call work code.
- In the **Call work code** field, enter the number of the of the call work code.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified call work code, if valid.

7. From the **Actions** menu, select **Delete**.

The specified call work code is removed from the Dictionary.

Administering constants in the Dictionary

Constants are items with fixed numeric values that you can enter in the Dictionary. They do not exist when CMS is installed. Constants are only used in custom and designer reports.

Adding a constant in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Constants**.

CMS Supervisor displays the list of constants administered for the system.

2. Click **Add Constant** to add a constant for use in custom and designer reports.
3. In the **Constant Name** field, enter a name for the constant.
4. In the **Value** field, enter a value for the constant.

The value can range from -99999 to 999999.

5. In the **Description** field, enter a brief description with additional information.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Modifying a constant in the Web Client

About this task

You can modify the value of a constant and its description. The constant name is read only and cannot be changed.

Procedure

1. Navigate to **Administration > Dictionary > Constants**.

CMS Supervisor displays the constants administered for the system.

2. Click  next to the item you want to modify.

The Modify Item window is displayed.

3. In the **Value** field, update the value for the constant.

4. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

5. Click **OK** to save your changes.

Deleting a constant in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Constants**.

CMS Supervisor displays the list of constants administered for the system.

2. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

3. Click **Yes** to complete the change.

Viewing a constant using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Constants**.

3. Click **OK**.

CMS Supervisor displays the Dictionary Constants window.

4. To find a constant to view, only one of the fields requires that you specify an entry. Perform one of the following actions to specify a constant in the Dictionary:

- In the **Constant Name** field, enter the name of the constant.
- In the **Value** field, enter the numeric value of the constant.

5. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified constant, if valid.

Listing all constants using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Constants**.

3. Click **OK**.

CMS Supervisor displays the Dictionary Constants window.

4. From the **Actions** menu, select **List all**.

Adding a constant using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Constants**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Constants window.

4. In the **Constant Name** field, enter the name of the new constant.
5. In the **Value** field, enter the numeric value of the constant. The value can range from -99999 to 999999.

You can enter any other information about the constant in the **Description** field. You can enter only 50 or fewer characters in this field.

6. From the **Actions** menu, select **Add**.

Modifying a constant using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Constants**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Constants window.

4. To find a constant to change, only one of the fields requires that you specify an entry. Perform one of the following actions to specify a constant in the Dictionary:

- In the **Constant Name** field, enter the name of the constant.
- In the **Value** field, enter the numeric value of the constant.

5. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified constant, if valid.

6. In the **Value** field, enter the new numeric value for the constant.

 Note:

You cannot change the name of the new constant. If you want to change the name, you must delete the old constant and add a new one.

7. From the **Actions** menu, select **Modify**.

Deleting a constant using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Constants**.
3. Click **OK**.
CMS Supervisor displays the Dictionary Constants window.
4. To find a constant to delete, only one of the fields requires that you specify an entry. Perform one of the following actions to specify a constant in the Dictionary:
 - In the **Constant Name** field, enter the name of the constant.
 - In the **Value** field, enter the numeric value of the constant.
5. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified constant, if valid.
6. From the **Actions** menu, select **Delete**.
The specified constant is removed from the Dictionary.

Administering custom database items in the Dictionary

You can define and update custom database items in the Dictionary. Database items are stored in the CMS database. These custom items enable you to combine your own data with the CMS data in custom or designer reports.

Ensure that the table is created in the database before you create a custom database item. For more information about database tables, see *Avaya Call Management System Database Items and Calculations*.

Adding a custom database item in the Web Client

About this task

Custom items are stored in database tables. When creating a custom item in the Dictionary, you must specify the database table.

Procedure

1. Navigate to **Administration > Dictionary > Custom Items**.
CMS Supervisor displays the custom database items administered for the system.
2. Click **Add Custom Database Item**.

3. In the **Database Item** field, enter a name for the custom database item.
4. In the **Table** field, enter the name of the database table that will contain the custom item.
5. In the **Description** field, enter a brief description with additional information.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
6. Click **OK** to save your changes.

Modifying a custom database item in the Web Client

About this task

You can modify the database table for a custom item and the item description. However, the **Database Item** field is read only. If you want to change the name of a custom database item, you must delete it and add a new custom item.

Procedure

1. Navigate to **Administration > Dictionary > Custom Items**.
CMS Supervisor displays the custom database items administered for the system.
2. Click  next to the item you want to modify.
The Modify Item window is displayed.
3. In the **Table** field, specify the database table for the custom item.
4. **(Optional)** Revise the information in the **Description** field.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
5. Click **OK** to save your changes.

Deleting a custom database item in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Custom Items**.
CMS Supervisor displays the custom database items administered for the system.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. Click **Yes** to complete the change.

Viewing a custom database item using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Custom Items**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Custom Items window.

4. In the **Database Item** field, enter the name of the custom database item.
5. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified custom database item, if valid.

Listing all custom database items using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Custom Items**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Custom Items window.

4. In the **Database Item** field, enter the name of the custom database item.
5. From the **Actions** menu, select **List all**.

Adding a custom database item using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Custom Items**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Custom Items window.

4. In the **Database Item** field, enter the name of the new database item.

You can enter any other information about the custom database item in the **Description** field. Only 50 or fewer characters can be entered in this field.

5. In the **Table** field, enter the name of the table that contains the new custom database item.
6. From the **Actions** menu, select **Add**.

Modifying a custom database item using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Custom Items**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Custom Items window.

4. In the **Database Item** field, enter the new name for the custom database item.
5. In the **Table** and **Description** fields, enter the new information for the custom database item.

You can enter only 50 or fewer characters in the **Description** field.

Note:

You cannot change the name of a custom database item. You must delete the old item and add the new item if you want a different name.

6. From the **Actions** menu, select **Modify**.

The specified custom database item and the changes are saved to the Dictionary.

Deleting a custom database item using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Custom Items**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Custom Items window.

4. In the **Database Item** field, enter the name of the database item to delete.
5. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified custom database item, if valid.

6. From the **Actions** menu, select **Delete**.

The specified custom database item is removed from the Dictionary.

Generic string value synonyms in the Dictionary

The option to change generic string values enables you to enter a replacement string for the default y for Yes and n for No values. The string values can be up to six characters long. These modified string values are displayed in custom or designer reports that use the Yes or No synonyms.

Modifying generic string values in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Generic String Values**.
2. In the **Current ACD** list, select the active ACD for which you want to administer generic string values.
3. Specify new string values for the Yes and No synonyms.
4. Click **Apply** to apply the change.

Viewing generic string values using the PC Client

Procedure

1. From the Controller window, select **Commands> Dictionary**.
2. In the **Operations** list, highlight **Generic String Values**.
3. In the **ACD** field, enter the ACD or ACD Group on which the generic string values reside.
4. Select **OK**.

CMS Supervisor displays the Dictionary Generic String Values window.

Modifying generic string values using the PC Client

Procedure

1. From the Controller window, select **Commands> Dictionary**.
2. In the **Operations** list, highlight **Generic String Values**.
3. In the **ACD** field, enter the ACD or ACD Group on which the generic string values reside.
4. Select **OK**.

CMS Supervisor displays the Dictionary Generic String Values window.

5. In the **YES** field, enter up to six characters.
6. In the **NO** field, enter up to six characters.

The characters entered in the **YES** and **NO** fields are displayed in reports that use these synonyms.

7. From the **Actions** menu, select **Modify**.

Administering location IDs in the Dictionary

A location ID represents the location or site where an agent works or the port network to which a trunk is assigned. You can name location IDs for ease of identification in reporting for multisite environments. The same location IDs and synonyms are used for both agents and trunks.

Adding a location ID in the Web Client

About this task

You can assign a name to a location ID in the Dictionary.

Procedure

1. Navigate to **Administration > Dictionary > Location IDs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer location IDs.

CMS Supervisor displays the location IDs administered for the selected ACD.

3. Click **Add Location ID**.
4. In the **Location ID** field, enter a numeric ID between 0 and 2000.
5. In the **Location Name** field, enter a name to represent the location.
6. In the **Description** field, enter a brief description with additional information about the location.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

7. Click **OK** to save your changes.

Modifying a location ID in the Web Client

About this task

You can change the name of a location and its description. The location ID is read only.

Procedure

1. Navigate to **Administration > Dictionary > Location IDs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer location IDs.

CMS Supervisor displays the location IDs administered for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. In the **Location Name** field, change the name of the location.
5. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Deleting a location ID in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Location IDs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer location IDs.

CMS Supervisor displays the location IDs administered for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the change.

Viewing a location ID using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Location IDs**.
3. In the **ACD** field, enter the ACD on which the location ID resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Location IDs window.

5. To find a location ID to view, only one of the fields requires that you specify a value. Perform one of the following actions to specify a location ID in the Dictionary:

- In the **Location Name** field, enter the name of the location.
- In the **Location ID** field, enter the number of the location.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified location ID, if valid.

Listing all location IDs using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Location IDs**.

3. In the **ACD** field, enter the ACD on which the location ID resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Location IDs window.
5. From the **Actions** menu, select **List all**.

Adding a location ID using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Location IDs**.
3. In the **ACD** field, enter the ACD on which you want to add the location ID.
4. Click **OK**.
CMS Supervisor displays the Dictionary Location IDs window.
5. In the **Location Name** field, enter the name of the new location.
6. In the **Location ID** field, enter the number from 1-250 for the new location.
You can enter any other information about the location ID in the **Description** field. You can enter only 50 or fewer characters in this field.
7. From the **Actions** menu, select **Add**.

Modifying a location ID using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Location IDs**.
3. In the **ACD** field, enter the ACD on which the location ID resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Location IDs window.
5. To find a location ID to change, only one of the fields requires that you specify a value. Perform one of the following actions to specify a location ID in the Dictionary:
 - In the **Location Name** field, enter the name of the location.
 - In the **Location ID** field, enter the number of the location.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified location ID, if valid.
7. In the **Location Name** field, enter the new name for the location.

8. From the **Actions** menu, select **Add**.

Deleting a location ID using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Location IDs**.
3. In the **ACD** field, enter the ACD on which the location ID resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Location IDs window.
5. To find a location ID to delete, only one of the fields requires a value to be specified. Perform one of the following actions to specify a location ID in the Dictionary:
 - In the **Location Name** field, enter the name of the location.
 - In the **Location ID** field, enter the number of the location.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified location ID.
7. From the **Actions** menu, select **Delete**.
The specified location ID is removed from the Dictionary.

Administering login ID names in the Dictionary

CMS uses agent login IDs to identify measured ACD agents. After an agent name is assigned to a login ID, CMS displays the agent's login ID name instead of the login ID number.

Adding agent names in the Dictionary is optional, but CMS administration pages and reports are easier to understand with agent names instead of login IDs. Depending on the amount of available space, agent names might be truncated.

Considerations for using login ID names

Consider the following when working with login ID names in the Dictionary:

- Login ID names are sorted alphabetically in the Dictionary based on the first character you enter in the **Agent Name** field.
 - For example, if the agent is listed as "Jane Brown", sorting in the Dictionary is based on the "J" for Jane. If the agent is listed as "Brown, Jane", the name is listed under "B" for Brown. CMS Supervisor reports do not automatically sort by agent name.

- You cannot assign the same agent name to multiple login IDs.
- Login IDs contain numbers only.
- When a login ID displayed on a report is changed, you must exit the report and run it again to see the change.

Adding a login ID name in the Web Client

About this task

You can associate a login ID with an agent name. Adding a name makes it easier to identify an agent.

Procedure

1. Navigate to **Administration > Dictionary > Login IDs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer login IDs.
CMS Supervisor displays the login IDs administered for the selected ACD.
3. Click **Add Login ID**.
4. In the **Login ID** field, enter the numeric login ID for the agent.
The login ID can contain 3 to 13 numbers.
5. In the **Agent Name** field, enter a name for the agent.
6. In the **Description** field, enter a brief description with additional information.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
7. Click **OK** to save your changes.

Modifying a login ID name in the Web Client

About this task

The login ID is read only and cannot be changed. You can change the associated name and its description.

Procedure

1. Navigate to **Administration > Dictionary > Login IDs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer login IDs.
CMS Supervisor displays the login IDs administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. In the **Agent Name** field, revise the name associated with the login ID.
5. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Deleting a login ID name in the Web Client

About this task

You can remove the name associated with a login ID.

Procedure

1. Navigate to **Administration > Dictionary > Login IDs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer login IDs.
CMS Supervisor displays the login IDs administered for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Adding a name to a login ID using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Login identification**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to view a login ID name.
4. Click **OK**.
CMS Supervisor displays the Dictionary Login Identifications window.
5. To find a login ID to view, only one of the fields requires that you specify a value. Perform one of the following actions to specify a login ID in the Dictionary:
 - In the **Login ID** field, enter the number of the login ID.
 - In the **Agent Name** field, enter the name of the agent.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified login ID name, if valid.

Listing all login ID names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Login identification**.
3. In the **ACD** field, enter the ACD or ACD Group in which you want to list all login ID names.
4. Click **OK**.

CMS Supervisor displays the Dictionary Login Identifications window.

5. From the **Actions** menu, select **List all**.

Adding a name to a login ID using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Login identification**.
3. In the **ACD** field, enter the ACD or ACD Group to which you want to assign a name to a login ID.
4. Click **OK**.

CMS Supervisor displays the Dictionary Login Identifications window.

5. In the **Login ID** field, enter the number of the login ID to which you want to assign a new name.
6. In the **Agent Name** field, enter the name of the agent that you want to associate with the Login ID number.
7. From the **Actions** menu, select **Add**.

Modifying a login ID name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Login identification**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to modify a login ID name.
4. Click **OK**.

CMS Supervisor displays the Dictionary Login Identifications window.

5. To find a login ID to change, only one of the fields requires you to specify a value. Perform one of the following actions to specify a login ID in the Dictionary:
 - In the **Login ID** field, enter the number of the login ID.
 - In the **Agent Name** field, enter the name of the agent.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information that is associated with the specified login ID name, if valid.

7. In the **Agent Name** field, enter the modified name of the agent.

8. From the **Actions** menu, select **Modify**.

The specified login ID name and the changes are saved in the Dictionary.

Deleting a login ID name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Login identification**.

3. In the **ACD** field, enter the ACD or ACD Group in which the login ID name to delete resides.

4. Click **OK**.

CMS Supervisor displays the Dictionary Login Identifications window.

5. To find a login ID to delete, only one of the fields requires that you specify a value. Perform one of the following actions to specify a login ID in the Dictionary:

- In the **Login ID** field, enter the number of the login ID.
- In the **Agent Name** field, enter the name of the agent.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified login ID name, if valid.

7. From the **Actions** menu, select **Delete**.

Administering logout reason code names in the Dictionary

Logout reason codes enable an agent to specify why they are logging out. For example, to attend training or because their shift has ended. You can add, change, or delete logout reason codes.

The reason code names you assign are displayed in the standard agent login/logout and agent trace historical reports.

Adding a logout reason code name in the Web Client

About this task

You can assign a name to each logout reason code.

Procedure

1. Navigate to **Administration > Dictionary > Logout Reason Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to administer logout reason codes.

CMS Supervisor displays the logout reason codes administered for the selected ACD.

3. Click **Add Logout Reason Code**.
4. In the **Logout Reason Code** field, enter a number between 0 and 9.
5. In the **Logout Reason Code Name**, enter a name for the reason code.
6. In the **Description** field, enter a brief description with additional information.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

7. Click **OK** to save your changes.

Modifying a logout reason code name in the Web Client

About this task

The logout reason code number is read only and cannot be changed. You can change the name associated with the reason code and its description.

Procedure

1. Navigate to **Administration > Dictionary > Logout Reason Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to administer logout reason codes.

CMS Supervisor displays the logout reason codes administered for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. In the **Logout Reason Code Name** field, update the name for the reason code.
5. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Deleting a logout reason code name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Logout Reason Codes**.

2. In the **Current ACD** list, select the active ACD for which you want to administer logout reason codes.

CMS Supervisor displays the logout reason codes administered for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the change.

Viewing a logout reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Logout Reason Codes**.

3. In the **ACD** field, enter the ACD or ACD Group on which you want to view a logout reason code name.

4. Click **OK**.

CMS Supervisor displays the Dictionary Logout Reason Codes window.

5. To find a logout reason code to view, only one of the fields requires that you specify a value. Perform one of the following actions to specify a logout reason code in the Dictionary:

- In the **Logout Reason Code Name** field, enter the name of the logout reason code.
- In the **Logout Reason Code** field, enter a number from 0 to 9 that is associated with the logout reason code.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor displays the Dictionary window retrieves and displays the information for the specified logout reason code name, if valid.

Listing all logout reason code names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Logout Reason Codes**.

3. In the **ACD** field, enter the ACD or ACD Group on which you want to view all logout reason code names.

4. Click **OK**.

CMS Supervisor displays the Dictionary Logout Reason Codes window.

5. From the **Actions** menu, select **List all**.

CMS Supervisor displays the Dictionary Logout Reason Codes - List All window.

Adding a logout reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Logout Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group in which you want to add a logout reason code.
4. Click **OK**.

CMS Supervisor displays the Dictionary Logout Reason Codes window.

5. In the **Logout Reason Code Name** field, enter the name of the new logout reason code.
6. In the **Logout Reason Code** field, enter a number from 0 to 9 to be associated with the logout reason code name.

You can enter any other information about the logout reason code in the **Description** field.
You can enter only 50 or fewer characters in this field.
7. From the **Actions** menu, select **Add**.

Modifying a logout reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Logout Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to modify a logout reason code name.
4. Click **OK**.

CMS Supervisor displays the Dictionary Logout Reason Codes window.

5. To find a logout reason code to change, only one of the fields requires that you specify a value. Perform one of the following actions to specify a logout reason code in the Dictionary:
 - In the **Logout Reason Code Name** field, enter the name of the logout reason code.
 - In the **Logout Reason Code** field, enter the number from 0 to 9 that is associated with the logout reason code.
6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified logout reason code name, if valid.

7. In the **Logout Reason Code Name** field, enter the new name for the logout reason code.
8. From the **Actions** menu, select **Modify**.

The specified logout reason code name and the changes are saved to the Dictionary.

Deleting a logout reason code name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Logout Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which the logout reason code name to delete resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Logout Reason Codes window.

5. To find a logout reason code to delete, only one of the fields requires that you specify a value. Perform one of the following actions to specify a logout reason code in the Dictionary:

- In the **Logout Reason Code Name** field, enter the name of the logout reason code.
- In the **Logout Reason Code** field, enter the number from 0 to 9 that is associated with the logout reason code.

6. From the **Actions** menu, select **Find one**.

Supervisor retrieves and displays the information for the specified logout reason code name, if valid.

7. From the **Actions** menu, select **Delete**.

The specified logout reason code name is removed from the Dictionary.

Administering split/skill names in the Dictionary

You can assign names to the splits/skills for an ACD. These names are displayed in split/skill reports, making your reports easier to identify and read. The names you assign should reflect the configuration of your splits/skills and ACDs. For example, if you want skills to be divided according to Sales, Customer Service, and Wholesale, assign these names to the skills that handle those areas of the business.

 Note:

The Web Client does not support the administration of splits in a non-EAS environment.

Considerations for split/skill names

Consider the following when working with split/skill names in the Dictionary:

- Be consistent with the names given by your ACD switch administrator.
- If you assign a name, the name is displayed on reports and other pages instead of the split/skill number.
- If you make changes to split/skill names when viewing a report, you must exit the report and run it again to see the changes.

Adding a skill name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Splits/Skills**.
2. In the **Current ACD** list, select the active ACD for which you want to administer skills.
CMS Supervisor displays the list of skills administered for the selected ACD.
3. Click **Add Skill**.
4. In the **Split/Skill Number** field, enter the number for the skill.
The number can be a value from 1 to 8000.
5. In the **Split/Skill Name** field, enter a skill name.
6. In the **Description** field, enter a brief description with additional information.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
7. Click **OK** to save your changes.

Modifying a skill name in the Web Client

About this task

The **Split/Skill Number** field is read only and cannot be changed. You can change the associated name and description.

Procedure

1. Navigate to **Administration > Dictionary > Splits/Skills**.
2. In the **Current ACD** list, select the active ACD for which you want to administer skills.
CMS Supervisor displays the list of skills administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.

4. In the **Split/Skill Name** field, update the skill name.
5. **(Optional)** Revise the information in the **Description** field.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
6. Click **OK** to save your changes.

Deleting a skill name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Splits/Skills**.
2. In the **Current ACD** list, select the active ACD for which you want to administer skills.
CMS Supervisor displays the list of skills administered for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing a split/skill name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Split/Skill**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to view a split/skill.
4. Click **OK**.
CMS Supervisor displays the Dictionary Splits/Skills window.
5. To find a split/skill to view, only one of the fields requires a split/skill to be specified. Perform one of the following actions to specify an existing split/skill in the Dictionary:
 - In the **Split/Skill Name** field, enter the name of the split/skill.
 - In the **Split/Skill Number** field, enter the number of the split/skill.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified split/skill name, if valid.

Listing all split/skill names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Split/Skill**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Splits/Skills window.

4. In the **ACD** field, enter the ACD or ACD Group on which you want to view all split/skill names.
5. From the **Actions** menu, select **List all**.

Adding a split/skill name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Split/Skill**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to name a split/skill.
4. Click **OK**.

CMS Supervisor displays the Dictionary Splits/Skills window.

5. In the **Split/Skill Name** field, enter the name of the split/skill.
6. In the **Split/Skill Number** field, enter the number of the split/skill.

Any additional information about the split/skill can be entered in the **Description** field. Only 50 or fewer characters can be entered in this field.

7. From the **Actions** menu, select **Add**.

Modifying a split/skill name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Split/Skill**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to modify the split/skill name.
4. Click **OK**.

CMS Supervisor displays the Dictionary Splits/Skills window.

5. To find a split/skill to modify, only one of the fields requires a split/skill to be specified. Perform one of the following actions to specify an existing split/skill in the Dictionary:
 - In the **Split/Skill Name** field, enter the name of the split/skill.

- In the **Split/Skill Number** field, enter the number of the split/skill.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified split/skill name, if valid.
 7. In the **Split/Skill Name** field, enter the new name of the split/skill.
 8. From the **Actions** menu, select **Modify**.
The split/skill name and its changes are saved to the Dictionary.

Deleting a split/skill name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Split/Skill**.
3. In the **ACD** field, enter the ACD or ACD Group on which the split/skill name to delete resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary Splits/Skills window.
5. To find a split/skill to delete, only one of the fields requires a split/skill to be specified. Perform one of the following actions to specify an existing split/skill in the Dictionary:
 - In the **Split/Skill Name** field, enter the name of the split/skill.
 - In the **Split/Skill Number** field, enter the number of the split/skill.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified split/skill name, if valid.
7. From the **Actions** menu, select **Delete**.
The split/skill name is removed from the Dictionary.

Administering split/skill string values in the Dictionary

Split/skill string values are descriptive words used in split/skill call profile reports. These descriptive words are used instead of the split/skill numeric values. From the Split/Skill String Values page, you can change the default string values.

Considerations for split/skill string values

- If you assign values that are too long for standard reports, the values are truncated to fit on the reports. You can create similar custom reports to accommodate longer string values.
- If you do not assign different split/skill string values, the default values are used in reports.

Modifying split/skill string values in the Web Client

About this task

Default string values are predefined in CMS. You can change the default string values in the Dictionary.

Procedure

1. Navigate to **Administration > Dictionary > Split/Skill String Values**.
2. In the **Current ACD** list, select the active ACD for which you want to modify the default string values.
3. Enter a new string value in each field that you want to modify.
For a description of the values, see [Split/skill string value descriptions](#) on page 97.
4. Click **Apply** to save your changes.

Viewing split/skill string values using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Split/Skill String Values**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to view the split/skill string values.
4. Select **OK**.
CMS Supervisor displays the Dictionary Split/Skill String Values window.

Modifying split/skill string values using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Split/Skill String Values**.
3. In the **ACD** field, enter the ACD or ACD group for which you want to modify the split/skill string values.
4. Select **OK**.

CMS Supervisor displays the Dictionary Split/Skill String Values window.

5. Enter a new string value in each field that you want to modify.

For a description of the values, see [Split/skill string value descriptions](#) on page 97.

6. From the **Actions** menu, click **Modify**.

The split/skill string values and the changes are saved to the Dictionary.

Split/skill string value descriptions

You can modify the default string values on the Split/Skill String Values page. The following table describes the options available under each area:

Area	Description
Service Level Changed	The service level is the time limit in seconds for calls to wait in the queue before being answered. Split/skill Call Profile reports can be used to see how many calls were either answered or abandoned within each service level increment. The string values in the following fields are displayed in reports: • YES: The string value in this field is displayed if the service level in the split/skill call profile has changed. • NO: The string value in this field is displayed if the service level in the split/skill call profile has not changed.
Period Changed	There are ten time increments in the real-time and historical split/skill Call Profile reports. The length of the time increments is configurable. The string values in the following fields are displayed on the split/skill Call Profile report: • YES: The string value in this field is displayed if the time in the split/skill call profile has changed. • NO: The string value in this field is displayed if the time in the split/skill call profile has not changed.

Table continues...

Area	Description
Skill State	The string values in the following fields represent different skill states: • UNKNOWN: Leave the default value. The default value is UNKN. • Normal: Enter a descriptive word for the state of a skill using the Service Level Supervisor feature when the skill is less than all overload thresholds. The default value is NORMAL. • Overload1: Enter a descriptive word for the state of a skill using the Service Level Supervisor feature when the skill exceeds the first overload threshold. The default value is OVRLD1. • Overload2: Enter a descriptive word for the state of a skill using the Service Level Supervisor feature when the skill exceeds both the first and second thresholds. The default value is OVRLD2. • BEHIND: This string indicates that a skill is either close to or failing to meet the administered target service level, and agents are not being automatically reserved to compensate for this situation. The default value for this string is BEHIND. • AUTORSV: This string indicates that a skill is either close to or failing to meet the administered target service level. level. In this case, agents are automatically reserved to achieve the necessary level. The default value for this string is AUTORSV.

Standard CMS database items in the Dictionary

Standard CMS database items store ACD data and are used in default reports. These database items are in a read-only section of the Dictionary, so you cannot modify them. The Dictionary displays the name of each standard database item, the associated database table, and the item description.

The following example shows a current real-time agent table with standard CMS database item column headings:

Extension	Split	Logid	Logon start	Work mode	Started	Direction	Changed	>*
1000	1	4000	8:00	AVAIL	8:00	NULL	8:00	>
1001	1	5966	7:58	ACD	8:04	IN	8:04	>
1002	1	2200	7:59	ACD	8:03	IN	8:03	>
.	.	.	.	.	.	.	.	>

 Note:

“>*” indicates that more database item column headings follow. A dot indicates that more data follows down the table.

Viewing standard CMS database items in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Standard CMS Items**.
2. In the **Current ACD** list, select the active ACD for which you want to view standard CMS database items.

Viewing a standard CMS database item using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Standard CMS Items**.
3. Select **OK**.
CMS Supervisor displays the Dictionary Standard CMS Items window.
4. In the **Database Item** field, enter the name of the database item entirely in uppercase letters.

Important:

If you do not know the entire database item name, enter part of the database item name along with an asterisk (*) to find the item. You can use pattern searching in any field in the window.

You can also enter information in the **Table** field to limit the search of a database item to a single table.

5. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified standard database item, if valid.

Note:

If you used pattern matching in your search for a standard database item, it is possible that more than one match was found. To view the next database item that matches the search parameter, select **Next** from the **Actions** menu. Continue to select **Next** until the appropriate database item is found.

Viewing all standard CMS database items alphabetically using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Standard CMS Items**.
3. Select **OK**.

CMS Supervisor displays the Dictionary Standard CMS Items window.

4. From the **Actions** menu, select **List all**.

Administering tenants in the Dictionary

Use the Tenants window to add tenant names, numbers, and descriptions. The tenant names are displayed in reports.

To manage tenants names, you need permissions for the Dictionary subsystem and the tenant partition.

Before using tenant names

Install the Tenancy feature package first. Ensure that you have planned out the division of the following resources on the given ACD: Trunk groups, splits/skills, agent login IDs (logids), call work codes, and VDNs.

Adding a tenant name in the Web Client

About this task

You can define a tenant number and name in the Dictionary.

Procedure

1. Navigate to **Administration > Dictionary > Tenants**.
2. In the **Current ACD** list, select the active ACD for which you want to administer tenants.
CMS Supervisor displays the tenants administered for the selected ACD.
3. Click **Add Tenant**.
4. In the **Tenant Number** field, enter a numeric value between 0 and 250.
5. In the **Tenant Name** field, enter a name for the tenant.
6. In the **Description** field, enter a brief description with additional information.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
7. Click **OK** to save your changes.

Modifying a tenant name in the Web Client

About this task

The tenant number is read only and cannot be changed. You can change the tenant name and its description.

Procedure

1. Navigate to **Administration > Dictionary > Tenants**.
2. In the **Current ACD** list, select the active ACD for which you want to administer tenants.
CMS Supervisor displays the tenants administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. In the **Tenant Name** field, update the tenant name.
5. **(Optional)** Revise the information in the **Description** field.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
6. Click **OK** to save your changes.

Deleting a tenant name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Tenants**.
2. In the **Current ACD** list, select the active ACD for which you want to administer tenants.
CMS Supervisor displays the tenants administered for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing a tenant name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Tenants**.
3. In the **ACD** field, enter the ACD for which you want to view a tenant.
4. Click **OK**.
CMS Supervisor displays the Dictionary Tenants window.

5. To find a tenant partition to view, only one of the fields requires a tenant partition to be specified. Perform one of the following actions to specify an existing tenant in the Dictionary:

- a. In the **Tenant Name** field, enter the name of the tenant partition.
- b. In the **Tenant Number** field, enter the number of the tenant partition.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified tenant, if valid.

Listing all tenant names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Tenants**.
3. In the **ACD** field, enter the ACD for which you want to list all tenants and click **OK**.
CMS Supervisor displays the Dictionary Tenants window.
4. From the **Actions** menu, select **List all**.

Adding a tenant name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Tenants**.
3. In the **ACD** field, enter the ACD for which you want to add a tenant.
4. Click **OK**.
CMS Supervisor displays the Dictionary Tenants window.
5. In the **Tenant Name** field, enter the name of the tenant partition.
6. In the **Tenant Number** field, enter the number of the tenant partition.

Note:

The tenant partition must be assigned a number from 1 to 250.

7. From the **Actions** menu, select **Add**.

Modifying a tenant name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Tenants**.
3. In the **ACD** field, enter the ACD for which you want to modify a tenant and click **OK**.

CMS Supervisor displays the Dictionary Tenants window.

4. Perform one of the following actions to specify an existing tenant in the Dictionary:
 - a. In the **Tenant Name** field, enter the name of the tenant partition.
 - b. In the **Tenant Number** field, enter the number of the tenant partition.
5. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified tenant, if valid.

6. In the **Tenant Name** or **Description** field, make the necessary changes for the tenant partition.
7. From the **Actions** menu, select **Modify**.

Deleting a tenant name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
2. In the **Operations** list, highlight **Tenants**.
3. In the **ACD** field, enter the ACD for which you want to delete a tenant and click **OK**.

CMS Supervisor displays the Dictionary Tenants window.

4. Perform one of the following actions to specify an existing tenant in the Dictionary:
 - a. In the **Tenant Name** field, enter the name of the tenant partition.
 - b. In the **Tenant Number** field, enter the number of the tenant partition.
5. From the **Actions** menu, select **Delete**.

The selected tenant name is removed from the Dictionary.

Administering trunk group names in the Dictionary

Use the Trunk Groups window to assign names to ACD trunk groups. The trunk group names are displayed in reports.

Considerations for trunk group names

Consider the following when working with trunk group names in the Dictionary:

- Try to be consistent with the ACD switch naming for trunk groups and splits/skills.
- If you assign a trunk group name, the name is displayed on trunk group reports and other pages instead of the trunk group number.
- If you make changes to trunk group names while viewing a report that includes those trunk groups, you must exit the report and run it again to see the changes.

Adding a trunk group name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Trunk Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to administer trunk group names.

CMS Supervisor displays the trunk group names administered for the selected ACD.

3. Click **Add Trunk Group**.
4. In the **Trunk Group Number** field, enter a numeric value between 1 and 2000.
5. In the **Trunk Group Name** field, enter a trunk group name.
6. In the **Description** field, enter a brief description with additional information.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

7. Click **OK** to save your changes.

Modifying a trunk group name in the Web Client

About this task

The trunk group number is read only and cannot be changed. You can change the trunk group name and its description.

Procedure

1. Navigate to **Administration > Dictionary > Trunk Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to administer trunk group names.

CMS Supervisor displays the trunk group names administered for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. In the **Trunk Group Name** field, update the trunk group name.

5. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. Click **OK** to save your changes.

Deleting a trunk group name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Trunk Groups**.
2. In the **Current ACD** list, select the active ACD for which you want to administer trunk group names.
CMS Supervisor displays the trunk group names administered for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the change.

Viewing a trunk group name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to view a trunk group name.
4. Click **OK**.
CMS Supervisor displays The Dictionary Trunk Groups window.
5. To find a trunk group to view, only one of the fields requires a trunk group to be specified. Perform one of the following actions to specify an existing trunk group in the Dictionary:
 - In the **Trunk Group Name** field, enter the name of the trunk group.
 - In the **Trunk Group Number** field, enter the number of the trunk group.
6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified trunk group, if valid.

Listing all trunk group names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to list all trunk group names.
4. Click **OK**.

CMS Supervisor displays The Dictionary Trunk Groups window.

5. From the **Actions** menu, select **List all**.

Adding a trunk group name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to name a trunk group.
4. Click **OK**.

CMS Supervisor displays The Dictionary Trunk Groups window.

5. In the **Trunk Group Name** field, enter the name of the trunk group.
6. In the **Trunk Group Number** field, enter the number of the trunk group.

Any additional information about the trunk group can be entered in the **Description** field.
Only 50 or fewer characters can be entered in this field.

7. From the **Actions** menu, select **Add**.

Modifying a trunk group name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to modify a trunk group name.
4. Click **OK**.

CMS Supervisor displays The Dictionary Trunk Groups window.

5. To find a trunk group to modify, only one of the fields requires a trunk group to be specified. Perform one of the following actions to specify an existing trunk group in the Dictionary:
 - In the **Trunk Group Name** field, enter the name of the trunk group.
 - In the **Trunk Group Number** field, enter the number of the trunk group.
6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified trunk group, if valid.

7. In the **Trunk Group Name** or **Description** field, make the necessary changes for the trunk group.
8. From the **Actions** menu, select **Modify**.

Deleting a trunk group name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Trunk Group Name** list, highlight **Trunk Groups**.
3. In the **Trunk Group Number** field, enter the ACD on which the trunk group to delete resides.
4. Click **OK**.
CMS Supervisor displays The Dictionary Trunk Groups window.
5. To find a trunk group to delete, only one of the fields requires a trunk group to be specified. Perform one of the following actions to specify an existing trunk group in the Dictionary:
 - In the **Trunk Group Name** field, enter the name of the trunk group.
 - In the **Trunk Group Number** field, enter the number of the trunk group.
6. From the **Actions** menu, select **Delete**.
The selected trunk group name is removed from the Dictionary.

Administering trunk string values in the Dictionary

Trunk string values are descriptive words such as IDLE, HOLD, or QUEUED. You can change the default trunk string values to meet the needs of your call center. These string values are displayed in the data fields of trunk reports. They are not displayed as headings.

Administering trunk string values in the Web Client

About this task

You can modify the default values for trunk strings.

Procedure

1. Navigate to **Administration > Dictionary > Trunk String Values**.
2. In the **Current ACD** list, select the active ACD for which you want to modify trunk string values.

3. Enter a new string value in each field that you want to modify.

For a description of trunk string values, see [Trunk string value descriptions](#) on page 108.

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

Administering trunk string values using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
2. In the **Operations** list, highlight **Trunk String Values**.
3. Click **OK**.

CMS Supervisor displays the Dictionary Trunk String Values window.

4. To change any of the default names, enter the new descriptive word in the text box next to the name that you want to change.

For a description of trunk string values, see [Trunk string value descriptions](#) on page 108.

5. From the **Actions** menu, click **Modify** when the necessary changes have been completed.

Trunk string value descriptions

You can modify the default trunk string values. The following table describes the options available under each area:

Area	Description
Trunk State	To change any of the trunk state default names, enter a new descriptive word next to any of the following: • IDLE: The trunk is waiting for a call. • SEIZED: An incoming or outgoing call is holding the trunk. • QUEUED: An ACD call has seized the trunk, is queued to a split/skill, and is waiting for an agent to become available. • CONN: The caller and an agent are connected on a call. • DABN: The caller has abandoned the call. • FBUSY: The caller receives a forced busy signal. • FDISC: The caller is disconnected. • HOLD: The agent has put the caller on hold. • MBUSY: The trunk is out of service for maintenance purposes. • RINGING: The call is ringing at an agent's voice terminal. • UNKNOWN: CMS does not recognize the trunk state.

Table continues...

Area	Description
Queue Type	To change the queue type default names, enter a new descriptive name next to MAIN or BACKUP. The name entered here is displayed instead of the default value in real-time reports containing the trunk QUETYPE database item. Standard reports do not contain this item. • MAIN: The call was queued to a split/skill as a result of a <code>queue to main split/skill</code> vector command. • BACKUP: The call was queued to a split/skill as a result of a vector command other than <code>queue to main split/skill</code>.
Call Priority (Non-Vectoring)	To change the call priority (non-vectoring) default names, enter a new descriptive name next to YES or NO. The name entered here is displayed instead of the default name in real-time reports containing the trunk PRIORITY database item. Standard reports do not contain this item. • YES: The call occupying the trunk has priority entering the trunk. • NO: The call occupying the trunk does not have priority entering the split.
Call Priority (Vectoring)	To change the call priority (vectoring) default names, enter a new descriptive name next to LOW, MED, HIGH, or TOP. The priority level at which calls on a trunk queue to a split/skill is specified using either the <code>queue to split/skill</code> or <code>check split/skill</code> command in the vector that is processing the call. The name entered here is displayed instead of the default name in real-time reports containing the trunk PRIORITY database item. Standard reports do not contain this item. • LOW: The call occupying the trunk is queued to a split/skill at the lowest priority level. • MED: The call occupying the trunk is queued to a split/skill at the second lowest priority level. • HIGH: The call occupying the trunk is queued to a split/skill at the second highest priority level. • TOP: The call occupying the trunk is queued to a split/skill at the highest priority level.
Call Direction	To change the call direction default names, enter a new descriptive word next to IN or OUT. • IN: The trunk is on an incoming call. • OUT: The trunk is on an outbound call.
All Trunks Busy	To change the all trunks busy default names, enter a new descriptive word next to YES or NO. • YES: All trunks in the trunk group are busy (in use or maintenance). • NO: Not all trunks in the trunk group are busy.

Administering VDN names in the Dictionary

You can assign a name to each VDN. The assigned names are displayed instead of numbers on VDN reports and administration pages. Ensure that the VDN names reflect the configuration of your ACD and convey one or more of the following:

- The purpose of the VDN. For example, sales or customer service.
- The VDN destination vector. For example, FBusy-Nat.Accts.
- The trunk groups assigned to the VDN. For example, WATS 800-331-1111.

Considerations for VDN naming

Consider the following when working with VDN names in the Dictionary:

- To administer VDNs, the Call Vectoring feature must be enabled on the ACD switch.
- Ensure that VDNs are created on the switch and assigned for measurement through CMS.
- Try to be consistent with the VDN naming on the ACD switch.
- To get a list of VDNs, run the vector configuration report. To conserve system resources, only name VDNs that are being used instead of naming all VDNs.
- If you make changes to VDN names when a report that includes those VDNs is running, you must exit the report and run it again to see the changes.

Adding a VDN name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > VDNs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDN names.

CMS Supervisor displays the VDNs administered for the selected ACD.

3. Click **Add VDN**.

The VDN can contain 3 to 13 numbers.

4. In the **VDN** field, enter the VDN.
5. In the **VDN Name** field, enter a VDN name.
6. In the **Description** field, enter any additional information.

This field cannot contain a pipe symbol (|), double quotes ("), or a semi-colon (;).

7. Click **OK** to save your changes.

Modifying a VDN name in the Web Client

About this task

The VDN is read only and cannot be changed. You can change the VDN name and its description.

Procedure

1. Navigate to **Administration > Dictionary > VDNs**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDN names.

CMS Supervisor displays the VDNs administered for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

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

Removing a VDN name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > VDNs**.
2. In the **Current ACD** drop-down list, select the active ACD for which you want to administer VDNs.

CMS Supervisor displays the list of VDNs administered for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the change.

Viewing a VDN name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **VDNs**.
3. In the **ACD** field, enter the ACD on which you want to view a VDN.
4. Click **OK**.

CMS Supervisor displays the Dictionary VDNs window.

5. To find a VDN name to view, only one of the fields requires a VDN to be specified. Perform one of the following actions to specify an existing VDN in the Dictionary:

- In the **VDN Name** field, enter the name of the VDN.
- In the **VDN** field, enter the number of the VDN.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified VDN name, if valid.

Listing all VDN names

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **VDNs**.
3. In the **ACD** field, enter the ACD on which you want to view all the VDNs.
4. Click **OK**.
CMS Supervisor displays the Dictionary VDNs window.
5. From the **Actions** menu, select **List all**.

Adding a VDN name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **VDNs**.
3. In the **ACD** field, enter the ACD on which you want to name a VDN.
4. Click **OK**.
CMS Supervisor displays the Dictionary VDNs window.
5. In the **VDN Name** field, enter the name of the VDN.
6. In the **VDN** field, enter the number of the VDN.
Any additional information about the VDN, can be entered in the **Description** field. Only 50 or fewer characters can be entered in this field.
7. From the **Actions** menu, select **Add**.

Modifying a VDN name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **VDNs**.
3. In the **ACD** field, enter the ACD on which you want to modify the name of a VDN.
4. Click **OK**.
CMS Supervisor displays the Dictionary VDNs window.

5. To find a VDN name to modify, only one of the fields requires a VDN to be specified. Perform one of the following actions to specify an existing VDN in the Dictionary:
 - In the **VDN Name** field, enter the name of the VDN.
 - In the **VDN** field, enter the number of the VDN.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified VDN name, if valid.
7. In the **VDN Name** or **Description** field, make the necessary changes.
8. From the **Actions** menu, select **Modify**.

Deleting a VDN name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **VDNs**.
3. In the **ACD** field, enter the ACD on which the VDN you want to delete resides.
4. Click **OK**.
CMS Supervisor displays the Dictionary VDNs window.
5. To find a VDN name to delete, only one of the fields requires a VDN to be specified. Perform one of the following actions to specify an existing VDN in the Dictionary:
 - In the **VDN Name** field, enter the name of the VDN.
 - In the **VDN** field, enter the number of the VDN.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified VDN, if valid.
7. From the **Actions** menu, select **Delete**.
The name and description for this VDN is removed from the Dictionary.

Administering vector names in the Dictionary

A vector is a series of steps that the contact center uses to route calls and determine the treatment for each call. From the Use the Dictionary to assign names to vectors. The vector names are displayed instead of numbers on vector reports and administration pages. Ensure that vector names reflect the configuration of your ACD and convey one or more of the following:

- The vector's purpose. For example, sales or customer service.

- The VDNs assigned to the vector.
- The splits/skills to which the vector sends calls.

Considerations for vector names

Consider the following when working with vector names in the Dictionary:

- To administer vectors, the Call Vectoring feature must be enabled on the ACD switch.
- You can assign a name to a vector even if the steps to the vector have not been assigned.
- The number of available vectors depends on the switch type.
- If you make changes to vector names when a report that includes those vectors is running, you must exit the report and run it again to see the changes.

Adding a vector name in the Web Client

About this task

You can define a name for a vector in the Dictionary.

Procedure

1. Navigate to **Administration > Dictionary > Vectors**.
2. In the **Current ACD** list, select the active ACD for which you want to administer vectors.
CMS Supervisor displays the vectors administered for the selected ACD.
3. Click **Add Vectors**.
4. In the **Vector Number** field, enter the number for the vector.
You can enter a value between 1 and 8000.
5. In the **Vector Name** field, enter a vector name.
6. Click **OK** to save your changes.

Modifying a vector name in the Web Client

About this task

The vector number is read only and cannot be changed. You can change the vector name and its description.

Procedure

1. Navigate to **Administration > Dictionary > Vectors**.
2. In the **Current ACD** list, select the active ACD for which you want to administer vectors.
CMS Supervisor displays the vectors administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.

4. In the **Vector Name** field, update a vector name.
5. Click **OK** to save your changes.

Deleting a vector name in the Web Client

Procedure

1. Navigate to **Administration > Dictionary > Vectors**.
2. In the **Current ACD** list, select the active ACD for which you want to administer vectors.
CMS Supervisor displays the vectors administered for the selected ACD.
3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing a vector name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to view a vector name.
4. Click **OK**.
CMS Supervisor displays the Dictionary Vectors window.
5. To find a vector name to view, only one of the fields requires a vector to be specified. Perform one of the following actions to specify an existing vector in the Dictionary:
 - In the **Vector Name** field, enter the name of the vector.
 - In the **Vector Number** field, enter the number of the vector.
6. From the **Actions** menu, select **Find one**.
CMS Supervisor retrieves and displays the information for the specified vector, if valid.

Listing all vector names using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, select **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to list all vector names.

4. Click **OK**.

CMS Supervisor displays the Dictionary Vectors window.

5. From the **Actions** menu, select **List all**.

Adding a vector name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to name a vector.
4. Click **OK**.

CMS Supervisor displays the Dictionary Vectors window.

5. In the **Vector Name** field, enter the name of the vector.
6. In the **Vector Number** field, enter the number of the vector.

Any additional information about the vector, can be entered in the **Description** field. Only 50 or fewer characters can be entered in this field.

7. From the **Actions** menu, select **Add**.

Modifying a vector name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to modify a vector name.
4. Click **OK**.

CMS Supervisor displays the Dictionary Vectors window.

5. To find a vector name to modify, only one of the fields requires a vector to be specified. Perform one of the following actions to specify an existing vector in the Dictionary:

- In the **Vector Name** field, enter the name of the vector.
- In the **Vector Number** field, enter the number of the vector.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified vector, if valid.

7. In the **Vector Name** or **Description** field, make the necessary changes.
8. From the **Actions** menu, select **Modify**.

Deleting a vector name using the PC Client

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, select **Vectors**.
3. In the **ACD** field, enter the ACD on which the vector name to delete resides.
4. Click **OK**.

CMS Supervisor displays the Dictionary Vectors window.

5. To find a vector name to delete, only one of the fields requires a vector to be specified. Perform one of the following actions to specify an existing vector in the Dictionary:

- In the **Vector Name** field, enter the name of the vector.
- In the **Vector Number** field, enter the number of the vector.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor retrieves and displays the information for the specified vector, if valid.

7. From the **Actions** menu, select **Delete**.

The name for this vector is removed from the Dictionary.

Chapter 5: Administering call center features

This chapter provides information about configuring call center features. You must have permissions for the Call Center Administration subsystem. For some tasks, such as assigning synonyms to an ACD group, you also need permissions for the Dictionary subsystem.

The items in the **Call Center Administration** menu vary depending on the ACD system you are using (for example, Communication Manager) and the features enabled on it.

ACD group administration

An ACD group is an administrator-assigned collection of ACDs. Putting multiple ACDs in an ACD group enables you to easily administer Dictionary synonyms across several ACDs in one administrative operation. You can also run reports on ACD groups to get data about multiple ACDs.

Considerations for administering ACD groups

Consider the following when working with ACD groups:

Availability

When you add an ACD group, you need to log out of CMS Supervisor and log back in to see the new group.

Capacities/Performance

- A maximum of 12 ACD groups can exist on an Avaya CMS server.
- Each ACD group can contain up to eight ACDs.
- CMS must be in single-user mode to administer ACD groups.

Roles/Definitions

- An ACD group cannot serve as the CMS master ACD.
- An ACD group cannot be deleted if it is set as the current ACD.
- When you create ACD groups, CMS automatically assigns an ACD ID number, which you cannot change.

- Pseudo-ACDs cannot be a member of an ACD group.
- When an ACD group is deleted, all synonyms assigned to its member ACDs will remain.

Synonyms

- Entity synonyms must be unique for an ACD group and across all ACDs that are members of the ACD group.
- In overlapping ACD groups with common ACD members, entity IDs must be mutually exclusive. Otherwise, a synonym conflict can occur.

Other

- User permissions are administered separately for an ACD group and its member ACDs.
- CMS real-time custom reports are only displayed if data collection is enabled and the ACD link status is up for at least one member ACD in the specified ACD group. An error message will be displayed if these conditions are not met.
- Custom reports that are created with the single ACD option enabled cannot be run for an ACD group and vice versa.
- If a backup is created on a CMS server where the Global Dictionary feature is authorized, the data can only be restored on a CMS server that also has this feature authorized. If the Global Dictionary authorizations between a backup and the target CMS server do not match, an error is displayed, a message is written to the error log, and the restore or migration fails.

Benefits of using ACD groups

ACD groups are optional. The following is a detailed description of the advantages ACD groups provide:

Dictionary synonyms

You can easily administer synonyms in the Dictionary across multiple ACDs. A synonym assigned to a CMS entity in an ACD group is then propagated to all members ACDs within that group. For example, if you assign skill 102 in the ACD group with the synonym “Sales”, this synonym is assigned to skill 102 for all ACDs within the group. Use this capability if multiple ACDs require the same synonym for the following entities:

- Agent login IDs
- Agent groups
- Splits/skills
- AUX reason codes
- Logout reason codes
- Agent string values
- Split/skill string values
- Generic string value synonyms

Data reporting

You can run a custom report to get data about multiple ACDs. Reports for ACD groups collect, aggregate, and display call center data as a single value for the ACD group instead of one set of values for each member ACD. Custom reports can be created through the CMS ASCII interface.

Adding an ACD group in the Web Client

About this task

Use this procedure to create an ACD group. After creating an ACD group, add member ACDs to the group.

Procedure

1. Navigate to **Administration > Call Center Administration > ACD Groups**.
2. Click **Add ACD Group**.
3. In the **ACD Group Name** field, enter a name for the ACD group.
4. Click **OK** to save your changes.

Adding an ACD to an ACD group in the Web Client

About this task

Use this procedure to add an ACD to an ACD group. Repeat this procedure until the ACD group contains all required member ACDs.

Procedure

1. Navigate to **Administration > Call Center Administration > ACD Groups**.
2. Click **Group Contents** for one of the ACD groups.
3. Click **Add ACD**.
4. In the **ACD Number** list, select the ACD you want to add.
5. Click **OK** to save your changes.
6. When prompted, if you want to propagate reason codes and string-valued database items from the ACD group to the ACD, click **Yes**.

Deleting an ACD from an ACD group in the Web Client

About this task

Use this procedure to remove an ACD from an ACD group.

Procedure

1. Navigate to **Administration > Call Center Administration > ACD Groups**.
2. Click **Group Contents** for one of the ACD groups.
CMS Supervisor displays the list of ACDs administered for the ACD group.
3. When prompted, click **Delete Synonyms** if you want to delete ACD group synonyms from the ACD.
Alternatively, click **Keep Synonyms**.

Deleting an ACD group in the Web Client

About this task

You can delete an ACD group that is no longer required.

Procedure

1. Navigate to **Administration > Call Center Administration > ACD Groups**.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. When prompted, click **Yes** to save.

Listing ACD groups using the PC Client

About this task

This topic provides the procedure for listing all ACD groups defined on the CMS server.

Listing all ACD groups can be done through either the Call Center Administration or Dictionary subsystems. Only those CMS users who have “read” permission for the Call Center Administration subsystem can use the procedure listed below. CMS users who only work with synonyms or running reports should use the procedure associated with the Dictionary subsystem for listing all ACD groups.

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **Operations** list, select **ACD Groups**.
3. Click **OK**.
CMS Supervisor displays the Call Center Administration ACD Groups window.
4. From the menu bar, select **Edit > Clear All** to remove any data from the fields.
5. Select **Actions > List all**.
Supervisor displays a dialog listing the ACD groups defined on this CMS server.

Viewing the contents of an ACD group using the PC Client

About this task

This topic provides the procedure for displaying the contents of an ACD group.

Viewing the contents of an ACD group can be done through either the Call Center Administration or Dictionary subsystems. Only those CMS users who have “read” permission for the Call Center Administration subsystem can use the following procedure. CMS users who only work with synonyms or running reports should use the procedure in [Viewing ACD group information in the Dictionary](#) on page 44.

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **ACD Groups**.

3. Click **OK**.

CMS Supervisor displays the Call Center Administration ACD Groups window.

4. In the **ACD Group Name** field, enter the name of the ACD group you want to view.

 Note:

If you are unsure of the name of the ACD group, use [Listing ACD groups using the PC Client](#) on page 121 to determine the name.

5. From the menu bar, select **Actions > Find one**.

If the ACD group name is valid, its numeric ID is displayed in the **ACD Group Number** field and `1 matches found` is displayed in the status bar.

6. Select **Actions > Get contents**.

Supervisor displays the Call Center Admin ACD Groups Get contents dialog.

7. In the **ACD** drop-down list box, select **(none)**.

 Note:

If you do not select the **(none)** item, only the selected item in the ACD list will be displayed in the resulting dialog if it is a member of the specified ACD group. If it is not a member of the ACD group, the resulting dialog will be blank.

8. From the menu bar, select **Actions > List all**.

Supervisor displays the Call Center Admin ACD Groups Get Contents List All dialog showing all ACDs that are members of this ACD group.

Adding an ACD group using the PC Client

About this task

Use this procedure to create an ACD group. After creating an ACD group, add member ACDs using the procedure [Adding an ACD to an ACD group using the PC Client](#) on page 123.

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

CMS must be in single-user mode to administer ACD groups.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **ACD Groups**.

3. Click **OK**.

CMS Supervisor displays the Call Center Administration ACD Groups window.

4. In the **ACD Group Name** field, enter a name for this new ACD group.

5. From the menu bar, select **Actions > Add**.

CMS creates the ACD group and assigns an ACD group number.

Adding an ACD to an ACD group using the PC Client

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

CMS must be in single-user mode to administer ACD groups.

This procedure can only be done after an ACD group has been created. See [Adding an ACD group using the PC Client](#) on page 122 for more information.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **ACD Groups**.

3. Click **OK**.

CMS Supervisor displays the Call Center Administration ACD Groups window.

4. In the **ACD Group Name** field, enter the name of the ACD group that will receive a new ACD member.

5. Select **Actions > Find one** from the menu bar.

If the ACD group name is valid, its numeric ID is displayed in the **ACD Group Name** field and `1 matches found` is displayed in the status bar.

6. From the menu bar, select **Actions > Get contents**.

Supervisor displays the Call Center Admin ACD Groups Get contents dialog.

7. From the **ACD** drop-down list box, select the ACD that will be added to this group.

 Note:

If a CMS user does not have read and write permissions for an ACD, that ACD will not appear in this list. To view all of the ACDs assigned to this ACD group, see [Viewing the contents of an ACD group using the PC Client](#) on page 121.

8. Select **Actions > Add** from the menu bar.

The selected ACD is added to this ACD group and `Successful` is displayed in the status bar.

Modifying an ACD group name using the PC Client

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

CMS must be in single-user mode to administer ACD groups.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **ACD Groups**.

3. Click **OK**.

CMS Supervisor displays the Call Center Administration ACD Groups window.

4. In the **ACD Group Name** field, enter the name of the ACD group to change.

If you do not know the name of the ACD group, use the procedure, [Listing ACD groups using the PC Client](#) on page 121.

5. From the menu bar, select **Actions > Find one**.

If the ACD group name is valid, its numeric ID is displayed in the **ACD Group Number** field and `1 matches found` is displayed in the status bar.

6. In the **ACD Group Name** field, change the name of this ACD group.

See [Considerations for administering ACD groups](#) on page 118 for information on naming conventions.

7. When you have finished changing the name of the ACD group, select **Actions > Modify** from the menu bar.

The modification for the ACD group is made to the CMS database and `Successful` is displayed in the status bar.

Deleting an ACD from an ACD group using the PC Client

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

CMS must be in single-user mode to administer ACD groups.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **ACD Groups**.

3. Click **OK**.

CMS Supervisor displays the Call Center Administration ACD Groups window.

4. In the **ACD Group Name** field, enter the name of the ACD group from which you want to delete a member ACD.

 Note:

If you are unsure of the name of the ACD group, use the procedure, [Listing ACD groups using the PC Client](#) on page 121.

5. From the menu bar, select **Actions > Get contents**.

Supervisor displays the Call Center Admin ACD Groups Get contents dialog.

6. In the **ACD** drop-down list box, select the ACD to remove from this ACD group.

 Note:

If a CMS user does not have read and write permissions for an ACD, that ACD will not appear in this list. To view all of the ACDs assigned to this ACD group, see [Viewing the contents of an ACD group using the PC Client](#) on page 121.

7. From the menu bar, select **Actions > Find one**.

If the select ACD is a member of the specified ACD group, 1 matches found is displayed in the status bar.

8. Select **Actions > Delete**.

The selected ACD is removed from the specified ACD group and CMS Supervisor displays a message box asking if the synonyms assigned to this ACD should be removed as well.

9. Select the **OK** button to remove all synonyms that were assigned to this ACD through ACD group administration.

Otherwise, select **NO** to preserve all synonyms on the ACD.

Deleting an ACD group using the PC Client

Before you begin

Before doing this procedure, you should ensure that you have read and understood the considerations for administering ACD groups.

CMS must be in single-user mode to administer ACD groups.

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **ACD Groups**.

3. Click **OK**.

CMS Supervisor displays the Call Center Administration ACD Groups window.

4. In the **ACD Group Name** field, enter the name of the ACD group to delete.

If you do not know the name of the ACD group, you can find it using the procedure, [Listing ACD groups using the PC Client](#) on page 121.

5. Select **Actions > Find one** from the menu bar.

If the ACD group name is valid, its numeric ID is displayed in the **ACD Group Number** field and `1 matches found` is displayed in the status bar.

6. Select **Actions > Delete**.

The specified ACD group is deleted from the CMS server.

Call work code administration

A call work code is a number that represents a particular call type or call center activity. For example, promotional ads, complaints, or repeat orders. Agents enter call work codes to track customer-related information associated with a call. This information is sent to CMS for management reporting and can then be viewed in the call work code and call record historical reports.

Considerations for call work codes

Consider the following when working with call work codes:

- Call work codes must be positive integers with 1 to 16 digits. Try to consistently use a fixed number of digits to make it easier to add, delete, and search for call work codes.
- Call work code 0 is always assigned and is used to collect information on unassigned call work codes. Call work code 0 cannot be deleted. If an agent enters an unassigned call work code, it is displayed as code 0 on the call work code report. If a call work code exception

is defined, the agent exceptions historical report shows the agents who entered invalid or unassigned call work codes.

- Disk space must be allocated for call work codes. Call work codes are assigned to a specific ACD. The number of call work codes that can be assigned depends on the data storage allocation settings for the ACD. See [Data storage allocation](#) on page 278 for more information.
- Daily, weekly, and monthly standard historical reports are available for call work codes. Call work codes are also displayed on the standard historical call record report. For more information about reports, see *Avaya CMS Supervisor Reports*.
- You can assign names to call work codes in the Dictionary. The assigned name is displayed in reports instead of the numerical code.

Adding call work codes in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Call Work Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to administer call work codes.

CMS Supervisor displays the call work codes administered for the selected ACD.

3. Click **Add Call Work Code**.

Removing a single call work code in the Web Client

About this task

Use this procedure to remove an individual call work code.

Procedure

1. Navigate to **Administration > Call Center Administration > Call Work Codes**.
2. In the **Current ACD** list, select the active ACD for which you want to administer call work codes.

CMS Supervisor displays the call work codes administered for the selected ACD.

3. Click  to remove a single call work code.

The Confirm Delete dialog box is displayed. CMS Supervisor displays the Confirm Delete window.

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

Removing multiple call work codes in the Web Client

About this task

Use this procedure to remove multiple call work codes in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Call Work Codes**.
2. In the **Current ACD** drop-down list, select the active ACD for which you want to administer call work codes.
CMS Supervisor displays the list of call work codes administered for the selected ACD.
3. Click **Remove Call Work Code**.
CMS Supervisor displays the Remove Call Work Code(s) window.
4. In the **Call Work Codes** field, enter one or more call work codes that you want to delete.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
5. Click **OK** to save your changes.

Viewing call work codes using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **Operations** list, select **Call Work Code**.
3. Click **OK**.
CMS Supervisor displays the Call Work Codes window.
4. Enter the call work code to view in the **Call work code(s)** field.
5. Select **Actions > Find one**.
If the call work code exists in the CMS database, the status bar displays the message, 1 matches found.

Listing all call work codes using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **Operations** list, select **Call Work Code**.
3. Click **OK**.
CMS Supervisor displays the Call Work Codes window.
4. Select **Actions > List all**.
Supervisor displays a secondary window that lists all call work codes having a synonym in the Dictionary.

Adding call work codes using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **Call Work Code**.
3. Click **OK**.

CMS Supervisor displays the Call Work Codes window.

The following fields are displayed in the Call Work Codes window:

- **Number of codes allocated** - Total number of call work codes that exist in the CMS database
- **Number of codes administered** - Total number of call work codes currently in use
- **Call work code(s)** - Used to specify a call work code that will receive an action

4. Enter the new call work code in the **Call work code(s)** field.
5. Select **Actions > Add**.

The status bar displays `Successful` if the call work code is added to the CMS database.

Deleting call work codes using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **Operations** list, select **Call Work Code**.
3. Click **OK**.

CMS Supervisor displays the Call Work Codes window.

4. Enter the call work code that you want to delete in the **Call work code(s)** field.
5. Select **Actions > Find one**.

If the specified call work code is found in the CMS database, the status bar displays the message, `1 matches found`.

6. Select **Actions > Delete**.

The status bar displays `Successful` if the call work code is deleted from the CMS database.

Administration of VDN skill preferences

VDNs must be assigned to a vector through the ACD system. A VDN can connect calls to a vector when the calls arrive over an assigned automatic-in trunk group or when calls arrive over a dial-repeating, Direct Inward Dialing (DID) trunk group and the final digits match the VDN. The VDN can be dialed to access the vector from any extension that is connected to the switch.

Calls use VDN skills for routing based on the assigned preferences. You can use CMS Supervisor to change the first, second, and third skill preferences assigned to a VDN.

Related links

[Administration of VDN assignments](#) on page 140

Considerations for working with VDN skill preferences

Consider the following:

- When VDN skill preferences are changed through CMS Supervisor, the change takes place immediately on the Communication Manager system. This can affect the processing of calls at the time of the change.
- VDN skill preference changes can be run through scripts that can then be scheduled through a third-party scheduling application.

Changing VDN skill preferences in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Change VDN Skill Preferences**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDN skill preferences.

CMS Supervisor displays the VDNs and skill preferences administered for the selected ACD.
3. Click  next to the item you want to modify.

The Modify Item window is displayed.
4. To assign the same skill preferences to additional VDNs, enter VDN names or IDs in the VDNs field.

The VDNs you enter are displayed in the Search Results area.
5. Click + to move VDNs from the Search Results area to the Selected VDNs area.
6. Enter up to three preferred skills in the **Skill Preferences** fields.
7. Click **OK** to save your changes.

Viewing VDN skill preferences using the PC Client

Procedure

1. From the Controller window, select **Commands > Call Center Administration**.

Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which VDN skill preferences will be viewed.
3. In the **Operations** list, highlight **Change VDN Skill Preferences**.
4. Select **OK**.

Supervisor displays the Change VDN Skill Preferences window.

5. In the **VDNs** field, enter the VDN for which skill preferences are to be viewed.
6. Select **Actions > Find one**.

The status bar displays a successful message if the VDN was found and lists the skill preferences, if any exist for this VDN.

Listing all VDN skill preferences using the PC Client

Procedure

1. From the Controller window, select **Commands > Call Center Administration**.

Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which the VDNs and their skill preferences will be viewed.
3. In the **Operations** list, highlight **Change VDN Skill Preferences**.
4. Select **OK**.

Supervisor displays the Change VDN Skill Preferences window.

5. Select **Actions > List all**.

Supervisor displays a window listing all VDNs on this ACD and the associated skill preferences.

Changing VDN skill preferences using the PC Client

Procedure

1. From the Controller window, select **Commands > Call Center Administration**.

Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which VDN skill preferences will be changed.
3. In the **Operations** list, highlight **Change VDN Skill Preferences**.
4. Select **OK**.

Supervisor displays the Change VDN Skill Preferences window.

5. In the **VDNs** field, enter the VDN for which skill preferences are to be changed.

6. Select **Actions > Find one**.

The status bar displays a successful message if the VDN was found.

7. Enter skill preferences for the VDN in the **1st**, **2nd**, and **3rd** fields using one of the following methods:

- Enter the skill name or number.
- Select the skill name or number from the drop-down list.
- Use the Browse button at the right of each field to select a skill.

8. Select **Actions > Modify**.

The status bar displays a successful message when the operation completes.

Split/skill call profile administration

Call profiles are settings for a split/skill that assist in determining how much time passes before a call is answered or abandoned. The accumulated number of seconds that have passed for an unanswered call are divided into different service-level increments. If a call surpasses the allocated time for the first service-level increment, it then moves to the next service-level increment. This information is recorded for each call and can later be viewed through the split/skill call profile report to determine the number of calls that were answered or abandoned in each increment.

Considerations for split/skill call profiles

Consider the following when working with split/skill call profiles:

- Each service-level increment value can be set to a different length of time in seconds.
- Each of the first nine service-level increments can have a different time length. Each represents a unit of wait time. The number of seconds for the second through the ninth increment must be at least one second greater than the number of seconds in the previous increment.
- CMS counts the calls that are either answered or abandoned within each increment and shows the totals on split/skill call profile reports. Therefore, the settings of these increments affect what is displayed in reports.
- To ensure that reports display accurate data, avoid making changes to the service level after data is collected. If you must change the service level, it is best to change the value at midnight on the first day of a month so that data for the entire month is gathered using the same service level value.

Adding split/skill call profiles in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Split/Skill Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer split/skill call profiles.
CMS Supervisor displays the split/ skill call profiles administered for the selected ACD.
3. Click **Add Split/Skill**.
4. In the **Split/Skill** field, enter split/skill names or IDs.
The system displays each entry in the **Search Results** pane.
5. Click each name or ID that you want to administer to move it into the **Selected Split(s)/ Skill(s)** pane.
6. In the **Acceptable service level** field, enter the speed of answer objective for the profile. The acceptable service level represents the maximum number of seconds for a call to be answered.
 - You must enter a value in this field.
 - Valid values are 0 to 9999.
 - This value should not be larger than intrahour interval set on CMS. For example; less than 1800 for a 30-minute intrahour interval or 3600 for a 60-minute intrahour interval.
7. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **To** field. Each field can support values from 0 to 999. If the unanswered call surpasses the time limit for an increment, it moves on to the next increment. For example, 0 to 5 to 10 to 25 represents 0 to 5 seconds, 6 to 10 seconds, and 11 to 25 seconds. Each of the nine increments can vary in length.
8. Click **OK** to save your changes.

Modifying a split/skill call profile in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Split/Skill Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer split/skill call profiles.
CMS Supervisor displays the split/skill call profiles administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. In the **Acceptable service level** field, update the speed of answer objective for the profile.

Acceptable service level represents the maximum number of seconds it should take for a call to be answered.

5. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **to** field.
6. Click **OK** to save your changes.

Removing a single split/skill profile in the Web client

About this task

Use this procedure to remove an individual single split/skill profile.

Procedure

1. Navigate to **Administration > Call Center Administration > Split/Skill Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer split/skill call profiles.

CMS Supervisor displays the list of split/skill call profiles administered for the selected ACD.
3. Click  to remove a single split/skill profile.
The Confirm Delete dialog box is displayed.
4. Click **OK** to save your changes.

Removing multiple split/skill profiles in the Web client

About this task

Use this procedure to remove split/skill profiles in bulk.

Procedure

1. Navigate to **Administration > Call Center Administration > Split/Skill Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer split/skill call profiles.

CMS Supervisor displays the list of split/skill call profiles administered for the selected ACD.
3. Click **Remove Split/skill**. CMS Supervisor displays the **Remove Split/skill** window.
4. In the **Split/skill** window, enter one or more split/skill profiles that you want to remove.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
5. Click **OK** to save your changes.

Viewing split/skill call profiles using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which the existing split or skill call profile resides.
3. In the **Operations** list, select **Split/Skill Call Profile Setup**.
4. Click **OK**.

CMS Supervisor displays the Split/Skill Call Profile Setup window.

5. In the **Split(s)/Skill(s)** field, enter the split or skill that is represented by the call profile to view.
6. From the **Actions** menu, select **Find one**.

The status bar displays a *Successful* message if the call profile for the specified split or skill is found. Additionally, Supervisor populates the **Service Level Increments (seconds)** fields with the service level increments for this call profile.

Adding split/skill call profiles using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which the new split or skill call profile will be created.
3. In the **Operations** list, select **Split/Skill Call Profile Setup**.
4. Click **OK**.

CMS Supervisor displays the Split/Skill Call Profile Setup window.

5. In the **Split(s)/Skill(s)** field, enter the split or skill numbers or names.
6. In the **Acceptable service level** field, enter the speed of answer objective for the profile.

Acceptable service level represents the maximum number of seconds it should take for a call to be answered. Valid values are 0 to 9999. This value should be no larger than the number of seconds in the intrahour interval that is set on CMS. For example, 1800 for a 30-minute intrahour interval or 3600 for a 60-minute intrahour interval. You must enter a value in this field.

7. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **To** field. Each field can support values from 0 to 999.

If the unanswered call surpasses the time limit for an increment, it moves on to the next increment. For example, 0 to 5 to 10 to 25 represents 0 to 5 seconds, 6 to 10 seconds, and 11 to 25 seconds.

Each of the nine increments can vary in length. For example, 0 to 15, 16 to 20, 21 to 26, 27 to 38, 39 to 43, and so forth.

The following example displays how an administrator might set up a call profile:

The screenshot shows a configuration window for a call profile. At the top, there is a field labeled "Acceptable service level:" with the value "1800" entered. Below this, a section titled "Service level increments (seconds):" contains ten increments, labeled "Inc 1" through "Inc 10". Each increment is defined by a range of seconds, with the start and end values entered in separate boxes. The ranges are: Inc 1 (0 to 5), Inc 2 (5 to 15), Inc 3 (15 to 30), Inc 4 (30 to 60), Inc 5 (60 to 90), Inc 6 (90 to 120), Inc 7 (120 to 180), Inc 8 (180 to 240), Inc 9 (240 to 360), and Inc 10 (360 and above). The "and above" text is placed after the final box for Inc 10.

Inc	Start (seconds)	End (seconds)
Inc 1	0	5
Inc 2	5	15
Inc 3	15	30
Inc 4	30	60
Inc 5	60	90
Inc 6	90	120
Inc 7	120	180
Inc 8	180	240
Inc 9	240	360
Inc 10	360	and above

In this example, the **Acceptable service level** field is set to 1800 seconds to correspond with the intrahour interval on the CMS server.

Inc 1 has been set for the range of 0 to 5 seconds. **Inc 2** ranges covers 5 to 15 seconds. The other service level increments continue on until **Inc 10**. This last service level increment is used in this example is for those calls that extend beyond 360 seconds. If a call is not answered after the acceptable service level of 1800 seconds, the call is then tracked in a different CMS database category.

8. Select **Actions > Add**.

The status bar displays a message stating if the operation succeeded or failed.

Modifying a split/skill call profile using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD on which the split or skill call profile to modify resides.
3. In the **Operations** list, select **Split/Skill Call Profile Setup**.
4. Click **OK**.

CMS Supervisor displays the Split/Skill Call Profile Setup window.

5. In the **Split(s)/Skill(s)** field, enter the split or skill on which the call profile to modify resides.
6. Select **Actions > Find one**.

The status bar displays a **Successful** message if the call profile for the specified split or skill is found. Additionally, Supervisor populates the **Service Level Increments (seconds)** fields with the service level increments for this call profile.

7. In the **Acceptable service level** field, enter the speed of answer objective for the profile.

Acceptable service level represents the maximum number of seconds it should take for a call to be answered. Valid values are 0 to 9999. This value should be no larger than the number of seconds in the intrahour interval that is set on CMS. For example, 1800 for a 30-minute intrahour interval or 3600 for a 60-minute intrahour interval. You must enter a value in this field.

8. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **To** field. Each field can support values from 0 to 999.

If the unanswered call surpasses the time limit for an increment, it moves on to the next increment. For example, 0 to 5 to 10 to 25 represents 0 to 5 seconds, 6 to 10 seconds, and 11 to 25 seconds.

Each of the nine increments can vary in length. For example, 0 to 15, 16 to 20, 21 to 26, 27 to 38, 39 to 43, and so forth.

The following example displays how an administrator might set up a call profile:

The screenshot shows a configuration window for a call profile. At the top, the 'Acceptable service level' is set to 1800. Below this, the 'Service level increments (seconds)' section is displayed. It contains two rows of increment fields. The first row shows increments 1 through 5: Inc 1 (0 to 5), Inc 2 (5 to 15), Inc 3 (15 to 30), Inc 4 (30 to 60), and Inc 5 (60 to 90). The second row shows increments 6 through 10: Inc 6 (90 to 120), Inc 7 (120 to 180), Inc 8 (180 to 240), Inc 9 (240 to 360), and Inc 10 (360 and above). Each increment is represented by a 'to' field with a numerical value in a text box.

In this example, the **Acceptable service level** field is set to 1800 seconds to correspond with the intrahour interval on the CMS server.

Inc 1 has been set for the range of 0 to 5 seconds. **Inc 2** ranges covers 5 to 15 seconds. The other service level increments continue on until **Inc 10**. This last service level increment is used in this example is for those calls that extend beyond 360 seconds. If a call is not answered after the acceptable service level of 1800 seconds, the call is then tracked in a different CMS database category.

9. From the **Actions** menu, select **Modify**.

The status bar displays a `Successful` message when the operation completes.

Deleting a split/skill call profile using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which the split or skill call profile to delete resides.
3. In the **Operations** list, select **Split/Skill Call Profile Setup**.
4. Click **OK**.

CMS Supervisor displays the Split/Skill Call Profile Setup window.

5. In the **Split(s)/Skill(s)** field, enter the split or skill on which the call profile to delete resides.
6. From the **Actions** menu, select **Find one**.

The status bar displays a `Successful` message if the call profile for the specified split or skill is found. Additionally, Supervisor populates the **Service Level Increments (seconds)** fields with the service level increments for this call profile.

7. From the **Actions** menu, select **Delete**.

Supervisor deletes the specified split or skill call profile and displays a `Successful` message in the status bar.

About viewing trunk group assignments

A trunk group is a group of circuits that are assigned the same dialing digits, either a telephone number or a DID prefix. Trunk groups can be assigned to VDNs or non-vector-controlled splits.

To add or change trunk group assignments, you must use the administration tool for your ACD system. You can only view trunk group assignments in CMS Supervisor, but you cannot change them from there. Therefore, you only need Read permissions for the Call Center Administration subsystem and for the affected trunk groups, splits, and VDNs.

Considerations for trunk group assignments

- You cannot use these procedures to change trunk group assignments. You can only change trunk group assignments from the administration tool for the ACD system (for example, Communication Manager).
- Automatic-in trunk groups, such as those that are used as Listed Directory Numbers, must be assigned to VDNs or splits through the ACD system.
- DID or dial-repeating trunks, such as those that toll-free numbers are assigned to, are not assigned to VDNs or splits. The Central Office (CO) passes VDN digits or the split extension number to the ACD system.
- Vector-controlled splits cannot have trunk groups assigned to them because they can only receive calls through vector processing.

Viewing trunk group assignments using the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Trunk Group Assignments**.
2. In the **Current ACD** drop-down list, select the active ACD for which you want to view the trunk groups assigned.

CMS Supervisor displays the trunk groups assigned for the selected ACD.

Viewing all trunk group assignments using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD on which trunk group assignments are to be viewed.
3. In the **Operations** list, highlight **Trunk Group Assignments**.

4. Click **OK**.

Supervisor displays the Trunk Group Assign window.

5. With all fields blank, select **Actions > List all**.

Supervisor displays the Trunk Group Assignments - List All window showing all trunk groups and their current assignments.

6. To clear all fields of information, select **Edit > Clear All**.

Viewing a single trunk group assignment using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD for which trunk group assignments are to be viewed.
3. In the **Operations** list, highlight **Trunk Group Assignments**.

4. Click **OK**.

Supervisor displays the Trunk Group Assign window.

5. In the **Trunk Groups** field, enter the trunk group for which assignments are to be viewed.

More than one trunk group can be entered in this field. Multiple trunk groups must be separated with a semicolon (;).

6. Select **Actions > Find one**.

The VDN or split assignment for the specified trunk group is displayed in the corresponding field.

If a VDN or split is not assigned to this trunk group, the status bar displays 0 matches found.

Viewing a trunk group assignment by VDN or split using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD for which trunk group assignments are to be viewed.
3. In the **Operations** list, highlight **Trunk Group Assignments**.
4. Click **OK**.

Supervisor displays the Trunk Group Assign window.

Either a VDN or split can be specified to display the trunk group or groups assigned to it. Complete one of the following two steps.

5. To display the trunk groups that are assigned to a VDN:
 - a. In the **Select one** group, select **VDN**.
 - b. Enter the VDN number or name in the field for the **VDN** option.
6. To display the trunk groups that are assigned to a split:
 - a. In the **Select one** group, select **Split**.
 - b. Enter the split number or name in the field for the **Split** option.
7. Select **Actions > Find one**.

Supervisor displays the first trunk group that is assigned to the specified VDN or split in the **Trunk Groups** field. If more trunk groups are currently assigned, click the **Next** button to view them.

Administration of VDN assignments

A VDN is an extension number that enables incoming calls to be connected to a vector for processing. A VDN is not assigned an equipment location, but it is assigned to a vector. You can dial the VDN by itself to access the vector from any extension that is connected to the ACD system.

Initial assignment of a VDN to a vector is done on the ACD system. However, you can change it later in CMS Supervisor.

Considerations for VDN assignments

Consider the following when working with VDN assignments:

- Changing any VDN-to-vector assignments can alter call processing.
- Multiple VDNs can be assigned to the same vector.
- VDNs cannot be assigned to more than one vector.
- You cannot exit the VDN-to-vector assignment window until CMS Supervisor receives a response to the requested change.
- Calls that are already in vector processing are not affected by a VDN-to-vector change.
- Changing the VDN-to-vector assignment affects the next call that enters the VDN.
- VDN-to-vector assignment changes that are scheduled should either be grouped together in a timetable or individually scheduled so that one assignment is completed before the next assignment change request is scheduled.

Managing VDN assignments in the Web Client

About this task

VDNs assignments are set up in the ACD system. You can modify them in CMS Supervisor.

Procedure

1. Navigate to **Administration > Call Center Administration > VDN Assignments**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDNs.
CMS Supervisor displays the VDNs administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. **(Optional)** Enter additional VDN names or IDs in the **VDNs** field. Do this only if you want to assign the same vectors to additional VDNs in addition to the VDN you originally selected. Separate entries using a semicolon (;).
The **Search Results** pane is displayed.
5. **(Optional)** Click each VDN to which you want to assign the same vector and move it into the **Selected VDN(s)** pane.
6. In the **Vector** list, select a vector to associate with the **VDNs**.
7. Click **OK** to save your changes.

Viewing VDN assignments using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD for which VDN-to-vector assignments are to be viewed.
3. In the **Operations** list, highlight **VDN Assignments**.
4. Click **OK**.

CMS Supervisor displays the VDN Assignments window.

5. Select **Actions > List all** from the menu bar.

CMS Supervisor displays a secondary window that lists all VDNs for which this user ID has “read” permission.

Listing VDNs associated with a vector using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which the vector resides.
3. In the **Operations** list, highlight **VDN Assignments**.
4. Click **OK**.

CMS Supervisor displays the VDN Assignments window.

5. In the **Vector** field, enter the name or number of the vector.
6. Select **Actions > List all** from the menu bar.

CMS Supervisor displays a secondary window that lists all VDNs assigned to the specified vector.

Administration of VDN call profiles

Call profiles are time ranges for a VDN that CMS uses to track how much time passes before a call is resolved by being answered, connected to a non-ACD destination, or abandoned. CMS refers to these time ranges as “service-level increments”.

The accumulated number of seconds that pass for an unanswered call are divided into different service-level increments. If a call surpasses the allocated time for the first service-level increment, it then moves to the next service-level increment. This information is recorded for each call and can later be viewed through VDN call profile reports to determine the number of calls addressed in each increment.

Considerations for administering VDN call profiles

Consider the following when working with VDN call profiles:

- When installed, CMS sets all service-level increments to 0 by default. This causes all calls to appear in the first increment on the VDN call profile report.
- Each service level can be set to different lengths of time.
- Service-level increments can only be used to categorize a call to a maximum limit of 999 seconds.
- The number of seconds for the second through the ninth increment must be at least 1 second higher than the number of seconds in the previous increment. For example, if the second increment covers the range of 5 to 10 seconds, the maximum value in the third increment must be set to 11 or higher.
- To ensure that reports display accurate data, avoid making changes to the service level after data is collected. If you must change the service level, it is best to change the value at midnight on the first day of a month so that data for the entire month is gathered using the same service level value.

Adding a VDN call profile in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > VDN Call Profile Setup**.

2. In the **Current ACD** list, select the active ACD for which you want to administer VDN call profiles.

CMS Supervisor displays the VDN call profiles administered for the selected ACD.

3. Click **Add VDNs**.

4. In the **VDNs** field, enter one or more VDN names.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

5. Click each name or ID that you want to administer to move it into the **Selected VDN(s)** pane.

6. Click **+** to move the VDNs from the Search Results area to the Selected VDN(s) area.

7. In the **Acceptable service level** field, enter the speed of answer objective for the profile. Acceptable service level represents the maximum number of seconds it should take for a call to be answered. Valid values are 0 to 9999. This value should be no larger than the number of seconds in the intrahour interval that is set on CMS.

8. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each To field.

If the unanswered call surpasses the time limit for an increment, it moves on to the next increment. For example, 0 to 5 to 10 to 25 represents 0 to 5 seconds, 6 to 10 seconds, and 11 to 25 seconds.

9. Click **OK** to save your changes.

Modifying a VDN call profile in the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > VDN Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDN call profiles.
CMS Supervisor displays the VDN call profiles administered for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. In the **Acceptable service level** field, update the speed of answer objective for the profile. Acceptable service level represents the maximum number of seconds it should take for a call to be answered.
5. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **to** field.
6. Click **OK** to save your changes.

Removing an individual VDN call profile in the Web Client

About this task

You can remove a VDN call profile that no longer needed. Use this procedure to remove one VDN call profile at a time.

Procedure

1. Navigate to **Administration > Call Center Administration > VDN Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDN call profiles.
CMS Supervisor displays the VDN call profiles administered for the selected ACD.
3. Click  you want to remove.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Removing multiple VDN call profiles in the Web Client

About this task

You can remove VDNs in bulk. Specify which VDNs you no longer need and remove them at one go.

Procedure

1. Navigate to **Administration > Call Center Administration > VDN Call Profile Setup**.
2. In the **Current ACD** list, select the active ACD for which you want to administer VDN call profiles.
CMS Supervisor displays the VDN call profiles administered for the selected ACD.
3. Click **Remove VDNs**.
4. From the **VDNs** field, enter the names of **VDNs** that is no longer needed.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
5. Click **+** to move VDNs from the Search Results area to the Selected VDN(s) area.
The VDNs in the Selected VDN(s) area will be removed.
6. Click **OK** to save your changes.

Viewing a VDN call profile using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD on which the VDN call profile will be viewed.
3. In the **Operations** list, select **VDN Call Profile Setup**.
4. Click **OK**.
CMS Supervisor displays the VDN Call Profile Setup window.
5. In the **VDNs** field, enter the name or number of the VDN for which the associated call profile is to be viewed.
6. Select **Actions > Find one** from the menu bar.
Supervisor populates the remaining fields on the VDN Call Profile Setup window with the call profile settings for this VDN. If no call profile has been created for this VDN, the **Service Level Increments (seconds)** values are set to 0.

Adding a VDN call profile using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD on which the VDN call profile will be added.
3. In the **Operations** list, select **VDN Call Profile Setup**.

4. Click **OK**.

CMS Supervisor displays the VDN Call Profile Setup window.

5. In the **VDNs** field, enter the name or number of the VDN which will have a new call profile.

6. In the **Acceptable service level** field, enter the speed of answer objective for the profile.

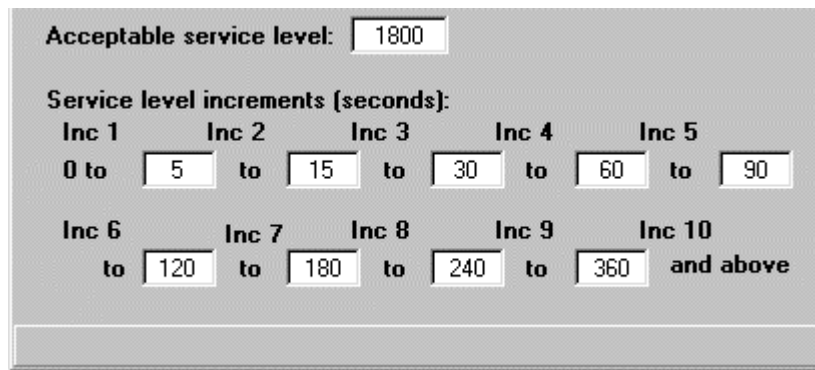
Acceptable service level represents the maximum number of seconds it should take for a call to be answered. Valid values are 0 to 9999. This value should be no larger than the number of seconds in the intrahour interval that is set on CMS. For example, 1800 for a 30-minute intrahour interval or 3600 for a 60-minute intrahour interval. You must enter a value in this field.

7. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **To** field. Each field can support values from 0 to 999.

If the unanswered call surpasses the time limit for an increment, it moves on to the next increment. For example, 0 to 5 to 10 to 25 represents 0 to 5 seconds, 6 to 10 seconds, and 11 to 25 seconds.

Each of the nine increments can vary in length. For example, 0 to 15, 16 to 20, 21 to 26, 27 to 38, 39 to 43, and so forth.

The following example displays how an administrator might set up a call profile:



The screenshot shows a window titled "VDN Call Profile Setup". It has two main sections. The first section is "Acceptable service level:" with a text box containing "1800". The second section is "Service level increments (seconds):". It contains ten rows of input fields. The first row is labeled "Inc 1" and has fields "0 to", "5", "to", "15", "to", "30", "to", "60", "to", "90". The second row is labeled "Inc 2" and has fields "to", "120", "to", "180", "to", "240", "to", "360", and "and above". The other rows are labeled "Inc 3" through "Inc 10" and have similar field structures.

In this example, the **Acceptable service level** field is set to 1800 seconds to correspond with the intrahour interval on the CMS server.

Inc 1 has been set for the range of 0 to 5 seconds. **Inc 2** ranges covers 5 to 15 seconds. The other service level increments continue on until **Inc 10**. This last service level increment is used in this example is for those calls that extend beyond 360 seconds. If a call is not answered after the acceptable service level of 1800 seconds, the call is then tracked in a different CMS database category.

8. Select **Actions > Add** from the menu bar.

The status bar displays a `Successful` message when the operation completes.

Modifying a VDN call profile using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. In the **ACD** field, select the ACD on which the VDN call profile will be modified.
3. In the **Operations** list, select **VDN Call Profile Setup**.
4. Click **OK**.

CMS Supervisor displays the VDN Call Profile Setup window.

5. In the **VDNs** field, enter the name or number of the VDN for which the associated call profile is to be modified.
6. Select **Actions > Find one** from the menu bar.

Supervisor populates the remaining fields on the VDN Call Profile Setup window with the call profile settings for this VDN. If no call profile has been created for this VDN, the **Service Level Increments (seconds)** values are set to 0.

7. In the **Acceptable service level** field, enter the speed of answer objective for the profile.

Acceptable service level represents the maximum number of seconds it should take for a call to be answered. Valid values are 0 to 9999. This value should be no larger than the number of seconds in the intrahour interval that is set on CMS. For example, 1800 for a 30-minute intrahour interval or 3600 for a 60-minute intrahour interval. You must enter a value in this field.

8. In the **Service Level Increments (seconds)** fields, enter a progressively greater number of seconds in each **To** field. Each field can support values from 0 to 999.

If the unanswered call surpasses the time limit for an increment, it moves on to the next increment. For example, 0 to 5 to 10 to 25 represents 0 to 5 seconds, 6 to 10 seconds, and 11 to 25 seconds.

Each of the nine increments can vary in length. For example, 0 to 15, 16 to 20, 21 to 26, 27 to 38, 39 to 43, and so forth.

The following example displays how an administrator might set up a call profile:

Acceptable service level: 1800

Service level increments (seconds):

Inc	Start	End
Inc 1	0	5
Inc 2	5	15
Inc 3	15	30
Inc 4	30	60
Inc 5	60	90
Inc 6	90	120
Inc 7	120	180
Inc 8	180	240
Inc 9	240	360
Inc 10	360	and above

In this example, the **Acceptable service level** field is set to 1800 seconds to correspond with the intrahour interval on the CMS server.

Inc 1 has been set for the range of 0 to 5 seconds. **Inc 2** ranges covers 5 to 15 seconds. The other service level increments continue on until **Inc 10**. This last service level increment is used in this example is for those calls that extend beyond 360 seconds. If a call is not answered after the acceptable service level of 1800 seconds, the call is then tracked in a different CMS database category.

9. Select **Actions > Modify** from the menu bar.

The status bar displays a `Successful` message when the operation completes.

Deleting a VDN call profile using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.
CMS Supervisor displays the Call Center Administration window.
2. In the **ACD** field, select the ACD on which the VDN call profile will be deleted.
3. In the **Operations** list, select **VDN Call Profile Setup**.
4. Click **OK**.

CMS Supervisor displays the VDN Call Profile Setup window.

5. In the **VDNs** field, enter the name or number of the VDN for which the associated call profile is to be deleted.
6. Select **Actions > Find one** from the menu bar.

Supervisor displays the call profile data for the selected VDN in the **Acceptable service level** and **Service Level Increments (seconds)** fields.

7. Select **Actions > Delete** from the menu bar.

The status bar displays a `Successful` message when the operation completes.

Administering a data summarization time zone using the PC Client

About this task

To allow for alternative time zone reporting for daily, weekly, and monthly data, a second time zone can be defined to archive the data. This second time zone is in addition to the default ACD time zone. Doing this results in aggregating the data for two different time zones. Each time zone is aggregated based on the boundary of a day for the selected time zone. You can choose one time zone from the possible 600+ time zones to use as the second time zone for an ACD.

If tenant partitioning is installed, the user can define a time zone for each tenant within an ACD and choose from those time zones to have the data additionally aggregated. This results in storing the data in up to three different time zones. With the multi-tenancy feature installed, one time zone per tenant and one additional time zone for the ACD are supported.

In addition, the agent trace and exception data will be stored in UTC/GMT time enabling filtering and reporting of agent trace and exception data based on the time zone selected on CMS Supervisor.

* Note:

The administration of time zones does not automatically create the time zone data in the daily, weekly, and monthly tables. The Archiver must run after the time zone is administered.

Before you begin

Change the system to single-user state before you do this task.

Procedure

1. From the Controller window, select **Tools > System Setup**.
2. In the CMS System Setup window, select **Data Summarization Time Zone** in the **Operations** list.
3. In the System Setup Data Summarization Time Zone window, do any of the following operations as explained in the table below:

* Note:

The System Setup Data Summarization Time Zone window displays the tenant option only if the customer has installed the tenancy feature.

Field	Description
Add	Adds the entry for the selected time zone and the associated ACD and tenant (if the tenancy feature is installed) in the current user window to the database. If an entry already exists, the system displays <i>Already exists</i> on the window status line.

Table continues...

Field	Description
Delete	Removes the entry for the selected time zone and the associated ACD and tenant (if the tenancy feature is installed) in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line.
Find one	Finds an entry in the database that matches the time zone and associated ACD and tenant (if the tenant feature is installed) in the current window. The status line for the current window indicates the total number of matches found.
List all	Lists all the ACDs, tenants and tenant users (if the tenancy feature is installed), and the time zones in the database that match with the values entered in the fields of the current user window.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Data summarization time zone fields

 Note:

The System Setup Data Summarization Time Zone window displays the tenant option only if the customer has installed the tenancy feature.

Field	Description
Add	Adds the entry for the selected time zone and the associated ACD and tenant (if the tenancy feature is installed) in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line.
Delete	Removes the entry for the selected time zone and the associated ACD and tenant (if the tenancy feature is installed) in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line.
Find one	Finds an entry in the database that matches the time zone and associated ACD and tenant (if the tenant feature is installed) in the current window. The status line for the current window indicates the total number of matches found.
List all	Lists all the ACDs, tenants and tenant users (if the tenancy feature is installed), and the time zones in the database that match with the values entered in the fields of the current user window.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Chapter 6: Administering call center agents

You can administer agents in CMS Supervisor. The items on the **Agent Administration** menu vary depending on the type of switch that CMS is connected to and the features that are activated on the switch.

Permissions for agent administration

You need permissions for the Agent Administration subsystem. To view information, you need Read access. For all other agent administration tasks, you must have Write access.

If you are a tenant user, you need permissions to manage agents and agent skills in the tenant to which you are assigned. As a tenant user, you can also activate or list agent tracing for any agent for whom you have permissions. For more information about tenancy, see [Managing tenant access](#) on page 246.

Agent skill changes

Use the Change Agent Skills page to manage the skills assigned to an agent. You can add a skill, delete a skill, or change skill settings. When adding and managing skills, you can apply the change immediately or set up scheduling. When applying skill changes for an agent, an optional field is available to select additional agents. Use caution before selecting additional agents because the current skill change will override the existing skills for these agents. For the main agent you are modifying, existing skills are not impacted.

Scheduling for agent skills

The scheduling option is only available in the Web Client. Scheduling is useful if your agent needs to handle different types of calls at different times. For example, you might want an agent to only handle auto insurance calls on Monday, Tuesday, and Thursday, and then handle other insurance calls on other days.

If you add a skill on the Change Agent Skills page after setting up scheduling, that skill is not added to your scheduled job. You can edit the schedule for an existing job from the Scheduler page, but you cannot add skills or modify other skill-related operations. If you want to add a skill after scheduling a job, you must delete the scheduled job and set up a new one.

Requirements and considerations for changing agent skills

Review the following before using the Change Agent Skills page:

- The option to change agent skills is only available for ACDs on which the EAS feature is activated.
- You must select an active ACD. You cannot modify skills if the ACD link is down. You also cannot set up scheduling if the ACD link is down.
- Use CMS Supervisor to change agent skills because it checks if the agent has the appropriate permissions for the newly-assigned skills. The CMS ASCII interface does not check permissions.
- Agent skill changes take effect on the ACD system. The skill change remains in effect until another change is made through CMS Supervisor or the ACD system.
- You can use a template when applying agent skill changes. A template is an existing agent profile where the skill settings are applied to other agent profiles. You can specify multiple agents individually and by using ranges. Entries can include up to 250 characters and are separated with semicolons. After you apply the skill settings, all agents specified will have the same skills, levels, interrupt types, and percentages as the agent profile being used as a template. Ensure that you have the same level of permissions for all agents specified in the change.
- Skill changes take effect immediately for agents who are in the AUX work mode, Available state, or logged out. Changes remain pending for agents on calls or in ACW until they enter the AUX work mode, become available, or log out. Agents who frequently have calls on hold might have skill changes pending for a longer time than expected.
- To modify the **Level** and **Interrupt Type** options for a skill, you must have Write permissions for that skill. You also need Write permissions to a skill to delete it.
- Tenant users must have Write permissions for the agent whose skills they want to modify. A tenant user can only manage agents within their tenant.

Adding agent skills in the Web Client

About this task

Use this procedure to assign a new skill to an agent.

Procedure

1. Navigate to **Administration > Agent Administration > Change Agent Skills**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent skills.
3. In the **Agent** list, select the agent whose skills you want to update.
If you do not see the agent you want to manage, you can type their name or ID.
4. Click **Add Skill** to assign a new skill.
5. From the **Skill** list, select an available skill.

6. In the **Level** list, select a priority level for the new skill.
 7. In the **Interrupt Type** list, select one of the following options:
 - **NA**: The agent cannot be interrupted.
 - **AUTO**: The agent can automatically be put into the Available state to receive calls.
 - **MANUAL**: The agent manually indicates if they are available to receive calls.
 - **NOTIFY**: The agent is notified and can choose to accept or reject the interruption.
 8. Click **OK** to close the Add Skill window and return to the Change Agent Skills page.
 9. If you want to replace the skills for additional agents, do the following:
 - a. In the **Select additional agents** field, type agent names, IDs, or a range of IDs.
If you enter multiple values, use a semicolon to separate each entry.
 - b. Click **+** to move agents from the Search Results area to the Selected Agents area.
-  **Important:**
- Do not perform this step unless you are sure that you want to override the existing skills for these additional agents.
10. Do one of the following:
 - Click **Apply** to apply the change immediately.
 - Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

Changing agent skills in the Web Client

About this task

After adding skills for an agent, you can change the skill settings if required.

Procedure

1. Navigate to **Administration > Agent Administration > Change Agent Skills**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent skills.
3. In the **Agent** list, select the agent whose skills you want to update.
If you do not see the agent you want to manage, you can type their name or ID.
4. In **Call Handling Preference**, select one of the following:
 - **Skill Level**
 - **Greatest Need**
 - **Percent Allocation**
5. **(Optional)** In **Direct Agent Skill**, select a skill to use when the agent is contacted directly.
6. **(Optional)** Select **Service Objective** to assign service objectives to the call handling preferences.

7. In the Agent Skills area, click the skill that you want to change and select values for **Level** and **Interrupt Type**.
 8. If you want to replace the skills for additional agents, do the following:
 - a. In the **Select additional agents** field, type agent names, IDs, or a range of IDs.
If you enter multiple values, use a semicolon to separate each entry.
 - b. Click **+** to move agents from the Search Results area to the Selected Agents area.
-  **Important:**
- Do not perform this step unless you are sure that you want to override the existing skills for these additional agents.
9. Do one of the following:
 - Click **Apply** to apply the change immediately.
 - Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

Deleting agent skills in the Web Client

About this task

You can delete a skill that an agent no longer needs. For example, if an agent will no longer be handling home insurance calls, they do not need the skill associated with home insurance. If the agent only has one assigned skill, you must add new skills for the agent before deleting the current skill.

Procedure

1. Navigate to **Administration > Agent Administration > Change Agent Skills**.
2. In the **Current ACD** list, select the active ACD for which you want to manage agent skills.
3. In the **Agent** list, select the agent whose skills you want to update.
If you do not see the agent you want to manage, you can type their name or ID.
4. Click  next to the skill entry you want to delete.
You cannot remove the direct agent skill, which is used when someone contacts the agent directly. If an agent only has one skill assigned, you cannot delete it.
5. If you want to replace the skills for additional agents, do the following:
 - a. In the **Select additional agents** field, type agent names, IDs, or a range of IDs.
If you enter multiple values, use a semicolon to separate each entry.
 - b. Click **+** to move agents from the Search Results area to the Selected Agents area.

 Important:

Do not perform this step unless you are sure that you want to override the existing skills for these additional agents.

6. Do one of the following:

- Click **Apply** to apply the change immediately.
- Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

About changing agent skills using the PC Client

Use the Change Agent Skills window to configure agent skills on systems with Expert Agent Selection (EAS).

Use this feature to perform the following actions:

- View the current skill assignment
- Change the skills of an agent or agent template
- Add agents to an agent template
- Set the skill of an agent or agent template to **Primary** or **Secondary**
- Set the level of the skill for an agent from 1 to 16

Changing agent skills using the PC Client

Procedure

1. From the Controller window, select **Commands > Agent Administration**.

CMS Supervisor displays the Agent Administration window.

2. In the **ACD** field, select the ACD for which you want to change agent skills.

3. In the **Operations** list, highlight **Change Agent Skills**.

4. Select **OK**.

Supervisor displays the Select Agent/Template window.

5. In the Select Agent/Template window, enter the Agent ID using one of the following methods in order view or change their skills:

- The agent login ID
- The name of the agent
- An agent template

See the beginning of this section for more information on agent templates.

6. Select **OK**.

Supervisor displays the Change Agent Skills window with the agent or template name and login ID in the title bar.

The skills and skill level for the agent or template that you named are shown in the **Assigned Skills** field and **Level** field, respectively.

Skill names are shown for the skills that are defined in the Dictionary. Skill numbers are shown for the skills that are not defined in the Dictionary.

These skill settings for an agent can be passed on to other agent profiles. To specify the agents who are to receive the skill settings, select **Use for one or more Agents** and enter the agent IDs in the associated field.

7. Choose one of the following options to change the skills of this agent or template:

- To change which calls an agent receives first, perform [Changing call handling preference](#) on page 156.
- To change the skill that is used to queue an agent's direct agent calls, perform [Changing skills for direct agent calls](#) on page 157.
- To change the level or type that is associated with the skill that is already assigned, perform [Changing the type associated with the skill](#) on page 157.
- To change the interrupt type associated with skill that is already assigned for Communication Manager version 6.0 and up, perform [Changing the interrupt type associated with the skill](#) on page 157.
- To remove skills that are assigned to this agent or template, perform [Removing skill assigned to the agent or template](#) on page 157.
- To add skills to this agent or template, perform [Adding skill to the agent or template](#) on page 158.
- To specify a new percent allocation when you have Avaya Business Advocate, perform [Specifying a new percent allocation](#) on page 158.
- To make a **Direct Agent Calls First** the **Top Skill** for this agent, perform [Assigning the top skill for the agent](#) on page 158.
- To apply the changes to multiple agents, perform [Applying changes to multiple agents](#) on page 158.
- To finish making changes, perform [Finishing making changes](#) on page 159.
- To change skill assignment for other agents or templates, perform [Making skill assignment changes for other agents](#) on page 159.

Changing call handling preference using the PC Client

Procedure

Select a different method in the **Call Handling Preference** group box.

Calls can be distributed to the selected agent based on:

- **Skill Level**
- **Greatest Need**
- **Percent Allocation**

The **Skill Level** for the agent is shown in the **Assigned Skills** list. All three call handling preferences are managed by Avaya Aura® Call Center Elite and are only available if Avaya

Business Advocate is enabled on the Communication Manager system. For more information about call handling preferences, see *Using Avaya Business Advocate*.

Changing skills for direct agent calls using the PC Client

Procedure

Perform one of the following actions:

- Select a new skill from the **Direct Agent Calls** drop-down list.
- Enter the name or number of the skill in the **Assigned Skills** column of the **Agent Skills and Skill Levels** group that will be used for queuing the direct agent calls to the specified agent. You may then select the skill from the **Direct Agent Calls** drop-down list.

The **Direct Agent Calls** list does not contain reserve skills. If the agent who is currently displayed has only reserve skills in the **Assigned Skills** list, no **Direct Agent Calls** can be assigned to that agent.

Changing the type associated with the skill using the PC Client

Procedure

1. In the **Assigned Skills** list, select the level of the skill for which you want to change the value.

If you have a Skill Level Call Handling Preference, an arrow indicates the agent's Top Skill assignment.

2. Select a new value for the skill level from the **Level** drop-down list in the **Agent Skills and Skill Levels** group.

If **Skill Level** is selected in the **Call Handling Preference** group and only reserve levels are assigned to an agent, that agent does not have a top skill and the **Make Top Skill** button is disabled.

3. Select **OK**.

Changing the interrupt type associated with the skill using the PC Client

Procedure

1. In the **Assigned Skills** list, select the interrupt type of the skill for which you want to change the value.
2. Select a new value for the interrupt type from the interrupt type drop-down list in the **Agent Skills and Skill Levels** group.
3. Select **OK**.

Removing skill assigned to the agent or template using the PC Client

Procedure

1. In the **Assigned Skills** field, select the skills to remove from the agent.
2. Select the **Delete Skills** button.

If an agent has only one assigned skill, this skill cannot be deleted.

Adding a skill to the agent or template using the PC Client

Procedure

1. Select the **Add Skills** button.
2. In the **Available Skills** list of the Add Agent Skills window, highlight one or more skills that you want to assign to the agent as well as the **Skill Level** for these new skills.

The **Available Skills** field lists all the skills that are defined on this ACD.

3. Select the **OK** button in the Add Agent Skills window.

Specifying a new percent allocation using the PC Client

Procedure

1. In the **Call Handling Preference** group, select **Percent Allocation**.

The **Percent Allocation** field is unavailable if a reserve level has already been specified for an agent or template.

2. Select the **YES** button from the warning window.

This indicates that you want to enable the Percent Allocation feature.

If an agent or template has **Percent Allocation** call handling preference, the total percent allocation for all standard skills must equal 100%.

By default, **Direct Agent Calls First** is activated. If a call handling preference other than **Percent Allocation** is selected, direct agent calls are delivered first, and the **Direct Agent Calls First** check box is not applicable.

Assigning the top skill for the agent using the PC Client

About this task

Use this task to make the selected skill the agent's top skill. The skill selected here becomes the highest level skill for the agent. For example, if you have an agent with skill 1 at level 4, skill 2 at level 6, skill 3 at level 10, and skill 4 at level 16, if the customer wants to make skill 4 the agent's top skill, selecting that skill here automatically changes skill 4 to level 1 and move it to the top of the agent's login skill list.

Procedure

1. In the **Assigned Skills** column of the **Agent Skills and Skill Levels** group, select the skill that you want to be the top skill of the agent.
2. Select the **Make Top Skill** button.

Applying changes to multiple agents using the PC Client

Procedure

1. Select the **Use for one or more Agents** check box.

2. Enter the agent names or login IDs in the **Agent names or logids** field, select them from the drop-down list, or select them from the Browse window.

If an error is encountered with changes to agent skills, Supervisor displays a message that states what is in error. Select **OK** or **Cancel** to dismiss the error message and return to the Change Agent Skills window so that the error can be corrected.

3. Select **OK**.

Changes are submitted to the CMS server. If a move is pending, you are notified that the operation will not occur until the pending conditions are resolved. If you are applying a template to multiple agents, Supervisor buffers the change agents skills requests and send them to the CMS server one at a time. Supervisor displays a status box that indicates the status of each requested agent change.

If an error is encountered with changes to agent skills, Supervisor displays a message that states what is in error. Select **OK** or **Cancel** to dismiss the error message and return to the Change Agent Skills window so that the error can be corrected.

4. Select **OK**.

If the change is successfully made, Supervisor displays a successful message in the status bar.

If the state of an agent is not in AUX or AVAIL, Supervisor displays a message which states that the changes will be applied when the agent returns to one of those states.

5. Select **OK**.

Supervisor closes the Change Agent Skills window.

Finishing making changes using the PC Client

Procedure

1. Select **OK** in the Select Agent/Template window.

This action saves the changes that you made to the agent skills.

2. Select **Cancel** in the Select Agent/Template window.

This action cancels any changes that you made.

Changing skill assignment for other agents or templates using the PC Client

Procedure

1. Select another agent or template in the Select Agent/Template window.
2. Resume from step 5 of the main procedure.

Multi-agent skill changes

The Multi-Agent Skill Change page is similar to the Change Agent Skills page. However, instead of assigning skills to an agent, you are assigning agents to a skill.

The Multi-Agent Skill Change page is useful for managing multiple agents. You can assign a new skill to the selected agents, move agents from one skill to another, and remove agents from a skill. The changes are only made for the selected skill. The other skills assigned to the agents are not impacted.

Scheduling for multi-agent skill changes

You can set up scheduling for agent skills in the Web Client. Scheduling is useful if the agents you select on the Multi-Agent Skill Change page need to handle calls for the specified skill at a specific time. For example, if you assign a Sales skill, you can configure scheduling so the selected agents only receive sales calls on the weekends. They can then focus on handling other types of calls on other days.

Considerations for multi-agent skill changes

- Agent skill changes take effect on the ACD system. The skill change remains in effect until another change is made through CMS Supervisor or the ACD system.
- Skill changes take effect immediately for agents who are in the AUX work mode, Available state, or logged out. Changes remain pending for agents on calls or in ACW until they enter the AUX work mode, become available, or log out. Agents who frequently have calls on hold might have skill changes pending for a longer time than expected.

Assigning a skill to multiple agents in the Web Client

About this task

You can select a configured skill and then add agents to it. The agents you add will receive calls for the skill.

Procedure

1. Navigate to **Administration > Agent Administration > Multi-Agent Skill Change**.
2. Click the **Add** operation.
3. In the **Current ACD** list, select the active ACD for the skill you are managing.
4. In the **Skill** list, select the skill to which you want to add agents.
5. In the **Level** list, select a priority level for the skill.
6. In the **Interrupt Type** list, select one of the following options:
 - **NA**: The agent cannot be interrupted.
 - **AUTO**: The agent can automatically be put into the Available state to receive calls.
 - **MANUAL**: The agent manually indicates if they are available to receive calls.
 - **NOTIFY**: The agent is notified and can choose to accept or reject the interruption.

7. In the **Agents** field, enter agent names or IDs.

If you enter multiple values, separate them with a semicolon. The entries are displayed in the Search Results area.

8. Click **+** to move the agents you want to assign from the Search Results area to the Selected Agents area.

The agents in the Selected Agents area will be assigned to the skill.

9. Do one of the following:

- Click **Apply** to apply the change immediately.
- Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

Moving agents from one skill to another in the Web Client

About this task

You can move multiple agents from one skill to another. The change only affects the skill you select. Other existing skills for the selected agents are not impacted.

Procedure

1. Navigate to **Administration > Agent Administration > Multi-Agent Skill Change**.
2. Click the **Move** operation.
3. In the **Current ACD** list, select the active ACD for the skill you are managing.
4. In the **From skill** list, select the current skill that will be replaced with another skill.
5. In the **To skill** list, select the new skill you want to assign.
6. Select **Level** and **Interrupt Type** values for the new skill.
7. In the **Agents** field, enter agent names or IDs.

If you enter multiple values, separate them with a semicolon. The entries are displayed in the Search Results area.

8. Click **+** to move agents from the Search Results area to the Selected Agents area.

9. Do one of the following:

- Click **Apply** to apply the change immediately.
- Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

Removing agents from a skill in the Web Client

About this task

You can remove a skill from multiple agents who currently have the skill assigned. The other skills assigned to the selected agents are not impacted.

Procedure

1. Navigate to **Administration > Agent Administration > Multi-Agent Skill Change**.
2. In **Operation**, click **Remove**.
3. In the **Current ACD** list, select the active ACD for the skill you are managing.
4. From the **Skill** list, select the skill that no longer needs to be assigned.
5. In the **Agents** field, enter the names or IDs of agents who currently have the skill assigned.
If you enter multiple values, separate them with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move agents from the Search Results area to the Selected Agents area.
7. Do one of the following:
 - Click **Apply** to apply the change immediately.
 - Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

Changing skills for multiple agents using the PC Client

About this task

You can modify the skills for multiple agents at a time. Use the Multi-Agent Skill Change window to view current skill assignments or to change a skill for as many as 32 agents. You can also use this window to specify the skill levels and type of skills.

Procedure

1. From the Controller window, select **Commands > Agent Administration**.
CMS Supervisor displays the Agent Administration window.
2. In the **ACD** field, select the ACD for which you want to change agent skills.
3. In the **Operations** list, highlight **Multi-Agent Skill Change** and click **OK**.
CMS Supervisor displays the Multi-Agent Skill Change window.
4. Use one of the following methods to choose a skill:
 - Double-click the skill name or number.
 - Highlight a skill and press the **Enter** key.Supervisor displays a second window that shows the agents assigned to this skill who are currently logged in.
5. To view or change the current skills of an agent in the skill window, double-click the agent name.
6. To move agents from the current skill to another skill, perform one of the following actions:
 - To move a single agent, use your mouse to drag-and-drop an agent to a new skill in the Skill List window.

- To move multiple agents to a new skill, hold down the **Ctrl** key and click on multiple agents to select them. You can select a range of agents by clicking the agent at the beginning of the range, holding down the **Shift** key, and then clicking the agent at the bottom of the range.

Note that holding down the **Ctrl** key while dragging and dropping agents will add, not move, the agent or agents to the new skill.

7. In the Move Agents Between Skills window, perform one of the following actions to finish moving agents from skill to skill:
 - Select the **Level** option and enter a skill-level value for each agent that you moved to this new skill.
 - To keep the current skill level of the agent, select the **Preserve Original Levels** option. This action deactivates the **Level** option.
 - Select the interrupt type for the new skill for the selected agents.

If the agent is being added to a new skill, not moved, the **From skill** information is blank and the **Preserve Original Levels** option is unavailable.

8. Click **OK**.

If one or more agent moves fail, CMS Supervisor displays a status window showing the reasons for failure. Otherwise, the status window notifies you that the change is pending.

Agent tracing

The Activate Agent Trace page is useful to view the current agent trace states. You can activate or deactivate the tracing of agents. Use the List Agents Traced page to specify agents, dates, or both to view a list of available agent trace data. The list is available if you activate agent tracing for one or more agents.

Viewing current agent trace states using the Web Client

Procedure

1. Navigate to **Administration > Agent Administration > Activate Agent Trace**.

CMS Supervisor displays the Activate Agent Trace window, showing the **Current ACD** and any active agents that have trace enabled.

2. In the **Current ACD** drop-down list, select the ACD for which you want to view current agent traces.

CMS Supervisor displays any active agents that have trace enabled.

Viewing current agent trace states using the PC Client

Procedure

1. From the Controller Window, select **Commands > Agent Administration**.
Supervisor displays the Agent Administration window.
2. In the **Operations** list, highlight **Activate Agent Trace**.
3. In the **ACD** drop-down list, select the ACD on which the agent trace will be run or is currently running.
4. Select **OK**.
Supervisor displays the **Activate Agent Trace** window.
5. Ensure that the **Agent names or logids** field is blank.
6. In the **Agent Trace** options, select the state to view:
 - **On** - Displays all currently active agent traces.
 - **Off** - The system cannot identify which agents do not have trace activated, but it does display those agents that are defined in the Dictionary with trace enabled.
7. From the menu bar, select **Actions > List all**.
Supervisor displays a window with a list of all agents who are currently in the selected trace state.

Activating agent tracing

You can activate (start) or deactivate (stop) the tracing of agents. After activating agent tracing, you can run an agent trace report to view information about agent activities, state changes, and the time when these events occurred. Use the agent trace report to help you evaluate how well agents use their time.

Considerations for starting or stopping an agent trace

Consider the following before working with agent tracing:

- To start or stop agent traces, ensure that the Data Collection feature is enabled.
- You can activate tracing for a limited number of agents across all ACDs from one CMS server. The number of supported active agent traces depends on the capacity for your configuration. For example, a small VMware configuration supports less active agent traces than a medium or large configuration. For more information about capacity specifications, see *Avaya Call Management System Overview and Specification*.
- Stopping or deactivating a trace does not delete the trace records for that agent. Agent trace records are overwritten automatically when the trace file reaches the maximum number of allocated records.
- The settings in the Data Storage Allocation window determine the maximum number of agent trace records that CMS can store. For more information about data storage allocation, see [Data storage allocation](#) on page 278.

Starting or stopping an agent trace using the Web Client

Procedure

1. Navigate to **Administration > Agent Administration > Activate Agent Trace**.
CMS Supervisor displays the Activate Agent Trace window, showing the **Current ACD** and any active agents that have trace enabled.
2. In the **Current ACD** drop-down list, select the ACD for which you want to start or stop agent traces.
3. Select **Activate Agent Trace** or **Deactivate Agent Trace**.
CMS Supervisor displays a selection window where you can search on agent names or login IDs. Use this window to select agents to either activate or deactivate agent trace.
4. After selecting one or more agents, select **Activate** or **Deactivate** to save your selections.
CMS Supervisor displays any active agents that have trace enabled. While viewing the trace results, you can:
 - Enter a search string in the “Enter a filter string to search” box to limit the agents being displayed.
 - Click **Remove** to stop tracing any of the displayed agents.

Starting or stopping an agent trace using the PC Client

Procedure

1. From the Controller window, select **Commands > Agent Administration**.
Supervisor displays the Agent Administration window.
2. In the **Operations** list, highlight **Activate Agent Trace**.
3. In the **ACD** drop-down list, select the ACD on which the agent trace will be run or is currently running.
4. Select **OK**.
Supervisor displays the **Activate Agent Trace** window.
5. In the **Agent names or logids** field, enter the names or login IDs of the agents who are to be traced or are being traced.
This field can accept multiple values. Multiple values must be separated by a semicolon (;).
Using the browse button to the right of this field will only display those agents that have synonyms assigned to them through the Dictionary.
6. Perform one of the following actions for the **Agent Trace** options:
 - To start an agent trace, select **On**.
 - To stop an agent trace that is currently running, select **Off**.
7. Select **Actions > Modify** from the menu bar to start or stop the agent trace.

The status bar displays **Working** and then, if successful, displays **Successful** when the operation finishes.

Listing of traced agents

You can specify agents, dates, or both to view a list of available agent trace data. This list is available if agent tracing is activated for one or more agents.

Listing agents traced using the Web Client

Procedure

1. Navigate to **Administration > Agent Administration > List Agents Traced**.
2. In the **Current ACD** drop-down list, select the ACD for which you want to list agent traces.
3. Do one or both of the following:
 - In the **Agent (optional)** field, select an agent from the drop-down list or type the name of the agent.
 - In the **Date(s) (optional)** field, enter a date or a range of dates. You can also use the calendar icon to select dates.
4. Click **Search**.

CMS Supervisor displays the list of the agents traced based on the search criteria.

Listing agents traced using the PC Client

About this task

The results for listing agents traced relies on the entries made in the **Agents** field, the **Date** field, or a combination of the two. For example, you can specify a small range of agents in the **Agents** field and a date range in the **Date** field. This will result in a list of only the specified agents for the date range entered.

Procedure

1. From the Controller window, select **Commands > Agent Administration**.
2. In the **Operations** list, select **List Agents Traced**.
3. In the **ACD** field, select the ACD for which you want to list agents being traced.
4. Click **OK**.
5. Do one or both of the following depending on whether you want to search for agents, dates, or both:
 - In the **Agents** field, specify one or more agents that have login IDs in the Dictionary. If you enter multiple values, separate them with a semicolon.
 - In the **Date** field, specify a single date, multiple dates, or a range of dates. Multiple dates must be separated with a semicolon.

Leave both the **Agents** and **Date** fields blank to have CMS Supervisor display all agent trace records.

6. Select **Actions > List all** to display the agent trace records that match the information that you entered in the **Agents** and **Date** fields.

CMS Supervisor displays a secondary window listing the dates and agents for which agent trace data is available, sorted by date.

About administering splits using the PC Client

Splits are supported only on systems without Expert Agent Selection (EAS) and can only be administered using the PC Client. Split administration is not supported on the Web Client.

About changing extension split assignments

This section provides the procedure for assigning an extension to a different split. This feature is used for Communication Manager systems without Expert Agent Selection (EAS). Use the Change Extension Split Assignments window to list the extensions that are in the currently assigned splits or to change the splits that are assigned to a specific extension number.

Before changing extension split assignments

The following should be read and understood before changing extension split assignments:

- You cannot exit from the Change Extension Split Assignments window until the Communication Manager system responds to the requested changes.
- Extension split assignment changes take effect immediately for agents who are in AUX work mode, AVAIL (available), or logged out. Changes are pending for agents on calls or in ACW work mode until the agent enters the AUX work mode, becomes available, or logs out.
- For agents who frequently have calls on hold, extension split assignment changes can remain pending for a long time.

Permissions required to change extension split assignments

Depending on the procedure that you want to perform, you need the following permissions:

- To view extension split assignments, you need “read” permission for the Agent Administration subsystem.
- To change extension split assignments, you need “write” permission for the Agent Administration subsystem and for the splits to which the extensions are assigned.

Changing extension split assignments

Procedure

1. From the Controller window, select **Commands > Agent Administration**.
Supervisor displays the Agent Administration window.
2. In the **ACD** field, select the ACD for which you want to change extension split assignments.

3. Select **Operations > Change Extension Split Assignments**.4. Select **OK**.

Supervisor displays the Select Extension window.

5. In the Select Extension window, enter the extension number for which the split assignment is to be changed.

The extensions that are assigned to each split can be viewed in the Move Extensions Between Splits window. See [Move extensions between splits](#) on page 168 for more information.

6. Select **OK**.

Supervisor displays the Change Extension Split Assignments window.

The **Move Extension From Split** field shows the current split assignment. The **Move Extension To Split** field shows available split names or numbers. If an agent is logged in on the extension, the logged-in icon is displayed as shown in the above graphic. If an agent is not logged in on the extension, an icon is not displayed.

7. Perform one of the following actions:

If...	Then...
You want to change split assignments for an extension other than the one that is displayed	Select Cancel to return to the Select Extension window and then return to step 5 on page 168.
You want to change split assignments for this extension	Continue with the next step.

8. Perform one of the following actions:

If...	Then...
You want to remove a split assignment from this extension	Select the split name or number that is to be removed from this extension in the Move Extension From Split box.
You want to assign a split assignment to this extension	Select the split name or number that is to be assigned to this extension in the Move Extension To Split box.

9. Select **OK**.

CMS applies the split assignment changes made to the extension.

Move extensions between splits

This section provides the procedures for adding a split to an extension, removing a split from an extension, and moving an extension to another split. This features is for those systems without Expert Agent Selection (EAS). You can also use the Move Extensions Between Splits window to view extension split assignments.

Before moving extensions between splits

The following items should be read and understood before moving extensions between splits:

- As many as 32 agents can be moved at one time.
- You cannot exit from the Move Extensions Between Splits window until the Communication Manager system responds to your request.
- Extension split assignment changes take effect immediately for agents who are in AUX work mode, AVAIL (available), or logged out. Changes are pending for agents on call or in ACW work mode until the agent enters the AUX work mode, becomes available, or logs out.
- For agents who frequently have calls on hold, an extension move request can remain pending for an extended period of time.

Permissions required to move extensions between splits

Depending on the procedure that you want to perform, you need the following permissions:

- To view extension assignments, the user ID used to log in to this Supervisor session requires “read” permission for the Agent Administration subsystem and the affected splits.
- To move extension assignments, the user ID used to log in to this Supervisor session requires “write” permission for the Agent Administration subsystem and the affected splits.

Moving extensions between splits

About this task

To move extensions between splits:

Procedure

1. From the Controller window, select **Commands > Agent Administration**.
Supervisor displays the Agent Administration window.
2. In the **ACD** field, select the ACD that contains the extensions to move.
3. In the **Operations** list, highlight **Move Extensions Between Splits**.
4. Select **OK**.
Supervisor displays the Move Extensions Between Splits window.
5. Select the split to work with by performing one of the following actions:
 - Double-click the split name or number in the Split List window.
 - Highlight the split to work with in the Split List window and then select **Split > Open selected split** from the menu bar.
6. To move one or more extensions from the current split to another split, perform one of the following actions:
 - To move a single extension, use the mouse to drag-and-drop an extension to a new split in the Split List window.

- To move multiple extensions to a new split, hold down the **Ctrl** key and click on multiple extensions to select them. You can select a range of extensions by clicking on the extension at the beginning of the range, holding down the **Shift** key, and then clicking the extension at the bottom of the range.

Use the drag-and-drop method to move the extensions from the window for their current split to a new split in the Split List window.

Another way of moving extensions from one split to another is to open a window for the new, target split by double-clicking that split in the Split List window. You can then drag-and-drop extensions between the two split windows.

Supervisor displays the Move Extensions Between Splits window.

7. Select **OK** in the Move Extensions Between Splits window to complete the moving of the selected extensions.

About running a split members report

Note:

The split members report is only available to customers who have non-EAS systems and to those using the PC Client.

This section provides the procedure for running a split members report. This report displays the extensions that are members of a specific split. Unlike regular reports, a custom or designer report cannot be created from the split members report. The split members report lists the selected splits in numerical order, each split's assigned name, and the extensions that are assigned to the split.

Permissions required to run a split members report

Depending on the procedure that you want to perform, you need the following permissions:

- To run a split members report, the user ID used to log in to this Supervisor session requires “read” permission for the Agent Administration subsystem and for all affected splits.

Running a split members report

Procedure

1. From the Controller window, select **Commands > Agent Administration**.
Supervisor displays the Agent Administration window.
2. Select the **Reports** tab.
Supervisor displays the Reports tab of the Agent Administration window.
3. In the **ACD** field, select the ACD on which to run the split members report.
4. In the **Reports** list, highlight **Split Members**.
5. Select **OK**.
Supervisor displays the Split Members window.

6. Enter the split information in the **Splits** field. This can be one split, multiple splits, or a range of splits. Multiple splits must be separated by a semicolon (;).
7. In the **Destination** group, select **View Report on Screen** or **Print Report on**.
8. Select **OK**.

Supervisor displays or prints the Split Members report.

If the split does not have a name assigned, the Split Name columns on the report shows the split number. If the split has no extensions assigned to it, the Extension column is blank.

Chapter 7: Administering users and user permissions

The User Permissions subsystem is used to create CMS user IDs and to administer the Read, Write, and Exception permissions for features, main menu additions, splits/skills, trunk groups, ACDs, vectors, VDNs, and tenants.

The default CMS administrator user ID, “cms”, provides access to the entire system. With this administrator ID, you can create users who require access to CMS and assign the permissions necessary for each user to perform their job duties.

Important:

Do not share user IDs for security reasons. Sharing user IDs can also affect system performance. Logging in with the same ID at multiple terminals uses more system resources than separate login IDs for each user.

Considerations for the User Permissions subsystem

Consider the following when working with user permissions:

- From **User Permissions > Feature Access**, you can assign permissions for various features, including the User Permissions feature. Any user (normal or administrator) with Write access to the User Permission feature can modify their own permissions for all CMS subsystems.
- If an ACD group is selected as the current ACD in the User Permissions window, only those operations that are valid for the ACD group are displayed in the list of available operations.

Required permissions and example

You need access to the User Permissions subsystem to view or manage user data, feature access, or other access items.

- You need Read access to view user data and other items under **User Permissions**.

- You need Write access to add or modify users and other access settings under **User Permissions**.

If you are a tenant user, you can only view your own data. You cannot modify your user data. You also cannot add, modify, or delete other users.

Example

The following table provides an example of the permissions that a supervisor might need:

The call center has a skill called...	And assigned to it are...	The Skill 1 supervisor requires read/write permissions for...
Skill 1	Trunk groups 22 and 23	• Skill 1 • Trunk groups 22 and 23 • Dictionary • Exceptions

User administration

From the User Data page, add users so they can access CMS Supervisor. The users you add can use their assigned ID to log in to CMS and CMS Supervisor.

When adding a user, configure the following:

- CMS user ID.
- User's name, room number, and phone number.
- Default CMS printer for the user ID.
- User type. You can designate the user as a Normal user, Administrator, or Tenant user.
- Enable LDAP authentication for an Active Directory user.
- Maximum number of CMS Supervisor windows that can be opened simultaneously.
- Minimum refresh rate for real-time reports.
- Default login ACD.

You can also modify or delete existing users from the User Data page.

Viewing CMS users

Viewing users using the Web Client

Procedure

1. Navigate to **Administration > User Permissions > User Data**.

All configured users are displayed.

2. Enter search text in the text box to search for specific users.

Viewing users using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **User Data**.
3. Click **OK**.
4. From the menu bar, click **Edit > Clear All**.

The information in all fields is removed, including the default information that is displayed.

5. Populate some or all of the fields with your search criteria.
6. From the **Actions** menu, click one of the following search options:
 - **List all**: Displays a secondary window showing all users whose settings match the entries in the fields. If no information is present in the fields, all users are displayed. This method is convenient when the need arises to look for one or more user IDs.
 - **Find one**: Uses the entries in the fields and queries the database for users with matching settings. For example, if you type 6 in the **Maximum user window count (1-12)** field with all other fields blank and then select **Find one**, all users with this window count setting are displayed. If multiple users are found, use the **Next** and **Previous** options under the **Actions** menu to navigate through each user. When you reach the last user, the **Next** option is not disabled, but it results in the first user being displayed again.

The **Find one** search option does not support partial text strings. Ensure that you enter the full search term.

Adding a CMS user

Considerations for adding a CMS user

Consider the following before adding a user:

- A user ID must be created before any permissions can be assigned to it.
- The following internal CMS user IDs cannot be added as regular CMS users: inads, sroot, init, craft, con, nul, aux, com1 through com9, and lpt1 to lpt9.
- If you add a user through an operating system utility, such as **useradd**, they must use the **su** command to assume the role of a valid CMS user. Users created through an operating system utility have the shell type `/usr/bin/ksh`. The User Data page in CMS Supervisor does not display users that were created using an operating system utility.
- Users added through the User Data page will automatically have CMS launch when they log in. The shell for these users is `/usr/bin/cms`.

Adding a user from the Web Client

Procedure

1. Navigate to **Administration > User Permissions > User Data**.
2. Click **Add User**.
3. Administer the options as described in [User data descriptions](#) on page 175.
4. When you are ready to add the user, click **OK**.

Adding a user from the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. From the **ACD** list, select the ACD or ACD group on which the user will be created.

The same user ID does not need to be created on each ACD. A user created on one ACD can be given permissions to other ACDs.
3. In the **Operations** list, select **User Data**.
4. Click **OK**.

CMS Supervisor displays the User Permissions User Data window.
5. Administer the options as described in [User data descriptions](#) on page 175.
6. Click **Actions > Add** from the menu bar.

The user ID is created on the specified ACD.

Next steps

A user password is required for SSH connections to the CMS server. As described in [Changing a user's password through the command line interface](#) on page 421, you can use the command line interface to force the user to change their password the next time they log in.

User data descriptions

The following table describes the options you configure for a user. You can change some of these options when modifying a user.

Field	Definition
User ID	This is a required field. Enter a user ID that contains 3 to 31 characters. LDAP-authenticated users are limited to 20 characters. This is a limitation of LDAP, not CMS. The user ID can include underscores, hyphens, or periods. Do not include other punctuation, spaces, or special characters.
User Name	Enter a name for the user. You do not need to complete this field to add the user.
Room Number	Add a room number. This is an optional field.
Phone Number	Enter a phone number for the user. This is an optional field.

Table continues...

Field	Definition
Printer	This is an optional setting. Ensure that the printer name matches the printer administered on the CMS server.
Login type	Select one of the following user types when creating a user: • Normal user: Select this option for a user that does not perform maintenance and administration tasks on CMS. By default, normal users have “Read” permissions for most features. • Administrator: Select this option for users that need to perform maintenance and administration tasks. By default, administrators have “Write” permissions for all features. • Tenant user: Select this option to provide limited tenant access to a user. Tenant users have limited access to CMS administration and reporting data. They can only access data for the tenants to which they are assigned. Tenant users can view their own user information but they cannot modify it and they also cannot add or modify other users. You can modify users after they are created. When modifying a user, you can change their designation from a normal user to an administrator or the other way around. However, changing the role when modifying a user does not change the assigned permissions. You must change the permissions manually. You cannot change the tenant user designation. If you want to change the tenant user designation, you can delete the user and then add the user again.
LDAP Authentication	Select this check box to identify the user as an LDAP-authenticated user. For more information about LDAP integration, see <i>Avaya Call Management System Overview and Specification</i> .
Maximum user window count (1-12)	Enter the number of CMS Supervisor windows that the user can have open simultaneously. The default for this field is 4. Note that having multiple windows open consumes more CMS processor resources.
Minimum refresh rate (seconds)	Enter the number of seconds from 3 to 300 for the refresh rate. Real-time report data for the user is retrieved from the database at this interval. Faster refresh rates consume more CMS processor resources.
Login ACD	Select the ACD that the user will use to log in. The user can change the current ACD after logging in, but the ACD defaults to the value you set at the next login. This is a required setting that you must configure when adding a user.

Table continues...

Field	Definition
Enterprise ID	Enter the enterprise ID. The enterprise ID is usually blank. However, you can map your enterprise ID to a CMS username that does not match the normal rules including all numeric values. Enterprise ID is only applicable when a user is logging in from the CMS Web Supervisor using the Enterprise Sign In button. The enterprise ID is validated for authentication when the primary user ID does not match a CMS username. Authentication for the primary user ID fails, especially in customer scenarios where only the numeric IDs are used as the user principal name (UPN) in the enterprise SSO platform. For example, 123456@example.com is the username that the supervisor uses to log in to the enterprise platform. However, CMS does not support new users with all numeric IDs. Hence, you can enter the enterprise ID as 123456 to map it to the CMS username.

Modifying CMS users

Considerations for modifying CMS users

Consider the following when modifying user data:

- You can change the login type for a user from **Normal user** to **Administrator** or the other way around. However, this does not change the user's permissions. You must modify the permissions manually.
- You cannot change a tenant user to a normal user or administrator. Similarly, you cannot change a normal user or administrator to a tenant user. You can delete the user and add them again.
- Changes to maximum window count, minimum refresh rate, or default login ACD for a user do not take effect until the user logs out and back in again.

Modifying a user from the Web Client

Procedure

1. Navigate to **Administration > User Permissions > User Data**.
2. Click  next to the user you want to edit.
CMS Supervisor displays the Modify Item window.
3. Administer the options as described in [User data descriptions](#) on page 175.
You cannot change the user ID.
4. Click **OK** to save your changes.

Modifying a user from the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **User Data**.
3. Click **OK**.

CMS Supervisor displays the User Permissions User Data window.

4. From the menu bar, click **Edit > Clear All** to clear all default values.
5. In the available fields, provide information about the user you want to modify.

For example, enter the user ID and select the login type.

6. Click **Actions > Find one**.

If found, the settings for the specified user ID are populated.

Tip:

If the user ID cannot be found, try selecting the other login type in the **Login type (select only one)** field.

7. Modify the settings for the user as needed.
8. When the modifications are complete, click **Actions > Modify** to update the settings for the user.

Deleting CMS users

Considerations for deleting CMS users

Consider the following before deleting users:

- Deleting a user removes their user ID and its associated permissions from CMS and the operating system.
- When you delete a user who has custom reports, designer reports, or timetables, you see a message asking if those items should be moved to your user ID. If you agree to move them and there is a conflict between the assigned names, you are prompted to rename the moved items. If not moved, any custom reports, designer reports, and timetables will be deleted along with the user ID.

Deleting a user from the Web Client

Procedure

1. Navigate to **Administration > User Permissions > User Data**.

CMS Supervisor displays the administered users.

2. Click  next to the user you want to delete.

The Confirm Delete dialog box is displayed.

3. Click **Yes** to proceed with deleting the user.
4. When prompted, confirm whether you want to move the user's reports to your user ID.

Respond to any additional prompts that are displayed. A confirmation message indicates that the user was successfully deleted.

Deleting a user from the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **User Data**.
3. Click **OK**.

CMS Supervisor displays the User Permissions User Data window.

4. From the menu bar, click **Edit > Clear All** to clear all default values.
5. In the available fields, provide information about the user you want to delete.

For example, enter the user ID and select the login type.

6. Click **Actions > Find one** and navigate through the list of users displayed.

Try modifying the information in the fields if the user you are looking for is not displayed.

7. When you find the user you want to delete, click **Actions > Delete**.

Password management in the Web Client

You can change your password from the Web Client. If you are an administrator with the Password permission, you can also change another user's password or create a temporary password for a new user.

Important:

Only the “cms” and “cmssvc” user IDs can grant or revoke the Password permission. You can use the Web Client to manage CMS user passwords. You cannot change the password for a Linux user ID, such as “root”.

Web Client password management is not available for LDAP-authenticated users or tenant users.

Changing your password in the Web Client

About this task

You can change your CMS password from the Web Client. You do not need administrative permissions to change your own password.

Procedure

1. In the Web Client, click your username in the top bar and then click **Change Password**.
2. Enter your old password.
3. Enter your new password.

4. Enter your new password again to confirm it.
5. Click **OK** to complete the change.

Changing another user's password in the Web Client

About this task

As an administrator, you can change an existing user's password or set a temporary password for a new user. For example, this capability is useful if a user cannot change their own password.

Procedure

1. In the Web Client, navigate to **Administration > Other > Change User Password**.
2. Enter the user ID that requires a password change.
3. Enter the new password.
4. Enter the new password again to confirm it.
5. **(Optional)** Select the **User must change password at next logon** check box to set this as a temporary password that the user will need to change the next time they log in to CMS.
6. Click **Apply** to make the change.

Alternatively, you can click **Reset** to clear the information you entered and reset the user's password.

CMS feature access

Use the Feature Access page to manage CMS user permissions for the following administrative features:

- Agent Administration
- Call Center Administration
- Custom Reports
- Dictionary
- Exceptions
- Forecast
- Maintenance
- Reports
- CMS System Setup
- Tenants
- Timetable

- User Permissions
- Unix (command line access)
- Password (Web Client only)

The assigned permissions affect which administration feature areas are displayed in CMS Supervisor. For example, a user that does not have Dictionary permissions will not see the Dictionary administration option.

Considerations for administering access to CMS features

Consider the following when working with feature access permissions:

- You can only assign feature access permissions to users that have been added on the User Data page.
- If you do not have Read access to a feature, you do not see it in CMS Supervisor.
- A user ID cannot have Write access without also having Read access. Note that some features only have the Write permission option.
- Users with Write access to the User Permissions feature can change permissions for all users.
- Feature Access permissions cannot be modified for the “cms” and “cmssvc” user IDs. This prevents a user with access to the User Permissions feature from disabling access to all or part of CMS for administration and services personnel.
- Default feature access permissions are assigned based on the login type selected when the user is created. Administrators have permission for all features by default. Normal users have Read access for all features except User Permissions, System Setup, Call Center Administration, and Forecasting. A normal user does not have permissions to the Tenant feature by default. A tenant user has restricted feature access. As a tenant user, you cannot turn on the Forecast, Maintenance, and System Setup features and you do not have access to the Linux command line shell.
- If the feature access permissions for a user are modified, the changes do not take effect until the user logs out and logs back in.

Managing feature access permissions in the Web Client

About this task

You can view and manage access to CMS administration features. Read and Write access options are available for most features. However, only Write access is available for some features, such as Unix and Password. The Password permission is intended for administrative users who need to set passwords for other users. You must enable the Unix permission for users who need to access the Linux command line interface.

Procedure

1. In the Web Client, navigate to **Administration > User Permissions > Feature Access**.

CMS Supervisor displays the feature permissions assigned to each user.

2. Click  next to the user whose permissions you want to change.
CMS Supervisor displays the Modify Item window.
3. Select the permissions you want to assign for each feature.
 - If you only want the user to view a feature, select **Read**.
 - If you want the user to perform administration or modification tasks, select **Read** and **Write** if both permissions are available.
 - For features where Read access is not available, select **Write** to provide access.
4. Click **OK** to save your feature access changes.

Viewing feature access permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Feature Access**.
3. In the **ACD** list, select the ACD or ACD group for which you want to view feature permissions.
4. Click **OK**.
CMS Supervisor displays the User Permissions Feature Access window.
5. In the **User ID** field, enter the ID of an existing CMS user.
You can enter multiple IDs separated with a semicolon.
6. From the menu bar, click **Actions > Find one**.
CMS Supervisor displays the permissions for the first user found. If you entered multiple user IDs, the status bar displays the number of matches found.
7. **(Optional)** If multiple matches are found, click **Actions > Next** to navigate through the user IDs and their permissions.

Listing all feature access permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Feature Access**.
3. In the **ACD** list, select the ACD or ACD group for which you want to view feature permissions.
4. Click **OK**.
Supervisor displays the User Permissions Feature Access window.
5. From the menu bar, click **Actions > List all**.

CMS Supervisor displays a secondary window listing all users and their associated feature permissions.

Modifying feature access permissions in the PC Client

About this task

In the PC Client, you can modify the feature access permissions for a CMS user. You must also specify the ACD or ACD group.

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Feature Access**.
3. In the **ACD** list, select the ACD or ACD group for which you want to modify feature permissions.
4. Click **OK**.

Supervisor displays the User Permissions Feature Access window.

5. In the **User ID** field, enter the ID of an existing CMS user.
6. From the menu bar, click **Actions > Find one** to display the permissions for the user.

CMS Supervisor displays the permissions for the user.

7. Select the **Read** and **Write** check boxes as required for each feature.
8. When you finish updating the feature permissions, click **Actions > Modify** from the menu bar.

The user permissions for the specified ACD are updated.

Custom menu item assignments and access

Use the Main Menu Addition Access page to identify the custom menu items displayed for each user in the CMS main menu. You can also specify access permissions for each menu item.

You can create custom menu items in the Web Client by navigating to **System Setup > Main Menu Addition**. You can also do this from the CMS ASCII interface. These custom menu items cannot be created through the PC Client.

You see custom menu items when you run the `cms` command to access the CMS Main Menu. You can do this through Terminal Emulator, a telnet session to the CMS server, or the CMS console. Custom menu items are not displayed in the CMS Supervisor interface.

Considerations for access permissions to custom menu items

Consider the following when using the Main Menu Addition Access feature to configure access to custom menu items:

- Ensure that the users you want to manage have been added on the User Data page.
- Before you can assign access to custom menu items, you must create the custom menu items. You can do this from **System Setup > Main Menu Addition** in the Web Client.
- If the assigned Main Menu Addition Access permission for a user is disabled, they will not see the custom menu item in the CMS main menu.
- When you change the access permissions for a user, those changes will not take effect until the user logs out and logs in again.

Adding custom menu item access permissions in the Web Client

About this task

After creating custom menu items, you can assign access permissions for them. You can choose whether you want the user to only view the menu item or you can enable access.

Procedure

1. Navigate to **Administration > User Permissions > Main Menu Addition Access**.
2. Click **Add Main Menu Addition Access** to assign a custom menu item to a user.
3. In the **User ID** list, search for and select the user.
4. From the **Addition** list, select the custom menu item you want to assign.
5. Select the **Access** check box to grant access to the custom menu item.

If you clear this check box, the user can view the menu item in the CMS main menu, but they cannot do anything with it.

6. Click **OK** to save your changes.

Modifying custom menu item access permissions in the Web Client

About this task

You can modify access permissions for assigned custom menu items. You cannot change the user ID or the assigned menu item.

Procedure

1. Navigate to **Administration > User Permissions > Main Menu Addition Access**.
CMS Supervisor displays the assigned custom menu items. It also indicates whether access is enabled.
2. Click  next to the item you want to modify.

The Modify Item window is displayed.

3. Select the **Access** check box to grant access to the custom menu item.

This is the only option you can modify. If you clear the **Access** check box, the user can view the menu item in the CMS main menu, but they cannot do anything with it.

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

Viewing custom menu item access permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Main Menu Addition Access**.
3. Click **OK**.

CMS Supervisor displays the User Permissions Main Menu Addition Access window.

4. In the **User ID** field, enter a CMS user ID.

If required, you can enter more than one user ID. Use a semicolon to separate each value.

5. From the menu bar, navigate to **Actions > Find one**.

CMS Supervisor retrieves the Main Menu Addition Access information for the specified CMS user ID and displays this information in the remaining fields.

6. **(Optional)** If you specified multiple user IDs, click **Actions > Next** to view the other users and their configurations.

Listing all custom menu item access permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Main Menu Addition Access**.
3. Click **OK**.

CMS Supervisor displays the User Permissions Main Menu Addition Access window.

4. From the menu bar, click **Actions > List all**.

CMS Supervisor displays a secondary window listing all CMS users who have custom menu items assigned and the permissions for those custom menu items.

Assigning or modifying custom menu item access permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Main Menu Addition Access**.

3. Click **OK**.

CMS Supervisor displays the User Permissions Main Menu Addition Access window.

4. In the **User ID** field, enter a CMS user ID.

If required, you can enter more than one user ID. Use a semicolon to separate each value.

5. From the menu bar, navigate to **Actions > Find one**.

CMS Supervisor retrieves the Main Menu Addition Access information for the specified CMS user ID and displays this information in the remaining fields.

6. **(Optional)** If you specified multiple user IDs, click **Actions > Next** to navigate through the other users.

7. In the **Addition** field, enter the custom menu item to be assigned.

8. Select the **Access** check box to grant access to the custom menu item.

If you clear this check box, the user can view the menu item in the CMS main menu, but they cannot do anything with it.

9. From the menu bar, click **Actions > Modify** to save your changes.

Only the current CMS user is modified. If other users are available through **Actions > Next**, modify the access permissions for each of them as required.

Access administration for splits and skills

Users do not have access to all splits/skills by default. When adding access on the Split/Skill Access page, you must specify the splits/skills the user will have access to and then assign permissions. The permissions you assign apply to all selected splits/skills. The available permission options are Read, Write, and Exception. With the Exception permission, you are notified of split/skill exceptions when they occur. Exceptions can help you identify call center performance issues.

You can administer split/skill call profiles from **Call Center Administration > Split/Skill Call Profile Setup**.

Considerations for administering access to splits/skills

Consider the following when working with split/skill permissions:

- Ensure that the users you want to manage have been added on the User Data page.
- Users do not have split/skill access by default. You must define which splits/skills a user can access.
- Before you can assign split/skill permissions, the user must first have permissions for the ACD on which the split/skill resides. If you assign split/skill permissions for a user ID that does not have the appropriate ACD permissions, an error is displayed.

- A user ID cannot be assigned the Write permission without also having the Read permission.
- When the permissions definition for a user is added or modified, the permission changes do not take effect until the user logs out and logs in again.
- The wildcard characters “*” and “?” are not supported.
- Tenant users can only have permissions to split/skills in their assigned tenants. A tenant user cannot be assigned a higher permission level than the tenant. For example, if the tenant does not have Write access to splits/skills, you cannot assign Write access to the users in that tenant.

Adding split/skill permissions in the Web Client

About this task

Users do not have access to all splits/skills by default. Specify which splits/skills the user needs and then assign access permissions. You can only assign splits/skills for the current ACD.

Procedure

1. Navigate to **Administration > User Permissions > Split/Skill Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage split/skill access.

CMS Supervisor displays the existing split/skill and exception access permissions for the selected ACD.
3. Click **Add Split/Skill Access** to assign split/skill access to user.
4. In the **User ID** list, search for and select the user.
5. In the **Splits/Skills** field, enter split/skill names or IDs.

Use a semicolon to separate each entry. The entries are displayed in the Search Results area.
6. Click **+** to move the splits/skills you want to assign from the Search Results area to the Selected Split(s)/Skills(s) area.
7. Select one or more of the following check boxes to assign permissions for the specified splits/skills:
 - **Read:** The user can view information and reports for the specified splits/skills.
 - **Write:** The user can administer or manage the specified splits/skills. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions:** The user is notified when active split/skill exceptions occur. For general information about split/skill exceptions, see [Split/skill exceptions](#) on page 226.
8. Click **OK** to save your changes.

Modifying split/skill permissions in the Web Client

About this task

When you modify an item on the Split/Skill Access page, you cannot change the user ID or the assigned splits/skills. You can only modify the access permissions.

Procedure

1. Navigate to **Administration > User Permissions > Split/Skill Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage split/skill access.

CMS Supervisor displays the existing split/skill and exception access permissions for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.

You cannot change any other options.

5. Click **OK** to save your changes.

Deleting split/skill permissions in the Web Client

About this task

You can delete split/skill access configurations that you no longer need. For example, if you want to change the splits/skills assigned to a user, you can delete the existing entry and then add a new one with the appropriate split/skill assignments.

Procedure

1. Navigate to **Administration > User Permissions > Split/Skill Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage split/skill access.

CMS Supervisor displays the existing split/skill and exception access permissions for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to finish deleting the split/skill access item.

Viewing split/skill permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.

2. In the **Operations** list, select **Split/Skill Access**.
3. In the **ACD** list, select the ACD or ACD group containing the split/skill access permissions you want to view.
4. Click **OK**.

CMS Supervisor displays the User Permissions Split/Skill Access window.

5. In the **User ID** field, enter the name of the user whose split/skill permissions you want to view.
6. **(Optional)** If you know which splits/skills you want to view, enter their names or IDs in the **Splits/Skills** field.

You can enter one or more split/skill values. If you enter multiple values, separate them with a semicolon.

To have all splits/skills returned for this user ID, leave this field blank.

7. From the menu bar, navigate to **Actions > Find one**.

CMS Supervisor queries the database and displays the number of matches found.

Listing all split/skill user permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Split/Skill Access**.
3. In the **ACD** list, select the ACD or ACD group containing the split/skill access permissions you want to view.
4. Click **OK**.

CMS Supervisor displays the User Permissions Split/Skill Access window.

5. From the menu bar, navigate to **Actions > List all** to display

If you do not complete any of the fields in the User Permissions Split/Skill Access window, all split/skill permissions for the specified ACD are displayed. The results are filtered based on any user ID or split/skill information you enter before clicking **List all**. For example, to only view user permission definitions for skill 26, enter 26 in the **Splits/Skills** field.

Adding split/skill permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Split/Skill Access**.
3. In the **ACD** list, select the ACD or ACD group for which you want to manage split/skill access.
4. Click **OK**.

CMS Supervisor displays the User Permissions Split/Skill Access window.

5. In the **User ID** field, enter the name of the user who will be assigned split/skill permissions.
6. In the **Splits/Skills** field, enter the names or IDs of the splits/skills you want to assign to the user.

If you enter multiple values, use a semicolon to separate each entry. Alternatively, you can enter a range such as 1–256.
7. Select one or more of the following check boxes to assign permissions for the specified splits/skills:
 - **Read**: The user can view information and reports for the specified splits/skills.
 - **Write**: The user can administer or manage the specified splits/skills. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions**: The user is notified when active split/skill exceptions occur. For general information about split/skill exceptions, see [Split/skill exceptions](#) on page 226.
8. From the menu bar, click **Actions > Add** to save your changes.

Modifying split/skill permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Split/Skill Access**.
3. In the **ACD** list, select the ACD or ACD group for which you want to manage split/skill access.
4. Click **OK**.

CMS Supervisor displays the User Permissions Split/Skill Access window.

5. In the **User ID** field, enter the name of the user whose split/skill permissions you want to manage.
6. **(Optional)** In the **Splits/Skills** field, enter the names or IDs of the splits/skills you want to view.

Use a semicolon to separate each value you enter.

To view all splits/skills for the specified user ID, leave this field blank.

7. From the menu bar, click **Actions > Find one**.
8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct split/skill entry.
9. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
10. After completing the permission changes, click **Actions > Modify** from the menu bar.

Deleting split/skill permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Split/Skill Access**.
3. In the **ACD** list, select the ACD or ACD group containing the split/skill access permissions you want to delete.
4. Click **OK**.

CMS Supervisor displays the User Permissions Split/Skill Access window.

5. In the **User ID** field, enter the name of the user whose split/skill permissions you want to manage.
6. **(Optional)** In the **Splits/Skills** field, enter the names or IDs of the splits/skills you want to view.

Use a semicolon to separate each value you enter.

To view all splits/skills for the specified user ID, leave this field blank.

7. From the menu bar, click **Actions > Find one**.
8. When you find the item you want to delete, click **Actions > Delete** in the menu bar.

CMS Supervisor deletes the selected permissions definition and its associated splits/skills, which are displayed in the **Splits/Skills** field. Other split/skill permission definitions for the user remain unchanged.

Access administration for trunk group data

Users do not have access to all trunk groups by default. When adding access on the Trunk Group Access page, you must specify which trunk groups the user will have access to and then assign permissions. With the Read permission, the user can view data for trunk group reports and view trunk group configuration information. The Write permission is required to change trunk group configurations. You can also assign the Exception permission so the user is notified of trunk group exceptions when they occur. Exceptions can help to identify call center performance issues.

Considerations for administering access to trunk group data

Consider the following when working with trunk group permissions:

- Ensure that the users you want to manage have been added on the User Data page.
- Users do not have trunk group access by default. You must define which trunk groups each user can access and then assign Read, Write, and Exception permissions as required.

- Before you can assign trunk group permissions, the user must first have permissions for the ACD on which the trunk group resides. If you assign trunk group permissions for a user ID that does not have the appropriate ACD permissions, an error is displayed.
- A user ID cannot be assigned the Write permission without also having the Read permission.
- When the permissions definition for a user is added or modified, the permission changes do not take effect until the user logs out and logs in again.
- The wildcard characters "*" and "?" are not supported.
- Tenant users can only be given permissions to the trunk groups that are available for their tenants. If the tenant does not have access to a trunk group, its tenant users cannot be given permissions for that trunk group. A tenant user cannot be assigned a higher permission level than the tenant. For example, if the tenant does not have Write access, then its tenant users cannot be given Write access.

Adding trunk group data permissions in the Web Client

About this task

Users can only access the trunk groups you assign to them. After specifying which trunk groups the user needs, you must assign access permissions. You can only assign trunk groups for the current ACD.

Procedure

1. Navigate to **Administration > User Permissions > Trunk Group Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage trunk group access.

CMS Supervisor displays the existing trunk group data and exception access permissions for the selected ACD.
3. Click **Add Trunk Group Access** to assign trunk group access to a user.
4. In the **User ID** list, search for and select the user.
5. In the **Trunk Groups** field, enter trunk group names or IDs.

Use a semicolon to separate each entry. The entries are displayed in the Search Results area.
6. Click **+** to move the trunk groups you want to assign from the Search Results area to the Selected Trunk Group(s) area.
7. Select one or more of the following check boxes to assign permissions for the specified trunk groups:
 - **Read:** The user can view trunk group report data and other trunk group information.
 - **Write:** The user can administer or manage the specified trunk groups. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions:** The user is notified when active trunk group exceptions occur. For general information about trunk group exceptions, see [Trunk group exceptions](#) on page 230.

8. Click **OK** to save your changes.

Modifying trunk group data permissions in the Web Client

About this task

When you modify an item on the Trunk Group Access page, you cannot change the user ID or the assigned trunk groups. You can only modify the access permissions.

Procedure

1. Navigate to **Administration > User Permissions > Trunk Group Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage trunk group access.

CMS Supervisor displays the existing trunk group data and exception access permissions for the selected ACD.

3. Click  next to the item you want to modify.

The Modify Item window is displayed.

4. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.

You cannot change any other options.

5. Click **OK** to save your changes.

Deleting trunk group data permissions in the Web Client

About this task

You can delete trunk group access configurations you no longer need. For example, if you want to change the trunk groups assigned to a user, you can delete the existing entry and then add a new one with the appropriate trunk group assignments.

Procedure

1. Navigate to **Administration > User Permissions > Trunk Group Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage trunk group access.

CMS Supervisor displays the existing trunk group data and exception access permissions for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the process.

Viewing trunk group data permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Trunk Group Access**.
3. In the **ACD** list, select the ACD containing the trunk group access permissions you want to view.
4. Click **OK**.

CMS Supervisor displays the User Permissions Trunk Group Access window.

5. In the **User ID** field, enter the name of the user whose trunk group permissions you want to view.
6. **(Optional)** If known, enter the trunk group names or IDs in the **Trunk Groups** field.

If you enter more than one trunk group, separate each entry with a semicolon.

To have all trunk groups returned for this user ID, leave this field blank.

7. From the menu bar, click **Actions > Find one**.

The database is queried and the number of matches are displayed.

Listing all trunk group data permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Trunk Group Access**.
3. In the **ACD** list, select the ACD containing the trunk group access permissions you want to view.
4. Click **OK**.

CMS Supervisor displays the User Permissions Trunk Group Access window.

5. From the menu bar, click **Actions > List all**.

If you do not complete any of the fields in the User Permissions Trunk Group Access window, all trunk group permissions for the specified ACD are displayed. The results are filtered if you specify a user ID or trunk groups before clicking **List all**. For example, to only view user permission definitions for trunk group 4, type 4 in the **Trunk Groups** field before clicking **List all**.

Adding trunk group data permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Trunk Group Access**.

3. In the **ACD** list, select the ACD containing the trunk groups for which you want to assign permissions.
4. Click **OK**.
CMS Supervisor displays the User Permissions Trunk Group Access window.
5. In the **User ID** field, enter the name of the user who will be assigned trunk group permissions.
6. In the **Trunk Groups** field, enter the names or IDs of the trunk groups you want to assign.
If you enter multiple trunk groups, separate each value with a semicolon.
7. Select one or more of the following check boxes to assign permissions for the specified trunk groups:
 - **Read**: The user can view trunk group report data and other trunk group information.
 - **Write**: The user can administer or manage the specified trunk groups. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions**: The user is notified when active trunk group exceptions occur. For general information about trunk group exceptions, see [Trunk group exceptions](#) on page 230.
8. From the menu bar, click **Actions > Add** to save your changes.

Modifying trunk group data permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Trunk Group Access**.
3. In the **ACD** list, select the ACD containing the trunk groups for which you want to manage permissions.
4. Click **OK**.
CMS Supervisor displays the User Permissions Trunk Group Access window.
5. In the **User ID** field, enter the name of the user whose access permissions you want to manage.
6. **(Optional)** If known, enter the trunk group names or IDs in the **Trunk Groups** field.
If you enter more than one trunk group, separate each entry with a semicolon.
To have all trunk groups returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.
8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct trunk group entry.
9. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
10. From the menu bar, click **Actions > Modify** to complete your changes.

Deleting trunk group data permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Trunk Group Access**.
3. In the **ACD** list, select the ACD containing the trunk group permissions you want to delete.
4. Click **OK**.

CMS Supervisor displays the User Permissions Trunk Group Access window.

5. In the **User ID** field, enter the name of the user whose access permissions you want to manage.
6. **(Optional)** If known, enter the trunk group names or IDs in the **Trunk Groups** field.
If you enter more than one trunk group, separate each entry with a semicolon.
To have all trunk groups returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.
8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct trunk group entry.
9. From the menu bar, click **Actions > Delete**.

CMS Supervisor deletes the selected permissions definition and its associated trunk groups. Other trunk group permissions for the user remain unchanged.

ACD access permissions

Use the ACD Access page to view or manage the ACD permissions assigned to a user. The available permission options include Read, Write, and Exception. Typically users are granted access to all ACDs, but you can modify or remove their permissions. You can also grant access to an ACD if required.

Considerations for administering access to ACDs

Consider the following when working with ACD access permissions:

- By default, a newly-created user is granted Read, Write, and Exceptions permissions for all ACDs.
- When you create a tenant user, they only have access to selected login ACD by default. As an administrator, you can give the tenant user access to another ACD if required.
- User permissions for ACD access are stored separately from the user ID created on the User Data page. Therefore, ACD permissions can be deleted and modified without affecting the state of the user ID.

- If the ACD permissions for a user are changed, the change does not take effect until the user logs out and logs back in again.
- Users can only access features on an ACD for which they have permissions. If you disable a user's Read and Write permissions, then the user cannot access any splits/skills, trunk groups, vectors, or VDNs in that ACD. If Read is enabled and Write is disabled, the user can view but cannot modify splits/skills, trunk groups, vectors, or VDNs in that ACD.
- In some instances, you might need to restrict a user from viewing information on an ACD. You can modify the user's ACD permissions or delete the user's ACD permissions definition. Deleting the permissions definition does not restrict the permissions for the user, but actually deletes the user from the specified ACD.
- If the permissions for a user's default login ACD are removed, the user must have another login ACD assigned.

Adding ACD access permissions in the Web Client

About this task

Use this procedure to grant access to an ACD and assign permissions for it.

Procedure

1. Navigate to **Administration > User Permissions > ACD Access**.
CMS Supervisor displays the list of administered users and their ACD access permissions.
2. Click **Add ACD Access**.
3. In the **User ID** list, select the user who needs ACD access.
4. In the **ACD** list, select the ACD to which you want to grant access.
5. Select one or more of the following check boxes to assign permissions to the specified ACD:
 - **Read**: The user can view ACD information.
 - **Write**: The user can modify ACD information, such as splits/skills, trunk groups, vectors, and VDNs. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions**: The user receives ACD exception notifications when they occur.
6. Click **OK** to save your changes.

Modifying ACD access permissions in the Web Client

About this task

You can modify the ACD permissions assigned to a user.

Procedure

1. Navigate to **Administration > User Permissions > ACD Access**.
CMS Supervisor displays the list of administered users and their ACD access permissions.

2. Click  next to the user whose ACD permissions you want to modify.
3. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
You cannot change any other options.
4. Click **OK** to save your changes.

Deleting ACD access permissions in the Web Client

About this task

Use this procedure to delete the ACD permissions assigned to a user. You cannot delete ACDs assigned to the "cmssvc" user ID.

Procedure

1. Navigate to **Administration > User Permissions > ACD Access**.
CMS Supervisor displays the list of administered users and their ACD access permissions.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. Click **Yes** to proceed with deleting the selected item.

Viewing ACD permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **ACD Access**.
3. Click **OK**.
Supervisor displays the User Permissions ACD Access window.
4. In the **User ID** field, enter the ID of the CMS user whose ACD permissions you want to view.
This field is required.
5. **(Optional)** If you want to search for specific ACDs, enter them in the **ACDs** field.
Use a semicolon to separate multiple values.
6. From the menu bar, click **Actions > Find one**.
The status bar displays how many matching permission definitions are available. The fields of this window display the user permissions definition for the first ACD.
7. **(Optional)** If more than one ACD is returned, click **Next** and **Previous** in the **Actions** menu as needed to navigate through the entries.

Listing all ACD permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **ACD Access**.
3. Click **OK**.

Supervisor displays the User Permissions ACD Access window.

4. From the menu bar, click **Actions > List all**.

User permission definitions are displayed with their corresponding ACDs. Only the ACDs for which you have Read permissions are shown.

Adding ACD permissions in the PC Client

About this task

You can grant access to any ACD or ACD group from the PC Client.

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **ACD Access**.
3. Click **OK**.

Supervisor displays the User Permissions ACD Access window.

4. In the **User ID** field, enter the ID of the user who needs ACD access.

If required, you can enter multiple users in this field. Separate each value with a semicolon.

5. In the **ACD** field, enter the names or IDs of the ACDs the user will be able to access (real, pseudo, or group).

You can enter one or more ACD values. If you enter multiple values, separate them with a semicolon.

6. Select one or more of the following check boxes to assign permissions:

- **Read:** The user can view ACD information.
- **Write:** The user can modify ACD information, such as splits/skills, trunk groups, vectors, and VDNs. To assign Write access, you must select both **Read** and **Write**.
- **Exceptions:** The user receives ACD exception notifications when they occur.

7. After assigning the necessary permissions, click **Actions > Add** from the menu bar.

The ACD permissions are saved. If you entered multiple user IDs, all specified users are granted access to the specified ACDs.

Modifying ACD permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **ACD Access**.
3. Click **OK**.

Supervisor displays the User Permissions ACD Access window.

4. In the **User ID** field, enter the ID of the user whose ACD permissions you want to modify.
5. **(Optional)** If you are searching for specific ACDs or ACD groups, enter them in the **ACDs** field.

If you enter multiple values, separate them with a semicolon.

6. From the menu bar, click **Actions > Find one**.
7. **(Optional)** If more than one ACD is returned, click **Next** and **Previous** in the **Actions** menu as needed until you find the ACD permissions definition you want to modify.
8. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required to modify the access permissions.
9. To finish changing the permissions, click **Actions > Modify** from the menu bar.

Deleting ACD permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **ACD Access**.
3. Click **OK**.

Supervisor displays the User Permissions ACD Access window.

4. In the **User ID** field, enter the ID of the user whose ACD permissions you want to remove.
5. **(Optional)** If you are searching for specific ACDs or ACD groups, enter them in the **ACDs** field.

If you enter multiple values, separate them with a semicolon.

6. From the menu bar, click **Actions > Find one**.
7. **(Optional)** If more than one ACD is found, click **Next** and **Previous** in the **Actions** menu as required to navigate through the permission definitions for the other ACDs.
8. When the correct permission definition is displayed, click **Actions > Delete** from the menu bar.

The ACD permission definition for this user is deleted.

Vector access administration

A vector is a series of steps that the contact center uses to route calls and determine the treatment for each call. You can manage vector data if Call Vectoring is enabled on your ACD.

You can assign vector access to users from the Vector Access page. When adding access, you must specify which vectors the user will have access to and then assign permissions. With the Read permission, the user can view vector data in reports and view vector configuration information. The Write permission is required to manage vector configurations. You can also assign the Exceptions permission so users are notified of vector exceptions when they occur.

Considerations for administering access to vector data

To manage vectors, the Call Vectoring feature must be enabled. Consider the following when working with vector permissions:

- Ensure that the users you want to manage have been added on the User Data page.
- Users do not have vector access by default. You must define which vectors each user can access and then assign Read, Write, and Exceptions permissions as required.
- Before assigning vector permissions, ensure that the user has permissions for the ACD on which the vector resides. before vector permissions can be assigned. If you assign vector permissions for a user ID that does not have the appropriate ACD permissions, an error is displayed.
- A user ID cannot be assigned the Write permission without also having the Read permission.
- When the permissions definition for a user is added or modified, the permission changes do not take effect until the user logs out and logs in again.
- The wildcard characters “*” and “?” are not supported.
- Tenant users can only be given permissions to vectors that are available for their tenants. A tenant user cannot be assigned a higher permission level than the tenant. For example, if the tenant does not have Write access for vectors, then its tenant users cannot be given Write access.

Adding vector access permissions in the Web Client

About this task

Users can only access the vectors you assign to them. After specifying which vectors the user can access, you must assign access permissions. You can only assign vectors for the current ACD.

Procedure

1. Navigate to **Administration > User Permissions > Vector Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage vector access.

CMS Supervisor displays the existing vector data and exception access permissions for the selected ACD.

3. Click **Add Vector Access** to assign vectors to a user and grant access permissions.
4. In the **User ID** list, search for and select the user.
5. In the **Vectors** field, enter vector names or IDs.
You can enter a range or specify multiple values separated with a semicolon.
6. Click **+** to move the vectors you want to assign from the Search Results area to the Selected Vector(s) area.
7. Select one or more of the following check boxes to assign permissions for the specified vectors:
 - **Read**: The user can view vector report data and other vector information.
 - **Write**: The user can administer or manage the specified vectors. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions**: The user is notified when active vector exceptions occur. For general information about vector exceptions, see [Vector exceptions](#) on page 240.
8. Click **OK** to save your changes.

Modifying vector permissions in the Web Client

About this task

When you modify an item on the Vector Access page, you cannot change the user ID or the assigned vectors. You can only modify the access permissions.

Procedure

1. Navigate to **Administration > User Permissions > Vector Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage vector access.

CMS Supervisor displays the existing vector data and exception access permissions for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
You cannot change any other options.
5. Click **OK** to save your changes.

Deleting vector permissions in the Web Client

About this task

You can delete vector access configurations you no longer need. If you want to change the vectors assigned to a user, you can delete the existing entry and then add a new one with the appropriate vectors assigned.

Procedure

1. Navigate to **Administration > User Permissions > Vector Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage vector access.

CMS Supervisor displays the existing vector data and exception access permissions for the selected ACD.
3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing vector permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Vector Access**.
3. In the **ACD** list, select the ACD containing the vectors for which the user has a permissions definition.
4. Click **OK**.

CMS Supervisor displays the User Permissions Vector Access window.
5. In the **User ID** field, enter the name of the user for which the vector permissions definition is to be viewed.
6. **(Optional)** If known, enter the names or IDs of the vectors you want to view in the **Vectors** field.

If you enter multiple values, use a semicolon to separate each entry.

To have all vectors returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.

The database is queried and the status bar displays the number of matches found for this user ID.

Listing all vector permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Vector Access**.
3. In the **ACD** list, select the ACD containing the vectors for which you want to view permissions.
4. Click **OK**.

CMS Supervisor displays the User Permissions Vector Access window.

5. From the menu bar, click **Actions > List all**.

If you do not complete any of the fields in the User Permissions Vector Access window, all vector permissions for the specific ACD are displayed. The results are filtered if you specify a user ID or vectors before clicking **List all**. For example, to only view the permission definitions for vector 1, type 1 in the **Vectors** field before clicking **List all**.

Adding vector permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Vector Access**.
3. In the **ACD** list, select the ACD containing the vectors for which you want to assign permissions.
4. Click **OK**.

CMS Supervisor displays the User Permissions Vector Access window.

5. In the **User ID** field, enter the name of the user who will be assigned vector permissions.
6. In the **Vectors** field, enter the name or IDs of the vectors you want to assign.

If you enter multiple values, separate them with a semicolon.

7. Select one or more of the following check boxes to assign permissions for the specified vectors:
 - **Read**: The user can view vector report data and other vector information.
 - **Write**: The user can administer or manage the specified vectors. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions**: The user is notified when active vector exceptions occur. For general information about vector exceptions, see [Vector exceptions](#) on page 240.
8. After assigning the necessary permissions, click **Actions > Add** from the menu bar.

The vector permissions for this user are saved.

Modifying vector permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Vector Access**.
3. In the **ACD** list, select the ACD containing the vectors for which you want to manage permissions.
4. Click **OK**.

CMS Supervisor displays the User Permissions Vector Access window.

5. In the **User ID** field, enter the name of the user whose permissions you want to modify.
6. **(Optional)** In the **Vectors** field, enter the names or IDs of the vectors you want to view.
If you enter multiple values, separate them with a semicolon.
To have all vectors returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.
The fields for the first match are populated.
8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct entry.
9. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
10. From the menu bar, click **Actions > Modify** to save your permission changes.

Deleting vector permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **Vector Access**.
3. In the **ACD** list, select the ACD containing the vector permissions you want to delete.
4. Click **OK**.
CMS Supervisor displays the User Permissions Vector Access window.
5. In the **User ID** field, enter the name of the user whose vector permissions you want to manage.
6. **(Optional)** In the **Vectors** field, enter the names or IDs of the vectors you want to view.
If you enter multiple values, separate them with a semicolon.
To have all vectors returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.
8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct entry.
9. From the menu bar, click **Actions > Delete**.

CMS Supervisor deletes the selected permissions definition and its associated vectors. Other vector permissions for the user are not affected.

VDN access administration

You can manage VDN data if Call Vectoring is enabled on your ACD.

When adding VDN access, you must specify which VDNs to the user will be able to access and then assign permissions. Users with the Read permission can view VDN report data and other VDN configuration information. The Write permission is required to change VDN configurations. You can also assign the Exceptions permission so users are notified when VDN exceptions occur.

Considerations for administering access to VDN data

Consider the following when working with VDN permissions:

- Ensure that the users you want to manage have been added on the User Data page.
- Users do not have VDN access by default. You must define which VDNs a user can access and then assign Read, Write, and Exceptions permissions as required.
- Before assigning vector permissions, ensure that the user has permissions for the ACD on which the VDN resides. If you assign VDN permission for a user ID that does not have the appropriate ACD permissions, an error is displayed.
- A user ID cannot be assigned the Write permission without also having the Read permission.
- When the permissions definition for a user is added or modified, the permission changes do not take effect until the user logs out and logs in again.
- The wildcard characters “*” and “?” are not supported.
- Tenant users can only be given permissions to VDNs that are available for their tenants. A tenant user cannot be assigned a higher permission level than the tenant. For example, if the tenant does not have Write access, then its tenant users cannot be given Write access.

Adding VDN data user permissions using the Web Client

About this task

You must specify which VDNs users will have access to and then assign permissions. You can only assign VDNs for the current ACD.

Procedure

1. Navigate to **Administration > User Permissions > VDN Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage VDN access.

CMS Supervisor displays the existing VDN data and exception access permissions for the selected ACD.
3. Click **Add VDN Access**.
4. In the **User ID** list, search for and select the user.
5. In the **VDNs** field, enter VDN names or IDs.

Use a semicolon to separate each entry.
6. Click **+** to move the VDNs you want to assign from the Search Results area to the Selected VDN(s) area.

7. Select one or more of the following check boxes to assign permissions for the specified VDNs:
 - **Read:** The user can view VDN data.
 - **Write:** The user can manage the specified VDNs. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions:** The user is notified when active VDN exceptions occur. For general information about VDN exceptions, see [VDN exceptions](#) on page 235.
8. Click **OK** to save your changes.

Modifying VDN permissions in the Web Client

About this task

When you modify an item on the VDN Access page, you cannot change the user ID or the assigned VDNs. You can only modify the access permissions.

Procedure

1. Navigate to **Administration > User Permissions > VDN Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage VDN access.

CMS Supervisor displays the existing VDN data and exception access permissions for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
You cannot change any other options.
5. Click **OK** to save your changes.

Deleting VDN permissions in the Web Client

About this task

You delete VDN access configurations you no longer need. If you want to change the VDNs assigned to a user, you can delete the existing entry and then assign a new one with the appropriate VDNs assigned.

Procedure

1. Navigate to **Administration > User Permissions > VDN Access**.
2. From the **Current ACD** list, select the active ACD for which you want to manage VDN access.

CMS Supervisor displays the existing VDN data and exception access permissions for the selected ACD.

3. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to complete the change.

Viewing VDN permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **VDN Access**.
3. In the **ACD** list, select the ACD containing the VDN for which the user has a permissions definition.
4. Click **OK**.
CMS Supervisor displays the User Permissions VDN Access window.
5. In the **User ID** field, enter the name of the user whose VDN permissions you want to view.
6. **(Optional)** If known, enter the names or IDs of the VDNs you want to view in the **VDNs** field.
Multiple entries must be separated with a semicolon.
To have all VDNs returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.
The database is queried and the status bar displays the number of matches found for this user ID.

Listing all VDN permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **VDN Access**.
3. In the **ACD** list, select the ACD containing the VDN for which all permission definitions will be shown.
4. Click **OK**.
CMS Supervisor displays the User Permissions VDN Access window.
5. From the menu bar, click **Actions > List all**.
If you did not complete any of the fields in the User Permissions VDN Access window, all VDN permissions for the specified ACD are displayed. The results are filtered if you specify a user ID or VDNs before clicking **List all**. For example, to only view the permission definitions for VDN 10, type 10 in the **VDNs** field before clicking **List all**.

Adding VDN permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **VDN Access**.
3. In the **ACD** list, select the ACD containing the VDNs for which you want to assign permissions.
4. Click **OK**.

CMS Supervisor displays the User Permissions VDN Access window.

5. In the **User ID** field, enter the name of the user who will be assigned VDN permissions.
6. In the **VDNs** field, enter the names or IDs of the VDNs you want to assign.

If you enter multiple values, separate them with a semicolon.

7. Select one or more of the following check boxes to assign permissions for the specified VDNs:
 - **Read**: The user can view VDN data.
 - **Write**: The user can manage the specified VDNs. To assign Write access, you must select both **Read** and **Write**.
 - **Exceptions**: The user is notified when active VDN exceptions occur. For general information about VDN exceptions, see [VDN exceptions](#) on page 235.
8. After assigning the necessary permissions, click **Actions > Add** from the menu bar.

Modifying VDN permissions in the PC Client

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **VDN Access**.
3. In the **ACD** list, select the ACD containing the VDNs for which you want to manage permissions.
4. Click **OK**.

CMS Supervisor displays the User Permissions VDN Access window.

5. In the **User ID** field, enter the name of the user whose permissions you want to modify.
6. **(Optional)** If known, enter the names or IDs of the VDNs you want to view in the **VDNs** field.

Multiple entries must be separated with a semicolon.

To have all VDNs returned for this user ID, leave this field blank.

7. From the menu bar, click **Actions > Find one**.

The fields for the first match are populated.

8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct entry.
9. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
10. From the menu bar, click **Actions > Modify** to save your permission changes.

Deleting VDN permissions in the PC Client

About this task

Use this procedure to delete the VDN permissions definition for a CMS user.

Procedure

1. From the Controller window, navigate to **Tools > User Permissions**.
2. In the **Operations** list, select **VDN Access**.
3. In the **ACD** list, select the ACD containing the VDN permissions you want to delete.
4. Click **OK**.
CMS Supervisor displays the User Permissions VDN Access window.
5. In the **User ID** field, enter the name of the user whose VDN permissions definition is to be deleted.
6. **(Optional)** If known, enter the names or IDs of the VDNs you want to view in the **VDNs** field.
Multiple entries must be separated with a semicolon.
To have all VDNs returned for this user ID, leave this field blank.
7. From the menu bar, click **Actions > Find one**.
The fields for the first match are populated.
8. **(Optional)** If multiple matches are found, click **Next** and **Previous** in the **Actions** menu as needed to navigate to the correct entry.
9. When you find the entry you want to delete, click **Actions > Delete** from the menu bar.
CMS Supervisor deletes the selected permissions definition and its associated VDNs.
Other VDN permissions for the user are not affected.

Access to tenant data

You can manage tenant data if the Tenancy feature package is licensed and installed.

From the Tenant Access page, you can assign tenant access to any CMS user. When adding tenant access, specify which tenants you want the user to access and then assign permissions for the selected tenants. The Read permission enables the user to view tenant data. The Write

permission is required to change tenant configurations. You can also assign the Exceptions permission so the user is notified about exceptions when they occur.

Specific tenant permissions are combined with Tenant and Dictionary feature permissions. The dictionary name for each tenant number is defined in the Dictionary. If a normal user or administrator has Write access to the Tenant feature, they can modify tenant assignments for the specific tenants to which they have access. Tenant users can view tenant assignments but cannot modify them.

Considerations for administering access to tenant data

Consider the following when working with tenant permissions:

- Ensure that the users you want to manage have been added on the User Data page.
- A user ID must first have permissions for the ACD on which the tenant resides before tenant permissions can be assigned.
- Users can only access the specific tenants for which they have permissions. Before you assign access to specific tenants from the Tenant Access page, the user must also have permissions for the Tenant feature on the Feature Access page.
- You can grant a normal user or administrator Read and Write permissions for tenant assignments. With the Write permission, the user can change tenant assignments for the specified tenants to which they have access.
- You can also grant a tenant user access to specific tenants. However, tenant users cannot have Write permissions for the Tenant feature so they cannot change tenant assignments.
- A user ID cannot be assigned the Write permission without also having the Read permission.
- When the permissions definition for a user is added or modified, the permission changes do not take effect until the user logs out and logs in again.
- The wildcard characters “*” and “?” are not supported.

Adding tenant permissions in the Web Client

About this task

Users can view or manage the specific tenants for which they have permissions. In this procedure, you must define which tenants a user can access and then assign permissions. You can add tenant access permissions for any user. Note that tenant users cannot modify tenant assignments.

Procedure

1. Navigate to **Administration > User Permissions > Tenant Access**.
2. In the **Current ACD** list, select the active ACD for which you want to administer tenant data permissions.

CMS Supervisor displays the list of administered users and their current tenant data and exception access permissions for the selected ACD.

3. Click **Add Tenant Access**.

4. In the **User ID** list, search for and select the user.
5. In the **Tenants** field, enter tenant names or IDs.
Use a semicolon to separate each entry.
6. Click **+** to move the tenants you want to assign from the Search Results area to the Selected Tenant(s) area.
7. Select one or more of the following check boxes to assign permissions for the specified tenants:
 - **Read**: To view tenant data.
 - **Write**: To assign Write permissions, you must select **Read** and **Write**. Note that tenant users cannot change tenant assignments.
 - **Exceptions**: To receive exception notifications.
8. Click **OK** to save your changes.

Modifying tenant permissions in the Web Client

About this task

When you modify an entry, you can only change the assigned permissions. You cannot change the user ID or the selected tenants.

Procedure

1. Navigate to **Administration > User Permissions > Tenant Access**.
2. In the **Current ACD** list, select the active ACD for which you want to administer tenant data permissions.

CMS Supervisor displays the list of administered users and their current tenant data and exception access permissions for the selected ACD.
3. Click  next to the item you want to modify.
The Modify Item window is displayed.
4. Select or clear the **Read**, **Write**, and **Exceptions** check boxes as required.
You cannot change any other options.
5. Click **OK** to save your changes.

Deleting tenant permissions in the Web Client

About this task

Delete tenant access permissions that are no longer required.

Procedure

1. Navigate to **Administration > User Permissions > Tenant Access**.

2. In the **Current ACD** list, select the active ACD for which you want to administer tenant data permissions.

CMS Supervisor displays the list of administered users and their current tenant data and exception access permissions for the selected ACD.

3. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

4. Click **Yes** to complete the change.

Administering access to tenant data using the PC Client

Use **Tools > User Permissions** to go to the **Tenant Access** menu item under the **Operations** list. Administrators must use **Tenant Access** to assign tenant permissions to users.

Tenant permissions have the following implications:

- For administrators and normal users, specific tenant permissions combined with tenant and dictionary feature permissions control the following:
 - whether the user can read and write tenant assignments for the specified tenant number.
 - whether the user can read and write the tenant dictionary name for the specified tenant number.
- For tenant users, specific tenant permissions combined with tenant and dictionary feature permissions control the following:
 - whether the user can read tenant assignments for the specified tenant number. It should be noted that tenant users are not allowed to have write permission for the Tenant feature and thus will never be able to add/delete tenant assignments.
 - When VDN, split/skill, and trunk group permissions are administered for a tenant user, the permissions for the associated tenant is checked to ensure that the tenant user has proper permissions for the associated tenant.
 - A tenant user can only access agents and tenant agent groups when the tenant user has proper permissions for the associated tenant for the agents/agent groups.

The Tenant Access window includes the following fields:

- **User ID** is the user's operating system (Linux) login identification.
- **Tenant Number** must be between 1 and 250.
- **Read**, **Write**, or **Exceptions** fields only allow **y** or **n**.

Tenant access operations using the PC Client

The Tenant Access window provides an action list containing the following actions:

Field	Description
Add	Adds the User id with the specified permissions on the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the User Permissions feature.
Delete	Removes the User Id and the associated permissions on the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the User Permissions feature. When a tenant permission record is deleted for a tenant user, all the permissions of the tenant user for the tenant's associated splits/skills, trunk groups, and VDNs are also deleted.
Find one	Finds an entry in the database that matches all the field values on the current window. The status line for the current window indicates the total number of matches found. The user must have read permission for the User Permissions feature.
Modify	Modifies the permissions of the user id entered in the current user window. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the User Permissions feature. When a tenant permission record is modified to be more restricted for a tenant user, the restriction is propagated down to all the user's permissions for the tenant's associated splits/skills, trunk groups, and VDNs.
List all	Lists all entries that match all the field values currently present in the Tenant Access window . The user must have read permission for the User Permissions feature.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Chapter 8: Administering exceptions

An exception is a type of activity in the ACD that falls outside the limits that have been defined and could indicate unacceptable performance. You can manage exceptions and run reports for the following exception areas:

- Agent
- Split/skill
- Trunk group
- VDN
- Vector
- Data collection
- Malicious call trace
- Real-time exceptions log



Note:

To administer exceptions and generate reports for VDNs and vectors, the Call Vectoring feature must be enabled. For skills, the EAS feature must be enabled.

Types of exceptions

An exception can be one of three types:

- Peg count
- Agent timed
- Other timed exceptions

Peg count exceptions

A peg count exception occurs when the number of occurrences for an ACD activity exceeds an occurrence threshold that is defined for your call center in the current interval. The current interval is a set number of either 15, 30, or 60 minutes. Many CMS exceptions are measured based on this interval.

Most exception conditions apply to ACD events that occur within the current interval that is defined for your call center. When the interval changes, ACD event occurrences are cleared and CMS

begins to count event occurrences again. Therefore, your exception conditions should realistically reflect what you want to trigger an exception within your current interval.

Agent timed exceptions

Agent timed exceptions are tracked from the time that the agent logs in until the agent logs out. These exceptions can occur many times during the login period and within an interval. The exception count is cleared when the agent leaves the state that triggered the exception. For example, you can configure an agent timed exception to occur when an agent spends more than 5 minutes in the AUX work mode. When the agent changes to another state, such as AVAIL, the exception is reset so that it can occur again when the agent reenters the AUX work mode.

Other timed exceptions

Other timed exceptions are triggered when the number of ACD activity occurrences exceeds the minimum or maximum time limits that are set for such activity. For example, you can set the time limit at 20 seconds for any call to wait in queue before being answered. You can then define an occurrence boundary of three for the acceptable number of calls that can wait in the queue for 20 seconds. An exception occurs if more than three calls wait in the queue for more than 20 seconds within an interval.

Timed occurrence boundaries for this type of exception apply to ACD activities within the last interval. At the beginning of the next interval, the occurrence count for any timed exception type, except for agent timed exceptions, is cleared and starts again from zero. However, since the time limit for a timed exception type can be more than one hour, the duration of an exception activity is not cleared at the end of the intrahour interval. CMS continues to track the time that is spent on an exception activity that continues from one interval to the next for this type of exception.

The following data collection exceptions are sent when the link is active:

- ACD <number>: data collection started
- ACD <number>: data collection started - new translations

When the primary ACD system (for example, Communication Manager) starts collecting data, exceptions are generated. When the secondary ACD starts collecting data, one of the following new exceptions is generated:

- ACD <number>: data collection to the secondary ACD system started
- ACD <number>: data collection to the secondary ACD system started - new translations

Exception capacities

To record contact center activities and exceptions, define storage space on the server. CMS handles exception records as follows:

- CMS store exception records for each element. There are exception records stored for elements like agents, split/skill, trunk groups, VDNs, and vectors across all ACDs.
- You can retrieve stored exception records from the ACD. The exception records are stored for a limited time, as defined by the following criteria:
 - The number of exception records that are allocated for storage in **System Setup > Data Storage**.

- The frequency with which exceptions are recorded each day. For example, if you allocate storage for 1000 exception records and approximately 100 exceptions occur each day, you can save exception records for nearly 10 days.

Considerations for exception thresholds

When exception thresholds are configured, consider the following:

- The occurrence threshold for any exception must be between 0 to 999.
- The time limit for timed exceptions must be between 0 to 28800 seconds.
- If a time limit is entered for an activity, an occurrence threshold for that activity must also be entered.
- When an exception is made active, CMS starts checking for the exception immediately as long as data collection is activated.
- The default setting for most exceptions is “off”. However, the following exceptions are always active and cannot be stopped:
 - Malicious call trace
 - Data collection disruptions
 - Audio difficulty
 - Agent attempts to log in with more than one login ID

Permissions for administering exceptions

Navigate to **User Permissions** to assign permissions. To access information in the Exceptions subsystem, you need permissions for the Exception feature on the Feature Access page.

The examples in the following table show what information a user can access based on their permission settings:

Read permission assigned for the Exceptions feature?	Exceptions permission assigned for splits/skills, trunk groups, ACDs, vectors, and VDNs?	Available exception information
Yes	Yes	• Exception reports • Messages in the Real-Time Exception Log • Real-time notification of exceptions

Table continues...

Read permission assigned for the Exceptions feature?	Exceptions permission assigned for splits/skills, trunk groups, ACDs, vectors, and VDNs?	Available exception information
Yes	No	Exceptions reports
No	Yes	Real-time notification of exceptions
No	No	No exception features are available

Other permissions

- To set up or change the method used to check for exceptions, you need the Write permission for the Exceptions feature.
- To be notified of a malicious call exception, you need the Exceptions permission for the appropriate call center entity.

About administering exception notification using the PC Client

An exception notification is a beep that is sounded by the CMS Supervisor PC Client when an exception is encountered. By default, this occurs when the user who is currently logged in to CMS Supervisor has the “exceptions” permission for the entity on which the exception occurred. If you do not want CMS Supervisor to beep when an exception occurs, you can turn off notifications.

Note:

Exception notification administration is available only using the PC Client.

Changing exception notification using the PC Client

Procedure

1. From the Controller window, select **Tools > Options**.
Supervisor displays the Options window.
2. Select the **General** tab.
3. Perform one of the following actions:
 - To activate exception notification, select the **Use Sound** option.
 - To turn off exception notification, deselect the **Use Sound** option.
4. Select **OK**.

Agent exceptions

You can configure exceptions for various agent activities. For example, exceptions can occur if there are too many calls in the queue or if the agent spends too long in an idle state. Agent exceptions are assigned based on splits/skills. When activating an exception, you can configure time limits and thresholds.

Considerations for administering agent exceptions

Consider the following when working with agent exceptions:

- Agent exceptions are assigned per split/skill and not for each agent. When an agent logs into a split/skill, any exceptions that are configured for that split/skill are applied to the agent.
- External outbound exceptions are a subset of outbound exceptions. If both types of exceptions are administered, the limit for external outbound covers external outbound calls and the limit for outbound covers only internal outbound calls.
- Agent exception records are not created by default in the CMS database when the split/skill is created. When adding an agent exception entry, you must manually associate the appropriate agent exceptions with a split/skill.

Permissions required to administer agent exceptions

Depending on the procedure that you want to perform, you need the following permissions:

- To view agent exceptions, the user ID used to log in to this Supervisor session requires “read” permission for the Exceptions subsystem and all affected splits/skills as well as the “exceptions” permission for the affected splits/skills.
- To add, delete, or modify agent exceptions, the user ID used to log in to this Supervisor session requires “write” permission for the Exceptions subsystem and all affected splits/skills as well as the “exceptions” permission for the affected splits/skills.

Administering agent exceptions in the Web Client

About this task

All available exception types are listed. You can manage which exception types are assigned and modify the settings for each exception type.

Procedure

1. Navigate to one of the following agent exception menus:
 - **Administration > Exceptions > Agent Exceptions**
 - **Administration > Exceptions > Agent Exceptions Reason Codes 0-49**
 - **Administration > Exceptions > Agent Exceptions Reason Codes 50-99**
2. In the **Current ACD** list, select the active ACD for which you want to administer exceptions.

3. In the **Split/Skill** field, select the split/skill for which you want to manage exceptions.

If exceptions are assigned, they are displayed.

4. **(Optional)** If you want to assign the same exceptions to additional splits/skills, enter the split/skill names or IDs in the **Select additional splits/skills (optional)** field.

Use a semicolon to separate each entry.

5. Click **+** to move splits/skills from the Search Results area to the Selected Split(s)/Skills(s) area.

Ensure that all splits/skills to which you want to assign exceptions are displayed in the Selected Split(s)/Skills(s) area.

6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. Do one of the following to save your changes:
 - Click **Add** when assigning a new set of exceptions.
 - Click **Modify** when modifying settings, such as the time limit or threshold, for an existing set of exceptions.
 - Click **Remove** to remove all administered exceptions.

Adding agent exceptions using the PC Client

About this task

Use this procedure when adding a new set of exceptions.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD for the split/skill where agent exceptions are to be created.
3. In the **Operations** list, highlight **Agent Exceptions**.

 Note:

If you need to add agent exceptions for AUX reason codes 10 through 99, select the appropriate operation for **Agent Exceptions Reason Codes 0-49** and **Agent Exceptions Reason Codes 50-99**.

4. Click **OK**.

Supervisor displays the Agent Exceptions Administration window.

This window appears with all fields blank when first opened.

5. In the **Split(s)/Skill(s)** field, enter the name or number of the split/skill for which an agent exceptions configuration is to be created.

The **Split(s)/Skill(s)** field can accept multiple entries. Each entry must be separated by a semicolon (;).

6. Do the following for each exception type you want to assign or modify:

- a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
- b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
- c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.

7. When all necessary time limits and thresholds have been entered, select **Actions > Add** from the menu bar.

Modifying agent exceptions using the PC Client

About this task

Use this procedure to modify the settings of exceptions that are already assigned. For example, you can modify the time limit or threshold.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD on which the split/skill to modify for agent exceptions resides.
3. In the **Operations** list, highlight **Agent Exceptions**.

 Note:

If you need to add agent exceptions for AUX reason codes 10 through 99, select the appropriate operation for **Agent Exceptions Reason Codes 0-49** and **Agent Exceptions Reason Codes 50-99**.

4. Click **OK**.

Supervisor displays the Agent Exceptions Administration window.

This window appears with all fields blank when first opened.

5. In the **Split(s)/Skill(s)** field, enter the name or number of the split/skill for which the agent exceptions configuration is to be modified.

6. From the menu bar, select **Actions > Find one**.

Supervisor locates the agent exception configuration for the specified split/skill and displays the data in the appropriate fields. If the exception configuration data cannot be found, the status bar displays `0 matches found`.

To return all splits/skills, leave the **Split(s)/Skill(s)** field blank before performing the **Find one** action. Supervisor will return all split(s)/skill(s) for which you have the “read” permission. You can then use the **Next** and **Previous** menu actions to cycle through the splits/skills.

7. Do the following for each exception type you want to assign or modify:

- a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
- b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
- c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.

8. When all necessary time limits and thresholds have been modified, select **Actions > Modify** from the menu bar.

Deleting agent exceptions using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD on which the split/skill to delete resides.

3. In the **Operations** list, highlight **Agent Exceptions**.

 Note:

If you need to add agent exceptions for AUX reason codes 10 through 99, select the appropriate operation for **Agent Exceptions Reason Codes 0-49** and **Agent Exceptions Reason Codes 50-99**.

4. Click **OK**.

Supervisor displays the Agent Exceptions Administration window.

5. In the **Split(s)/Skill(s)** field, enter the name or number of the split/skill for which an agent exceptions configuration is to be deleted.

6. From the menu bar, select **Actions > Find one**.

Supervisor locates the agent exception configuration for the specified split/skill and displays the data in the appropriate fields. If exception configuration data cannot be found, the status bar displays *0 matches found*.

To return all splits/skills, leave the **Split(s)/Skill(s)** field blank before performing the **Find one** action. Supervisor will return all splits/skills for which you have the Read permission. You can then use the **Next** and **Previous** menu actions to cycle through the splits/skills.

7. From the menu bar, select **Actions > Delete**.

Supervisor deletes the agent exception configuration for this split/skill from the CMS database and displays a *Successful* message in the status bar.

Agent exception descriptions

The following table describes the available agent exceptions:

Exception type	Description
Time available	The time that an agent spends in the Available state. This is idle time. Note that all time limits are defined in seconds.
Time on inbound ACD call (min)	The minimum time an agent spends on an ACD call.
Time on inbound ACD call (max)	The maximum time an agent can spend on an ACD call.
Time in after call work	The maximum time an agent can spend in the ACW state.
Time on inbound ACW call	The maximum time an agent can spend on an inbound call during ACW.
Number of inbound ACW calls/agent	The total number of inbound calls an agent can receive during ACW time. This exception can only be triggered once per interval.
Time on outbound ACW call	The maximum time an agent can spend on an outbound call during ACW.
Number of outbound ACW calls/agent	The total number of outbound calls an agent can make during ACW. This exception can only be triggered once per interval.

Table continues...

Exception type	Description
Time in AUX work	The maximum time an agent can spend in the AUX state. AUX refers to the auxiliary time during which agents are not available to take calls.
Time on inbound AUX call	The maximum time an agent can spend on an inbound call while in the AUX state.
Number of inbound AUX calls/agent	The total number of inbound calls an agent can receive while in the AUX state. This exception can only be triggered once per interval.
Time on outbound AUX call	The maximum time an agent can spend on an outbound call while in the AUX state.
Number of outbound AUX calls/agent	The total number of outbound calls an agent can make while in the AUX state. This exception can only be triggered once per interval.
Time in AUX with Reason Code X	The maximum time an agent can spend in the AUX state with Reason Code X, where X is a value from 0 to 99. You can set the time limit for each reason code. On the main Agent Exceptions page, this exception type is listed for Reason Codes 0 to 9. To define this exception type for more reason codes, use the separate page for reason codes 0 to 49 or the page for codes 50 to 99. The separate pages for reason codes do not contain any other agent exception types.
Login identification	Activate this exception to receive notifications for login violations. A violation occurs when an agent attempts to log in with an ID that is not in the Dictionary or if an agent tries to log in with more than one ID on the same terminal. If you deactivate this exception, you are not notified if an agent logs in with an ID that is not in the Dictionary, but you still are notified if an agent tries to log in with more than one ID.
Time on outbound ACD call (min)	The minimum time an agent spends on an outbound ACD call.
Time on outbound ACD call (max)	The maximum time an agent can spend on an outbound ACD call.
Number calls transferred	The maximum number of calls an agent can transfer.
Time ACD call spent on hold	The maximum time that an ACD call can be on hold. This time value is cumulative for each call. If an agent removes a call from hold and places it back on hold again, this value is not reset.
Number ACD calls placed on hold	The maximum number of ACD calls that an agent can put on hold. This exception can only be triggered once per interval.
Number ACD calls abandoned while on hold	The maximum number of calls that are abandoned after being put on hold by an agent. This exception can only be triggered once per interval.

Table continues...

Exception type	Description
Time ACD call spends ringing	The maximum time that a split/skill or direct agent ACD call can ring at the agent's voice terminal before an exception is triggered.
Ringing call automatically redirected from agent	Activate this exception to be notified when an ACD call rings for long enough that it is automatically redirected. To use this exception, Redirection on No Answer (RONA) must be enabled on the ACD.
Time on direct agent call	The maximum time that an agent can spend on a direct agent ACD call.
Number calls in direct agent queue	The maximum number of direct agent ACD calls an agent can have waiting in the queue.
Time call waited in direct agent queue	The maximum time that a call can wait in the direct agent queue.
Number calls abandoned from direct agent queue	The maximum number of direct agent ACD calls that can be abandoned before an exception is triggered. Calls are considered abandoned if they are in the queue for too long. This exception can only be triggered once per interval.
Number calls outflowed from direct agent queue (maximum)	The maximum number of direct agent calls that outflow from the direct agent queue. This exception can only be triggered once per interval.
Time on external outbound ACW call	The maximum time an agent can spend on an external outbound call during ACW.
Number external outbound ACW calls/agent	The maximum number of external outbound calls an agent can make while in the ACW state. This exception can only be triggered once per interval.
Time on external outbound AUX call	The maximum time an agent can spend on an external outbound call while in the AUX state.
Number external outbound AUX calls/agent	The maximum number of external outbound calls that an agent can make while in the AUX state. This exception can only be triggered once per interval.
Agent logged out with active/held calls	Activate this exception to be notified when an agent logs out with active or held calls on the voice terminal.
Logout attempt without valid reason code	The acceptable number of times that an agent can enter an invalid reason code when trying to log out. This exception can only be triggered once per interval.
AUX attempt without valid reason code	The acceptable number of times that an agent can enter an invalid AUX reason code. This exception can only be triggered once per interval.
Agent entered invalid call work code	An exception that is pegged for CWC 0, which occurs when an agent enters a call work code that is not configured. This exception should be turned off if you are collecting call work codes in call records only.

Split/skill exceptions

Split/skill exceptions can help you identify the splits and skills that need to be adjusted to achieve more efficiency in the call center. These exceptions are useful for identifying the following types of problems:

- The length of time that calls wait for different handling options.
- The number of calls that are directed through different handling options.
- The average speed with which the calls are being answered.

Considerations for split/skill exceptions

Consider the following when working with split and skill exceptions:

- To administer exceptions for skills, the EAS feature must be enabled. However, this feature is not required for split exceptions.
- When a split/skill is created, exceptions are configured by default in the CMS database. You must add the required exceptions for each split/skill.

Permissions required to administer split/skill exceptions

Depending on the procedure that you want to perform, you need the following permissions:

- To view split/skill exceptions, the user ID used to log in to this Supervisor session requires read permission for the Exceptions subsystem and all affected split/skills as well as the exceptions permission for all affected split/skill.
- To add, delete, or modify split/skill exceptions, the user ID used to log in to this Supervisor session requires write permission for the Exceptions subsystem and all affected split/skill as well as the exceptions permission for all affected split/skill.

Administering split/skill exceptions in the Web Client

About this task

All available exception types are listed. You can manage which exception types are assigned and modify the settings for each exception type.

Procedure

1. Navigate to **Administration > Exceptions > Split/Skill Exceptions**.
2. In the **Current ACD** list, select the active ACD for which you want to administer exceptions.
3. In the **Split/Skill** field, select the split/skill for which you want to manage exceptions.

If exceptions are assigned, they are displayed.

4. **(Optional)** If you want to assign the same exceptions to additional splits/skills, enter the split/skill names or IDs in the **Select additional splits/skills (optional)** field.

Use a semicolon to separate each entry.

5. Click **+** to move splits/skills from the Search Results area to the Selected Split(s)/Skills(s) area.

Ensure that all splits/skills to which you want to assign exceptions are displayed in the Selected Split(s)/Skills(s) area.

6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. Do one of the following to save your changes:
 - Click **Add** when assigning a new set of exceptions.
 - Click **Modify** when modifying settings, such as the time limit or threshold, for an existing set of exceptions.
 - Click **Remove** to remove all administered exceptions.

Adding split/skill exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the splits/skills for which you want to configure exceptions.
3. In the **Operations** list, select **Split/Skill Exceptions**.
4. Click **OK**.
Supervisor displays the Split/Skill Exception Administration window.
5. In the **Split(s)/Skill(s)** field, enter the names or IDs of the splits/skills for which an exceptions configuration is to be created.
6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.

- b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. When all necessary time limits and thresholds have been entered, click **Actions > Add** from the menu bar.

Modifying split/skill exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the splits/skills for which you want to modify exceptions.
3. In the **Operations** list, select **Split/Skill Exceptions**.
4. Click **OK**.
Supervisor displays the Split/Skill Exception Administration window.
5. In the **Split(s)/Skill(s)** field, enter the names or IDs of the splits/skills for which you want to modify exceptions.
6. From the menu bar, click **Actions > Find one**.
Supervisor locates the exception configuration for the specified split/skill and the displays the data in the appropriate fields.
To have all splits/skills returned in this step, leave the **Split(s)/Skill(s)** field blank before performing the **Find one** action. Supervisor will return all split(s)/skill(s) for which you have the “read” permission. You can then use the **Next** and **Previous** menu actions to cycle through the splits/skills.
7. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.

- c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
8. When all necessary time limits and thresholds have been entered, click **Actions > Modify** from the menu bar.

Deleting split/skill exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the split/skill exception configuration.
3. In the **Operations** list, select **Split/Skill Exceptions**.
4. Click **OK**.

Supervisor displays the Split/Skill Exception Administration window.

5. In the **Split(s)/Skill(s)** field, enter the names or IDs of the splits/skills for which the exception configuration is to be deleted.
6. From the menu bar, click **Actions > Find one**.

Supervisor locates the exception configuration for the specified split/skill and the displays the data in the appropriate fields.

To have all splits/skills returned in this step, leave the **Split(s)/Skill(s)** field blank before performing the **Find one** action. Supervisor will return all split(s)/skill(s) for which you have the “read” permission. You can then use the **Next** and **Previous** menu actions to cycle through the splits/skills.

7. From the menu bar, click **Actions > Delete**.

Supervisor deletes the exception configuration from the CMS database.

Split/skill exception descriptions

The following table describes the available split/skill exceptions:

Exception type	Description
Time call has waited in queue	The acceptable amount of time that a call can remain unanswered in the queue before an occurrence is counted against the threshold limit.
Number calls waiting	The maximum number of calls that can be in the queue at any given time.
Number calls abandoned	The acceptable number of abandoned calls. This exception can only be triggered once per interval.

Table continues...

Exception type	Description
Average speed of answer (seconds)	The maximum time in seconds that a call waits in the split/skill queue before an agent answers. This exception can only be triggered once per interval.
Number intraflowed-out calls	The maximum number of calls that can intraflow from a split/skill. This exception can only be triggered once per interval.
Number intraflowed-in calls	The acceptable number of calls that can intraflow into a split/skill before an occurrence is counted against the threshold limit. This exception can only be triggered once per interval.
Number interflowed-out calls	The acceptable number of calls that can interflow out of the split/skill. This exception can only be triggered once per interval.
Number calls handled as backup	The acceptable number of calls that the current split/skill can handle as a backup for another split/skill. This exception can only be triggered once per interval.
Number calls transferred	The acceptable number of calls that can be transferred. This exception can only be triggered once per interval.
Number calls offered while queue full	The acceptable number of calls offered or routed to the split/skill while the queue is full. This exception can only be triggered once per interval.
Expected Wait Time (pri Top) exceeds threshold	The maximum acceptable time in seconds that a call is expected to wait at top priority before connecting to an agent. This exception can only be triggered once per interval.
Expected Wait Time (pri High) exceeds threshold	The maximum acceptable time in seconds that a call is expected to wait at high priority before connecting to an agent. This exception can only be triggered once per interval.
Expected Wait Time (pri Medium) exceeds threshold	The maximum acceptable time in seconds that a call is expected to wait at medium priority before connecting to an agent. This exception can only be triggered once per interval.
Expected Wait Time (pri Low)	The maximum acceptable time in seconds that a call is expected to wait at low priority before connecting to an agent. This exception can only be triggered once per interval.
Rolling Average Speed of Answer (seconds)	The maximum acceptable amount of time in seconds that is calculated for the rolling Average Speed of Answer (ASA) for a split/skill. Rolling ASA refers to the average time that it takes for a call to be answered. This exception can only be triggered once per interval. An occurrence is counted (in seconds) when CMS receives an ASA that exceeds the specified time limit. An exception is triggered when the threshold is exceeded.

Trunk group exceptions

Trunk group exceptions are used to identify performance and capacity issues for the trunk groups in the call center.

 Note:

An Audio Difficulty exception is associated with each trunk group. This exception is provided for all ACD systems that support event counts and it cannot be disabled. For this reason, this exception is not available on the Trunk Group Exceptions page.

Permissions required to administer trunk group exceptions

Depending on the procedure that you want to perform, you need the following permissions:

- To view trunk group exceptions, the user ID used to log in to this Supervisor session requires “read” permission for the Exceptions subsystem and all affected trunk groups as well as the “exceptions” permission for all affected trunk groups.
- To add, delete, or change trunk group exceptions, the user ID used to log in to this Supervisor session requires “write” permission for the Exceptions subsystem and all affected trunk groups as well as the “exceptions” permission for all affected trunk groups.

Administering trunk group exceptions in the Web Client

About this task

All available exception types are listed. You can manage which exception types are assigned and modify the settings for each exception type.

Procedure

1. Navigate to **Administration > Exceptions > Trunk Group Exceptions**.
2. In the **Current ACD** list, select the active ACD for which you want to administer exceptions.
3. In the **Trunk Groups** field, enter the name or ID of the trunk group for which you want to manage exceptions.

If exceptions are assigned, they are displayed.

4. **(Optional)** If you want to assign the same exceptions to additional trunk groups, enter the trunk group names or IDs in the **Select additional trunk groups (optional)** field.

Use a semicolon to separate each entry.

5. Click **+** to move trunk groups from the Search Results area to the Selected Trunk Group(s) area.

Ensure that all trunk groups to which you want to assign exceptions are displayed in the Selected Trunk Group(s) area.

6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.

- b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. Do one of the following to save your changes:
 - Click **Add** when assigning a new set of exceptions.
 - Click **Modify** when modifying settings, such as the time limit or threshold, for an existing set of exceptions.
 - Click **Remove** to remove all administered exceptions.

Adding trunk group exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD for the trunk group that will receive the new exceptions configuration.
3. In the **Operations** list, select **Trunk Group Exceptions**.
4. Click **OK**.
Supervisor displays the Trunk Group Exception Administration window.
5. In the **Trunk Groups** field, enter the names or IDs of the trunk groups for which an exceptions configuration is to be created.
6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. When all necessary time limits and thresholds have been entered, click **Actions > Add** from the menu bar.

Modifying trunk group exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the trunk group and its exception configuration.
3. In the **Operations** list, select **Trunk Group Exceptions**.
4. Click **OK**.

Supervisor displays the Trunk Group Exception Administration window.

5. In the **Trunk Groups** field, enter the names or IDs of the trunk groups for which you want to modify exceptions.
6. From the menu bar, click **Actions > Find one**.

Supervisor locates the exception configuration data for the specified trunk group and displays it in the appropriate fields.

To return all trunk groups, leave the **Trunk Groups** field blank before performing the **Find one** action. Supervisor will return all trunk groups for which you have the Read permission. You can then use the **Next** and **Previous** menu actions to cycle through the trunk groups.

7. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
8. When all necessary time limits and thresholds have been entered, click **Actions > Modify** from the menu bar.

Deleting trunk group exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the trunk group and its exception configuration.
3. In the **Operations** list, select **Trunk Group Exceptions**.
4. Click **OK**.
- Supervisor displays the Trunk Group Exception Administration window.
5. In the **Trunk Groups** field, enter the names or IDs of the trunk groups for which the exception configuration is to be deleted.
6. From the menu bar, click **Actions > Find one**.

The exception configuration is found for the specified trunk group and the data displays in the appropriate fields.

To return all trunk groups, leave the **VDNs** field blank before performing the **Find one** action. Supervisor will return all trunk groups for which you have the Read permission. You can then use the **Next** and **Previous** menu actions to cycle through the trunk groups.

7. From the menu bar, click **Actions > Delete**.

The exception configuration for this trunk group is deleted from the CMS database.

Trunk group exception descriptions

The following table describes the available exceptions for trunks within a trunk group:

Exception type	Description
Time trunk in use (min)	The minimum acceptable time in seconds for a trunk to be in use. This exception can only be triggered once per interval for the same trunk.
Time trunk in use (max)	The maximum acceptable time in seconds that a trunk can be in use. This exception can only be triggered once per interval for the same trunk.
Time any trunk maintenance busy	The maximum acceptable time in seconds that a trunk can be in the maintenance busy state.
Length of time all trunks busy	The maximum time in seconds that all trunks in the trunk group can be busy at once. This exception can only be triggered once per interval.
Number trunk failures in group	The maximum number of trunk failures that can occur in the trunk group. An exception occurs when the number of failures exceeds the threshold within the interval.
Number of trunks in use	The maximum number of trunks that can be in use at the same time. An exception occurs when number of trunks in use exceeds the threshold within the interval.
Number of trunks maintenance busy	The maximum number of trunks that can be in the maintenance busy state in the trunk group. An exception occurs when the number of trunks in this state exceeds the threshold within the interval.
Number of failures on a single trunk	The maximum number of failures that can occur in a single trunk. An exception occurs when the number of failures exceeds the threshold within the interval.

VDN exceptions

VDNs must be assigned to a vector on the ACD system. VDN exceptions can help you identify problems in the following areas:

- The amount of time that calls remain in the vector or connected to an agent.
- The number of calls that reach specific states, such as disconnected, busy, and abandoned.
- The number of calls that are routed in or out of the VDN.

Related links

[Administration of VDN assignments](#) on page 140

[Administration of VDN call profiles](#) on page 142

Considerations for administering VDN exceptions

Consider the following when working with VDN exceptions:

- To administer VDN exceptions, the Call Vectoring feature must be enabled.
- The “Time in Vector” exception type might include the time that a call spends in more than one vector.
- CMS starts monitoring for VDN exceptions when a call connects to the VDN and stops when the call is disconnected, sent to another VDN, sent to an external destination, or transferred. The call remains connected to the VDN if one of the following occurs:
 - The call is routed to another vector through a `go to vector` command.
 - The call is sent through a `route to` or `adjunct routing link` command to a non-VDN extension that is internal to the local ACD system.
- Some VDN exception types require specific vector routing commands. For example, to get exceptions for unsuccessful interflow attempts, the vector must have at least one `route to` command that routes calls to a vector on a remote ACD.

Permissions required to administer VDN exceptions

Depending on the procedure that you want to perform, you need the following permissions:

- To view VDN exceptions, the user ID used to log in to this Supervisor session requires “read” permission for the Exceptions subsystem and all affected VDNs as well as the “exceptions” permission for all affected VDNs.
- To add, delete, or change VDN exceptions, the user ID used to log in to this Supervisor session requires “write” permission for the Exceptions subsystem and all affected VDNs as well as the “exceptions” permissions for all affected VDNs.

Administering VDN exceptions in the Web Client

About this task

All available exception types are listed. You can manage which exception types are assigned and modify the settings for each exception type.

Procedure

1. Navigate to **Administration > Exceptions > VDN Exceptions**.
2. In the **Current ACD** list, select the active ACD for which you want to administer exceptions.
3. In the **VDNs** field, enter the name or ID of the VDN for which you want to manage exceptions.

If exceptions are assigned, they are displayed.

4. **(Optional)** If you want to assign the same exceptions to additional VDNs, enter the VDN names or IDs in the **Select additional VDNs (optional)** field.

Use a semicolon to separate each entry.

5. Click **+** to move VDNs from the Search Results area to the Selected VDN(s) area.

Ensure that all VDNs to which you want to assign exceptions are displayed in the Selected VDN(s) area.

6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. Do one of the following to save your changes:
 - Click **Add** when assigning a new set of exceptions.
 - Click **Modify** when modifying settings, such as the time limit or threshold, for an existing set of exceptions.
 - Click **Remove** to remove all administered exceptions.

Adding VDN exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the VDNs for which you want to configure exceptions.

3. In the **Operations** list, select **VDN Exceptions**.

4. Click **OK**.

Supervisor displays the VDN Exception Administration window.

5. In the **VDNs** field, enter the names or IDs of the VDNs for which the exceptions configuration is to be created.
6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. When all necessary time limits and thresholds have been entered, click **Actions > Add** from the menu bar.

Modifying VDN exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the VDNs for which you want to configure exceptions.
3. In the **Operations** list, select **VDNs**.
4. Click **OK**.

Supervisor displays the VDN Exception Administration window.

5. In the **VDNs** field, enter the names or IDs of the VDNs for which exception configuration is to be modified.
6. From the menu bar, click **Actions > Find one**.

Supervisor locates the exception configuration data for the specified VDN and displays it in the appropriate fields.

To have all VDNs returned in this step, leave the **VDNs** field blank. Supervisor will return all VDNs for which you have the “read” permission. You can then use the **Next** and **Previous** menu actions to cycle through the VDNs.

7. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
8. When all necessary time limits and thresholds have been entered, click **Actions > Modify** from the menu bar.

Deleting VDN exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the VDNs for which you want to configure exceptions.
3. In the **Operations** list, select **VDN Exceptions**.
4. Click **OK**.
Supervisor displays the VDN Exception Administration window.
5. In the **VDNs** field, enter the names or IDs of the VDNs for which the exception configuration is to be deleted.
6. From the menu bar, select **Actions > Find one**.
Supervisor locates the exception configuration for the specified VDN and the data displays in the appropriate fields.
To have all VDNs returned through this step, leave the **VDNs** field blank. Supervisor displays the total number of matches in the status bar. The VDNs can then be navigated by using the **Next** and **Previous** actions.
7. From the menu bar, click **Actions > Delete**.
Supervisor deletes the exception configuration from the CMS database.

VDN exception descriptions

The following table describes the available exceptions for calls to a VDN:

Exception type	Description
Time in vector (max)	The maximum acceptable time in seconds that a call can spend in vector processing. This exception can only be triggered once per interval.
Time at agent (min)	The minimum time in seconds that a VDN call is connected to an agent. This exception can only be triggered once per interval.
Time at agent (max)	The maximum time in seconds that a VDN call is connected to an agent. This exception can only be triggered once per interval.
Number calls abandoned while in vector	The maximum number of calls that can be abandoned while in the vector for processing. This exception can only be triggered once per interval.
Number calls forced busy	The maximum number of calls that receive a busy signal from the switch during an interval. This exception can only be triggered once per interval.
Number calls disconnected	The maximum number of calls that can be disconnected during vector processing. Disconnects can be caused by the disconnect vector command, by the vector disconnect timer, or because a call reached the end of vector processing without being queued. Calls that are disconnected after receiving a busy signal are not included. This exception can only be triggered once per interval.
Number calls in ACD split queue	The maximum number of calls in a split/skill queue.
Number calls that flowed into VDN	The maximum number of calls that can enter the VDN through vector routing command or a transfer from a local extension. This exception can only be triggered once per interval.
Number calls that flowed out of VDN	The maximum number of calls that can be routed from the current VDN to another VDN or external destination. This exception can only be triggered once per interval.
Number calls interflowed out of VDN	The maximum number of calls that can interflow to an external destination. This exception can only be triggered once per interval.
Number calls handled by backup split	The maximum number of calls that can be connected to a backup split/skill during an interval. A check backup split , check backup skill , messaging split , or messaging skill vector command causes a call to be handled by a backup split/skill. This exception can only be triggered once per interval.
Number unsuccessful look ahead interflow attempts	The maximum number of calls that fail to interflow to another ACD system during an interval. This exception can only be triggered once per interval.
Number unsuccessful adjunct routing attempts	The maximum number of failed attempts to connect a call to an adjunct host computer during an interval. The failure can occur because the connection to the adjunct is out of service or busy, or because the adjunct software rejects control. This exception can only be triggered once per interval.

Table continues...

Exception type	Description
Rolling Average Speed of Answer (seconds)	The maximum amount of time in seconds that is calculated for the rolling ASA for a VDN. This exception can only be triggered once per interval. An occurrence is counted when CMS receives an ASA that exceeds the specified time limit. An exception is triggered when the threshold is exceeded.

Vector exceptions

Vector exception tracking starts when a call enters the vector and continues until the call connects to an agent, is abandoned, or is routed to another destination. Vector exceptions can help you identify problems in the following areas:

- The amount of time that a call waits in a vector.
- The number of calls that are abandoned, disconnected, or receive a forced busy signal while in the vector.
- Routing failures.

Considerations for administering vector exceptions

Consider the following when working with vector exceptions:

- Calls might generate exceptions even after the vector has given routing control to the adjunct.
- Some exception types require specific vector routing commands. For example, to get exceptions for unsuccessful interflow attempts, the vector must have at least one **route to** command that routes calls to a remote ACD.

Permissions required to administer vector exceptions

Depending on the procedure that you want to perform, you need the following permissions:

- To view vector exceptions, the user ID used to log in to this Supervisor session requires “read” permission for the Exceptions subsystem and all affected vectors as well as the “exceptions” permission for the affected vectors.
- To add, delete, or change vector exceptions, the user ID used to log in to this Supervisor session requires “write” permission for the Exceptions subsystem and all affected vectors as well as the “exceptions” permission for the affected vectors.

Administering vector exceptions in the Web Client

About this task

All available exception types are listed. You can manage which exception types are assigned and modify the settings for each exception type.

Procedure

1. Navigate to **Administration > Exceptions > Vector Exceptions**.
2. In the **Current ACD** list, select the active ACD for which you want to administer exceptions.
3. In the **Vectors** field, enter the name or ID of the vector for which you want to manage exceptions.

If exceptions are assigned, they are displayed.

4. **(Optional)** If you want to assign the same exceptions to additional vectors, enter the vector names or IDs in the **Select additional vectors (optional)** field.

Use a semicolon to separate each entry.

5. Click **+** to move vectors from the Search Results area to the Selected Vector(s) area.

Ensure that all vectors to which you want to assign exceptions are displayed in the Selected Vector(s) area.

6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. Do one of the following to save your changes:
 - Click **Add** when assigning a new set of exceptions.
 - Click **Modify** when modifying settings, such as the time limit or threshold, for an existing set of exceptions.
 - Click **Remove** to remove all administered exceptions.

Adding vector exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the vectors for which you want to configure exceptions.

3. In the **Operations** list, select **Vector Exceptions**.

4. Click **OK**.

Supervisor displays the Vector Exceptions Administration window.

5. In the **Vectors** field, enter the names or IDs of the vectors for which an exceptions configuration is to be created.
6. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
7. When all necessary time limits and thresholds have been entered, click **Actions > Add** from the menu bar.

Modifying vector exceptions in the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the vectors for which you want to configure exceptions.
3. In the **Operations** list, select **Vector Exceptions**.
4. Click **OK**.

Supervisor displays the Vector Exceptions Administration window.

5. In the **Vectors** field, enter the names or IDs of the vectors for which the exception configuration is to be modified.
6. From the menu bar, click **Actions > Find one**.

Supervisor locates the agent exception configuration for the specified split/skill and displays the data in the appropriate fields.

To have all vectors returned when performing this step, leave the **Vectors** field blank. Supervisor will return all vectors for which you have the “read” permission. You can then use the **Next** and **Previous** menu actions to cycle through the vectors.

7. Do the following for each exception type you want to assign or modify:
 - a. Select the **Active** check box to activate the exception type. When activated, CMS tracks activities for the exception. If the check box is not selected, the exception type is disabled, but if you enter a time limit and threshold, this information is saved so you can activate the exception later.
 - b. In the **Time Limit** field, enter a time limit in seconds. You can enter a value from 0 to 28800 seconds. Depending on the type of exception, this value represents the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field.
 - c. In the **Threshold** field, enter a value from 0 to 999. This value represents the number of acceptable occurrences for an activity. If you enter 0 in this field, an exception is created the first time the activity occurs.
8. When all necessary time limits and thresholds have been entered, click **Actions > Modify** from the menu bar.

Deleting vector exceptions using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the vector and its exception configuration.
3. In the **Operations** list, highlight **Vector Exceptions**.
4. Click **OK**.
Supervisor displays the Vector Exceptions Administration window.
5. In the **Vectors** field, enter the name or number of the vector for which the exception configuration is to be deleted.
6. From the menu bar, select **Actions > Find one**.
Supervisor locates the agent exception configuration for the specified split/skill and displays the data in the appropriate fields. If the exception configuration data cannot be found, the status bar displays `0 matches found`.

To have all vectors returned in this step, leave **Vectors** field blank before performing the **Find one** action. Supervisor will return all vectors for which you have the “read” permission. You can then use the **Next** and **Previous** menu actions to cycle through the vectors.
7. From the menu bar, select **Actions > Delete**.
Supervisor deletes the exception configuration for this vector from the database and displays a `Successful` message in the status bar.

Vector exception definitions

The following table describes the available exceptions for calls in vector processing:

Name	Description
Time in vector (max)	The maximum acceptable time in seconds that a call can spend in vector processing. This exception can only be triggered once per interval.
Number calls abandoned while in vector	The maximum number of calls that can be abandoned while in the vector for processing. This exception can only be triggered once per interval.
Number calls forced busy	The maximum number of calls that can receive a forced busy signal from the vector during an interval. This exception can only be triggered once per interval.
Number calls disconnected	The maximum number of calls that can be disconnected during vector processing. Disconnects can be caused by the <code>disconnect</code> vector command, by the vector disconnect timer, or because a call reached the end of vector processing without being queued. This exception can only be triggered once per interval.
Number calls in ACD split queue	The maximum number of vector calls that can be in a split/skill queue.
Number unsuccessful look ahead interflow attempts	The maximum number of vector calls that fail to interflow to another ACD system during an interval. The <code>route-to</code> vector command causes a call to interflow. This exception can only be triggered once per interval.
Number unsuccessful adjunct routing attempts	The maximum number of failed attempts for a vector call to connect to an adjunct host computer during an interval. This exception can only be triggered once per interval..

Supervisor sends a malicious call trace report to the specified output method.

Real-time exceptions log

You can view a real-time exceptions log, which shows all types of exceptions for which you have the Exceptions permission. The log lists the last ten exceptions that occurred.

Each exception record in the log includes the following information:

- The date and time that the exception occurred.
- The name of the ACD for which the exception occurred.
- The ACD element, such as the specific agent, split/skill, or VDN involved in the exception.

Considerations for the real-time exceptions log

Consider the following information when viewing the real-time exceptions log:

- When you first view the log, the oldest exception is displayed first. As long as the page remains open, the log automatically scrolls to display each new exception record.
- If you defined element names in the Dictionary, the log displays these names. The names are truncated if they are too long for the exception record.
- For a peg count exception, the exception record shows the occurrence threshold you set even if the actual number of occurrences is higher. For a timed exception, the exception record shows the time limit you set, not the actual duration of the occurrence.
- The real-time exception log can hold a maximum of 100 records. If a new exception occurs when the log is full, the oldest exception is deleted so the new exception can be recorded.

Viewing the real-time exceptions log using the Web Client

Procedure

Navigate to **Administration > Exceptions > Real-Time Exception Log**.

CMS Supervisor displays the list of the ten most recent exceptions that have occurred on the system.

Viewing the real-time exceptions log using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD for which exceptions will be shown.
3. In the **Operations** list, highlight **Real-Time Exception Log**.
4. Click **OK**.

Supervisor displays the Real-time Exception Log window.

Chapter 9: Managing tenant access

To use CMS tenancy, ensure that the Tenancy feature package is enabled. With tenancy, you can partition a subset of ACD resources and assign these resources to tenants. The call center resources assigned to one tenant partition are isolated from the resources in the other tenant partitions. Therefore, different tenants on an ACD do not share agents, call work codes, split/skills, trunk groups, VDNs, and vectors. Some call center resources can be assigned across all tenants.

Users that are created as tenant users have tenant-level access only. Each tenant user has access to a restricted set of call center resources and data based on their tenant assignment. A tenant user can be granted access to more than one tenant. Note that a tenant user can create custom reports or design reports that only they can access.

ACD administration impact

The CMS and ACD tenancy features are not directly related. However, the ACD configuration controls how calls are handled and delivered to agents. Therefore, ACD administration impacts the data in CMS tenant reports. For example, agent 1 and skill 1 are assigned to CMS tenant 1. Agent 2 and skill 2 are assigned to CMS tenant 2. If agent 1 logs in to skill 2 and receives calls for skill 2, the tenant 1 users will see the skill 2 call data in reports run for agent 1. Even though the tenant user is restricted to running reports for agents assigned to tenant 1, CMS will display all the call data for agent 1. This means that the tenant user will see call data for skills assigned to a different tenant. CMS must display all the data for an agent or the summary data will be incomplete. Therefore, you must carefully plan tenant administration on both the ACD and CMS prior to implementation.

Tenancy examples

The following are examples of situations where the tenancy feature is useful:

- Service providers can partition their ACDs so CMS can be used by multiple tenants or customers within the same ACD, but without access to each other's data.
- A call center with multiple business units that have separate independent functions can create tenants to allocate a different set of tenant partitions to each business unit.
- Call centers with a hierarchical reporting structure can use tenancy to enable supervisors and report users to manage only a subset of call center resources.

Prerequisite tasks for tenancy administration

Before using this chapter to manage tenant assignments, you must enable the Tenancy feature and set up tenants.

CMS server commands for enabling tenancy

- Ensure that you can log in to the CMS server with root privileges.
- Use the `cms svc` command to authorize the Tenancy feature.
- Use the `cms adm` command to install the Tenancy feature package.

Tenant management in the Dictionary

Use the CMS Supervisor Dictionary to add and manage tenants. When adding a tenant, define a tenant number, name, and description.

Tenant access

From CMS Supervisor, navigate to **User Permissions > Tenant Access** to grant tenant access to users. Specify which tenants each user can access and grant them “Read”, “Write”, or “Exceptions” permissions.

Tenant user access restrictions

User access restrictions affect what tenant users can access based on the tenants for which they have permission. Review the following tenant user access restrictions:

- Special Agent/Agent Group restriction: Tenant users can only access tenant-specific agents and agent groups for which they have permissions.
- Special Call Work Code (CWC) restriction: Tenant users can only access the CWCs for which they have permissions.
- Reports restriction: The report data is restricted to only show ACD data for which the tenant user has permissions.
- Dictionary restriction: Tenant users cannot access Dictionary menu items and windows corresponding to agent groups and ACD groups. Tenant users can only access permissible tenant partitions for a single ACD.
- Call Center Administration restriction: Tenant users cannot access call center administration for vector content. Tenant user access to call center administration for ACD groups is filtered based on the permissions assigned.
- Tenant Administration restriction: Even if a tenant user is granted Write permission for the Tenancy feature, they cannot add, modify, or delete tenant assignments.
- User Permissions restriction: Tenant users cannot have Write access to the User Permissions feature. Tenant users cannot view permission information for other users. They can only view their own permission information.

As a tenant user, you can use the **Tenant Access Permissions** menu to access the following information:

- Your tenant access permissions.
- Your vector access permissions.
- Your ACD access permissions.
- Your trunk group access permissions.
- Your VDN access permissions.
- Your split/skill access permissions.
- Your tenant user data.
- Your feature access. For each feature, you see whether you have Read access, Write access, both, or neither.
- Your Main Menu Addition access, which shows the menu items for which you have access.

Working with tenant features in the Web Client

Adding agents to a tenant in the Web Client

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the list of agents administered for the selected tenant.

4. Click **Add Agent** to add agents to the tenant.
5. In the **Agents** field, enter agent extensions or IDs.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

6. Click **+** to move the agents you want to add from the Search Results area to the Selected Agents area.
7. Click **OK** to save your changes.

Removing an individual agent from a tenant in the Web Client

About this task

You can remove an agent from the list of agents administered for the tenant. Use this procedure to remove one agent or a few agents one at a time.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the list of agents administered for the selected tenant.

4. Click  next to the agent you want to remove.

The Confirm Delete dialog box is displayed.

5. Click **Yes** to complete the change.

Removing multiple agents from a tenant in the Web Client

About this task

Use this procedure to remove agents in bulk. Specify up to 32 agents and then remove them in one go.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the list of agents administered for the selected tenant.

4. Click **Remove Agent**.

5. In the **Agents** field, enter the extensions or IDs of existing agents.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

6. Click **+** to move the agents you want to remove from the Search Results area to the Selected Agents area.

7. Click **OK** to remove the specified agents.

Creating a tenant agent group in the Web Client

About this task

Use this procedure to add a new agent group to a tenant.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Groups**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. Click **Add Tenant Agent Group**.

4. In the **Tenants** list, select the tenant for which you want to add an agent group.
5. In the **Agent Group Name** field, enter a name for the new agent group.
The first character must be a letter. For the remaining characters, you can use a letter, number from 0 to 9, underscore, space, period, or comma.
6. Click **OK** to save your changes.

Adding agents to a tenant agent group in the Web Client

About this task

After creating an agent group, you must add agents to it.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Groups**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. Click  next to the agent group you want to modify.
4. On the Tenant Agent Groups: Content page, click **Add Tenant Agent**.
5. In the **Add Tenant Agent** field, enter agent names or IDs.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move agents from the Search Results area to the Selected Agents area.
The agents in the Selected Agents area will be added to the tenant agent group.
7. Click **OK** to save your changes.

Removing an individual agent from a tenant agent group in the Web Client

About this task

Use this procedure to remove an individual agent from an agent group or to remove a few agents one at a time.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Groups**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. Click  next to the agent group you want to modify.
4. Click  next to the agent you want to remove.
The Confirm Delete dialog box is displayed.
5. Click **Yes** to complete the change.

Removing multiple agents from a tenant agent group in the Web Client

About this task

Use this procedure to remove agents from a tenant agent group in bulk. Specify which agents no longer need to be in the agent group and then remove them.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Groups**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. Click  next to the agent group you want to modify.
4. On the Tenant Agent Groups: Content page, click **Remove Tenant Agent**.
5. In the **Remove Tenant Agent** field, enter the names or IDs of agents that are currently in the agent group but no longer need to be there.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move agents from the Search Results area to the Selected Agents area.

The agents in the Selected Agents area will be removed from the agent group.
7. Click **OK** to save your changes.

Copying a tenant agent group in the Web Client

About this task

Use this procedure to copy the contents from one tenant agent group to a new tenant agent group. Under the “to” heading, you can enter a name for the new agent group. The new agent group is created in the same tenant and it contains the same content as the agent group you copied from.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Groups**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. Click  next to the agent group you want to copy.

The Copy Tenant Agent Group window displays the tenant number and the name of the agent group you are copying from. You cannot modify these fields.
4. In the **Agent Group Name** field under the “to” heading, enter a name for the new agent group.
5. Click **OK**.

The new agent group is created with the same content as the agent group you copied from.

Deleting a tenant agent group in the Web Client

About this task

You can delete a tenant agent group that you no longer need. If the agent group you are deleting has agents, consider adding those agent to another agent group. Alternatively, you can copy the tenant agent group before deleting it.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Agent Groups**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. Click  next to the agent group you want to delete.
The Confirm Delete dialog box is displayed.
4. Click **Yes** to finish deleting the tenant agent group.

Related links

[Adding agents to a tenant agent group in the Web Client](#) on page 250

[Copying a tenant agent group in the Web Client](#) on page 251

Adding call work codes to a tenant in the Web Client

About this task

Assign call work codes to a tenant. Tenant agents can use the available call work codes to track information associated with a call.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Call Work Code Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the call work codes administered for the selected tenant.
4. Click **Add Call Work Code**.
5. In the **Call Work Codes** field, enter call work code names or IDs.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move call work codes from the Search Results area to the Selected Call Work Codes area.
The call work codes in the Selected Call Work Codes area will be assigned to the tenant.
7. Click **OK** to save your changes.

Related links

[Call work code administration](#) on page 126

Removing an individual call work code from a tenant in the Web Client

About this task

If a call work code is no longer required for a tenant, remove it. Use this procedure to remove one call work code at a time.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Call Work Code Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the call work codes administered for the selected tenant.
4. Click  next to the call work code you want to remove.
The Confirm Delete dialog box is displayed.
5. Click **Yes** to complete the change.

Removing multiple call work codes from a tenant in the Web Client

About this task

You can remove call work codes assigned to a tenant in bulk. Specify which call work codes are no longer required and remove them in one go.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Call Work Code Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the call work codes administered for the selected tenant.
4. Click **Remove Call Work Code** to delete call work codes in bulk.
5. In the **Call Work Codes** field, enter the names or IDs of existing call work codes for the tenant.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

6. Click **+** to move call work codes from the Search Results area to the Selected Call Work Codes area.

The tenant call work codes in the Selected Call Work Codes area will be removed.

7. Click **OK** to save your changes.

Adding splits/skills to a tenant in the Web Client

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Split/Skill Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the splits/skills administered for the selected tenant.

4. Click **Add Split/Skill**.

5. In the **Splits/Skills** field, enter split/skill names or IDs.

To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.

6. Click **+** to move splits/skills from the Search Results area to the Selected Split(s)/Skills(s) area.

The splits/skills displayed in Selected Split(s)/Skills(s) area will be assigned to the tenant.

7. Click **OK** to save your changes.

Removing an individual split/skill from a tenant in the Web Client

About this task

You can remove an individual split/skill from the list of splits/skills assigned to a tenant.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Split/Skill Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the splits/skills administered for the selected tenant.

4. Click  next to the split/skill you want to remove.

The Confirm Delete dialog box is displayed.

5. Click **Yes** to complete the change.

Removing multiple splits/skills from a tenant in the Web Client

About this task

You can remove splits/skills assigned to a tenant in bulk. Specify which splits/skills are no longer required and remove them in one go.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Split/Skill Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the call work codes administered for the selected tenant.
4. Click **Remove Split/Skill** to remove splits/skills in bulk.
5. In the **Splits/Skills** field, enter the names or IDs of existing splits/skills that no longer need to be assigned to the tenant.
6. Click **+** to move splits/skills from the Search Results area to the Selected Split(s)/Skills(s) area.
The splits/skills in the Selected Split(s)/Skills(s) area will be assigned to the tenant.
7. Click **OK** to save your changes.

Adding trunk groups to a tenant in the Web Client

About this task

Use this procedure to assign trunk groups to a tenant.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Trunk Group Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the trunk groups administered for the selected tenant.
4. Click **Add Trunk Group**.
5. In the **Trunk Groups** field, enter trunk group names or IDs.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move trunk groups from the Search Results area to the Selected Trunk Group(s) area.
The trunk groups in the Selected Trunk Group(s) area will be assigned to the tenant.
7. Click **OK** to save your changes.

Related links

[About viewing trunk group assignments](#) on page 138

Removing an individual trunk group from a tenant in the Web Client

About this task

You can remove an individual trunk group from the list of trunk groups assigned to the tenant.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Trunk Group Assignment**.

2. In the **Current ACD** list, select the active ACD for the tenant.

3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the trunk groups administered for the selected tenant.

4. Click  next to the trunk group you want to remove.

The Confirm Delete dialog box is displayed.

5. Click **Yes** to complete the change.

Removing multiple trunk groups from a tenant in the Web Client

About this task

You can remove trunk groups assigned to a tenant in bulk. Specify which trunk groups are no longer required and remove them in one go.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Trunk Group Assignment**.

2. In the **Current ACD** list, select the active ACD for the tenant.

3. In the **Tenants** list, select the tenant you want to manage.

CMS Supervisor displays the trunk groups administered for the selected tenant.

4. Click **Remove Trunk Group** to remove trunk groups in bulk.

5. In the **Trunk Groups** field, enter the names or IDs of existing trunk groups that no longer need to be assigned to the tenant.

6. Click **+** to move trunk groups from the Search Results area to the Selected Trunk Group(s) area.

The trunk groups in the Selected Trunk Group(s) area will be removed.

7. Click **OK** to save your changes.

Adding VDNs to a tenant in the Web Client

About this task

A VDN is an extension number that enables incoming calls to be connected to a vector for processing. Use this procedure to assign VDNs to a tenant.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant VDN Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the VDNs administered for the selected tenant.
4. Click **Add VDNs**.
5. In the **VDNs** field, enter VDN names or IDs.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move VDNs from the Search Results area to the Selected VDN(s) area.
The VDNs in the Selected VDN(s) area will be assigned to the tenant.
7. Click **OK** to save your changes.

Removing an individual VDN from a tenant in the Web Client

About this task

You can remove a VDN that no longer needs to be assigned to a tenant. Use this procedure to remove one VDN at a time.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant VDN Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the VDNs administered for the selected tenant.
4. Click  next to the VDN you want to remove.
The Confirm Delete dialog box is displayed.
5. Click **Yes** to complete the change.

Removing multiple VDNs from a tenant in the Web Client

About this task

You can remove VDNs assigned to a tenant in bulk. Specify which VDNs are no longer required and remove them in one go.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant VDN Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the VDNs administered for the selected tenant.
4. Click **Remove VDNs**.
5. In the **VDNs** field enter the names or IDs of VDNs that no longer need to be assigned to the tenant.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move VDNs from the Search Results area to the Selected VDN(s) area.
The VDNs in the Selected VDN(s) area will be removed.
7. Click **OK** to save your changes.

Adding vectors to a tenant in the Web Client

About this task

Use this procedure to assign vectors to a tenant.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Vector Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the vectors administered for the selected tenant.
4. Click **Add Vectors**.
5. In the **Vectors** field, enter vector names or IDs.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move vectors from the Search Results area to the Selected Vector(s) area.
The vectors in the Selected Vector(s) area will be assigned to the tenant.
7. Click **OK** to save your changes.

Removing a vector from a tenant

About this task

You can remove a vector that no longer needs to be assigned to a tenant. Use this procedure to remove one vector at a time.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Vector Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the vectors administered for the selected tenant.
4. Click  next to the vector you want to remove.
The Confirm Delete dialog box is displayed.
5. Click **Yes** to complete the change.

Removing multiple vectors from a tenant in the Web Client

About this task

You can remove vectors assigned to a tenant in bulk. Specify which vectors are no longer required and remove them in one go.

Procedure

1. Navigate to **Administration > Tenant Administration > Tenant Vector Assignment**.
2. In the **Current ACD** list, select the active ACD for the tenant.
3. In the **Tenants** list, select the tenant you want to manage.
CMS Supervisor displays the vectors administered for the selected tenant.
4. Click **Remove Vectors**.
5. In the **Vectors** field, enter the names or IDs of vectors that no longer need to be assigned to the tenant.
To enter multiple values, separate each with a semicolon. The entries are displayed in the Search Results area.
6. Click **+** to move vectors from the Search Results area to the Selected Vector(s) area.
The vectors in the Selected Vector(s) area will be removed.
7. Click **OK** to save your changes.

PC Client tenant administration sub-menus

Using the PC Client, you can click **Commands > Tenant Administration** to navigate to the Tenant Admin sub menu window. The **Operations** tab in the Tenant Admin sub menu window include the following menu items:

- **Tenant Agent Assignment**
- **Tenant Agent Groups**
- **Tenant Call Work Code Assignment**
- **Tenant Split/Skill Assignment**
- **Tenant Trunk Group Assignment**
- **Tenant VDN Assignment**
- **Tenant Vector Assignment**

 Note:

Tenant login IDs have read access only to Tenant Agent, VDN, Vector, Trunk Group, CWC, and Split/skill assignments. Tenant users have read/write access to Tenant Agent Groups.

 Note:

You can use synonyms in the fields of all the tenant assignment screens.

Tenant Agent Assignment administrative operations

 Important:

- A tenant number has to be between 1 and 250.
- Agents can have up to 16 digits based on Communication Manager releases.

The PC Client Tenant Admin Agent Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated agent in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the agent belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number. When agents are removed from a tenant, the agents will also be automatically removed from agent groups pertaining to the tenant.

Table continues...

Field	Description
Find one	Finds an entry in the database that matches the tenant and agent fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number.
List all	Lists all tenant and agent entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Tenant Agent Groups administrative operations

Use the Tenant Admin Agent Groups Assignment window to build tenant specific agent groups. The tenant specific agent groups created using this window are different from the agent groups built using **Dictionary > Agent Groups**. The agent groups created using **Dictionary > Agent Groups** can contain any agents from the ACDs. The Tenant specific agent groups are limited to agents within a specific tenant partition. Tenant users can only access tenant agent groups pertaining to permissible tenants. Tenant users are not allowed to use the non-tenant specific agent groups.

Important:

- A tenant number has to be between 1 and 250.
- An agent group name must begin with an alphabetic character and can be up to 20 characters long.

The PC Client Tenant Admin Agent Groups Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated agent group in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the agent group belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number.

Table continues...

Field	Description
Find one	Finds an entry in the database that matches the tenant and agent group fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number.
List all	Lists all tenant and agent group entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.
Copy	Copies the contents of the specified tenant agent group to the new agent group. If an entry already exists, the system displays <i>Already exists</i> on the window status line. Use the Tenant Admin Agent Groups Assignment window to enter the agent group to copy from. The user must have write permission for the Tenant feature and write permission for the tenant number.
Get contents	Use this option to manipulate the contents of the agent group. Use the login ID field in this window to add, delete, or list agents for the tenant specific agent group.

Tenant Call Work Code Assignment administrative operations

Important:

- A tenant number has to be between 1 and 250.
- Each Call Work Code (CWC) can have up to 16 digits.

The PC Client Tenant Admin Call Work Code Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated CWC in the current user window to the database. If an entry already exists, the system displays <i>Already exists</i> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the CWC belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <i>Does not exist</i> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number.

Table continues...

Field	Description
Find one	Finds an entry in the database that matches the tenant and CWC fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number.
List all	Lists all tenant and CWC entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Tenant split/skill assignment

Important:

- A tenant number has to be between 1 and 250.
- Split/Skills numbers are between 1 and up to 8000 depending on Communication Manager releases.

The Tenant Admin Split/Skill Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated split/skill in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the split/skill belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Find one	Finds an entry in the database that matches the tenant and split/skill fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number.
List all	Lists all tenant and split/skill entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.

Table continues...

Field	Description
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Tenant Trunk Group Assignment administrative operations

! Important:

- A tenant number has to be between 1 and 250.
- Trunk Group numbers are between 1 and up to 2000 depending on Communication Manager releases.

The PC Client Tenant Admin Trunk Group Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated trunk group in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the trunk group belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Find one	Finds an entry in the database that matches the tenant and trunk group fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number.
List all	Lists all tenant and trunk group entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Tenant VDN Assignment administrative operations

! Important:

- A tenant number has to be between 1 and 250.
- VDNs can have up to 16 digits based on Communication Manager releases.

The PC Client Tenant Admin VDN Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated VDN in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the VDN belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Find one	Finds an entry in the database that matches the tenant and VDN fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number.
List all	Lists all tenant and VDN entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Tenant Vector Assignment administrative operations

Important:

- A tenant number must be between 1 and 250.
- Vector numbers are between 1 and 8000.

The PC Client Tenant Admin Vector Assignment window consists of an action list which is described in the following table:

Field	Description
Add	Adds the entry for a tenant and the associated vector in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line. The user must have write permission for the Tenant feature and write permission for the tenant number.
Delete	Removes the vector belonging to the tenant entry in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line. The user must have write permission for the Tenant feature and write permission for the tenant number.

Table continues...

Field	Description
Find one	Finds an entry in the database that matches the tenant and vector fields. The status line for the current window indicates the total number of matches found. The user must have read permission for the Tenant feature and read permission for the tenant number
List all	Lists all tenant and vector entries in the database that match with the values entered in the fields of the current user window. The user must have read permission for the Tenant feature and read permission for the tenant number.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

Chapter 10: Configuring CMS system settings

You can view and manage the CMS settings configured during initial installation. You can access many of these settings from the System Setup area in CMS Supervisor. You can perform tasks such as switching between single-user mode and multi-user mode, and managing the collection, storage, and retrieval of data. Changes to configuration settings can affect system performance, disk space usage, and data collection.

Switch setup data

Use the Switch Setup page to view information about the configured ACD systems. For each ACD switch, you see information such as the following:

- ACD number and name.
- Switch type. For example, Communication Manager.
- Release number for the ACD switch.
- Activated ACD switch features, such as call vectoring, call prompting, and EAS.
- Phantom abandon call timer value. If this metric is not enabled for the ACD, “off” is displayed.

Calls that are shorter than the configured value (between 1 and 10 seconds) are considered phantom abandoned calls.

CMS software information, such as the release and build, is not available under Switch Setup in the Web Client. You can find this information from **Help > About**.

Considerations for viewing switch setup data

Consider the following before working with the Switch Setup page:

- You can only view information on the Switch Setup page. You cannot modify ACD settings.
- Information about all real ACDs is displayed. Pseudo-ACDs are not displayed.
- The ACD name is only displayed if you assigned a name in the Dictionary. For more information, see [Administering ACD names in the Dictionary](#) on page 41.
- If configured, the phantom abandon call timer value is displayed. The phantom abandon call timer is used to determine which calls to count as abandoned calls rather than ACD calls.

The timer value can be set between 1 and 10 seconds. Calls that are shorter than this duration are considered abandoned calls. This feature is useful in areas where the central office or mobile network does not provide disconnect supervision on trunks.

Viewing switch setup data in the Web Client

About this task

You can view ACD switch information, but you cannot change it.

Procedure

Navigate to **Administration > System Setup > Switch Setup**.

CMS Supervisor displays information for all ACDs.

Viewing Switch Setup data using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Switch Setup**.

3. Click **OK**.

CMS Supervisor displays the Switch Setup window.

4. In the **ACD** field, enter the name or number of the ACD to display.

To have all ACDs returned from the query so that you can cycle through them in this dialog, leave this field blank and proceed to the next step.

5. From the menu bar, select **Actions > Find one**.

CMS Supervisor displays the setup information for the specified ACD. If more than one match was found, use the **Next** and **Previous** items found under the **Actions** menu to cycle through them.

Listing all Switch Setup data using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Switch Setup**.

3. Click **OK**.

CMS Supervisor displays the Switch Setup window.

4. From the menu bar, select **Actions > List all**.

CMS Supervisor displays a secondary window listing all ACDs and their associated settings.

Pseudo-ACD administration

A pseudo-ACD is an area created on the CMS server to store previously backed-up ACD data. Unlike a real ACD, a pseudo-ACD does not communicate with a Communication Manager ACD system.

Pseudo-ACDs are used to store data which can then be viewed in reports. This can be useful in the following scenarios:

- Storing data from an off-site call center for the purposes of reporting in conjunction with an on-site CMS.
- Storing data for archiving purposes. This data can no longer be deleted by the Data Storage Allocation feature and can be used to generate reports with older data for comparison with more recent ACD data.

Considerations for administering pseudo-ACDs

Consider the following before working with pseudo-ACDs:

- Each pseudo-ACD is given a number from 9 through 26. Numbers 1 through 8 are reserved for eight real ACDs connected to the CMS server.
- To load pseudo-ACD data, the CMS server must have enough free space available. Use the Free Space Allocation page to see how much space is required for the existing ACDs and how much is available for pseudo-ACD data.
- Use Data Storage Allocation to define how much historical data will be stored for the pseudo-ACD. Enter storage values equal to or greater than those used for the ACD which originally held the data.
- Set storage intervals for the pseudo-ACD data to match the interval size and data collection times of the ACD from which the data was taken.
- Data collection can be running when modifications are made in the Data Storage Allocation or Storage Intervals page for a pseudo-ACD, but CMS must be in single-user mode.
- For users to access a pseudo-ACD, they must have ACD access permissions, which can be granted from the User Permissions page.
- Before deleting a pseudo-ACD, turn off permissions to it so that users will not be working in the pseudo-ACD when it is deleted.
- CMS does not automatically summarize pseudo-ACD data.
- The following menu items are applicable to a pseudo-ACD:

Reports	CMS System Setup	Maintenance
Historical Dictionary — all submenu items Custom Reports — all submenu items User Permissions — all submenu items	Data Storage Allocation Data Summarizing Free Space Allocation Load Pseudo-ACD Data Pseudo-ACD Setup	Archiving Status Backup/Restore Devices Printer Administration

Adding a pseudo-ACD in the Web Client

Procedure

1. Navigate to **System Setup > Pseudo-ACD Setup**.
CMS Supervisor displays the list of administered pseudo-ACDs.
2. Click **Add Pseudo-ACD Setup**.
3. In the **ACD Number** field, enter an unused number from 9 to 26 to correspond with the new pseudo-ACD.
4. Click **OK** to save your changes.

Deleting a pseudo-ACD in the Web Client

Procedure

1. Navigate to **System Setup > Pseudo-ACD Setup**.
CMS Supervisor displays the list of administered pseudo-ACDs.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. Click **Yes** to complete the change.

Viewing pseudo-ACDs using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **Pseudo-ACD Setup**.
3. Click **OK**.
CMS Supervisor displays the Pseudo-ACD Setup window.
4. From the menu bar, select **Actions > List all**.

CMS Supervisor displays a secondary window listing all ACDs. The status bar displays the total number of pseudo-ACDs on the CMS server. Only those ACDs for which you have “read” permission are displayed.

Adding a pseudo-ACD using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **Pseudo-ACD Setup**.
3. Click **OK**.
Supervisor displays the Pseudo-ACD Setup window.
4. In the **ACD** field, enter the number or the name of the pseudo-ACD. The number can range from 9 to 26. This field requires a number to be entered if a name for this pseudo-ACD has not been defined in the Dictionary.
5. From the menu bar, select **Actions > Add**.
CMS creates the pseudo-ACD.
6. Log out of Supervisor and log in again to acquire permission to the newly created pseudo-ACD.
7. From the Controller window, select **Tools > System Setup**.
Supervisor displays the CMS System Setup window.
8. In the **Operations** list, highlight **CMS State**.
Supervisor displays the CMS State window.
9. Select option **Single-user mode**.
10. From the menu bar, select **Actions > Modify**.
11. Close the CMS State window.
12. Turn off data collection as described in [Turning data collection on and off using the PC Client](#) on page 296.
13. In the **Operations** list, highlight **Data Storage Allocation**.
14. In the **ACD** list, highlight the appropriate pseudo-acd.
15. Select **OK**.
Supervisor displays the Data Storage Allocation window.
16. Enter storage values equal to or greater than the values used for the ACD which originally stored the data.
17. From the menu bar, select **Actions > Modify**.
Supervisor displays the following message:

You may have increased or decreased the amount of storage. Do you want to continue?

18. Select **YES**.
19. Close the Data Storage Allocation window.
20. In the **Operations** list, highlight **Storage Intervals**.
21. In the **ACD** list, highlight the appropriate pseudo-acd.
22. Select **OK**.

Supervisor displays the Storage Intervals window.

23. Enter storage values equal to the values used for the ACD which originally stored the data.
24. From the menu bar, select **Actions > Modify**.

Supervisor displays a message if changes are made to the **Intrahour interval**.

For example, if you change a 30 minute Intrahour interval to a 15 minute Intrahour interval, the system displays the following:

Data will be migrated to the new interval. The data will be divided by 2. Do you want to continue?

- If you want to continue with these settings, select **YES**.
 - If you do not want to continue with these settings, select **NO**. Change any incorrect fields until the form entries are correct.
25. Close the Storage Intervals window.
 26. Turn on data collection as described in [Turning data collection on and off using the PC Client](#) on page 296.
 27. In the **Operations** list, highlight **CMS State**.
Supervisor displays the CMS State window.
 28. Select the option **Multi-user mode**.
 29. From the menu bar, select **Actions > Modify**.
 30. Close the CMS State window.
 31. Do one of the following:
 - If you want to create a Dictionary name for the pseudo-ACD just created, continue with Step [29](#) on page 272.
 - If you do not want to create a Dictionary name for the pseudo-ACD just created, continue with [Viewing pseudo-ACDs using the PC Client](#) on page 270.
 32. From the menu bar, select **Commands > Dictionary**.

 Note:

A pseudo-ACD must exist before a dictionary name for the pseudo-ACD can be created.

Supervisor displays the Dictionary window.

33. In the **Operations** list, highlight **ACDs**.

34. Select **OK**.

Supervisor displays the Dictionary ACDs window.

35. In the **ACD Name** field, enter the name for the pseudo-ACD.

36. In the **ACD Number** field, enter the number for the pseudo-ACD from Step 4.

37. In the **Description** field, a description for the pseudo-ACD. The origin of the data can be useful information in the description field.

38. From the menu bar, select **Actions > Add**.

Supervisor adds the pseudo-ACD name to the dictionary.

 Note:

After creating a dictionary name for a pseudo-ACD, you must log out of Supervisor and log in again to see the dictionary name of the pseudo-ACD displayed in drop down lists.

39. Continue with [Viewing pseudo-ACDs using the PC Client](#) on page 270.

Deleting a pseudo-ACD using the PC Client

About this task

This section provides the procedure for deleting a pseudo-ACD on a CMS server.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Pseudo-ACD Setup**.

3. Click **OK**.

Supervisor displays the Pseudo-ACD Setup window.

4. In the **ACD** field, enter the name or number of a pseudo-ACD to delete.

5. From the menu bar, select **Actions > Find one**.

The status bar displays whether a match was found for the specified pseudo-ACD.

6. From the menu bar, select **Actions > Delete**.

CMS deletes the pseudo-ACD, the associated data, and returns any associated disk space to the database. When the operation completes, Supervisor displays a `Successful` message in the status bar.

About backing up data from a real ACD to load on a pseudo-ACD

You must back up historical data archived from an existing real ACD. This backed up data is loaded onto a pseudo-ACD.

Before performing this task, you need Write permissions for the Maintenance subsystem and for the Back Up Data option.

Considerations for backing up data from a real ACD to load on a pseudo-ACD

Consider the following before backing up real ACD data for a pseudo-ACD:

- You must create a pseudo-ACD as described in [Pseudo-ACD administration](#) on page 269.
- Archive data from an existing ACD before using it for a pseudo-ACD.
- The data from a full backup might be more than needed. Loading a pseudo-ACD with a full backup can result in disk space problems. To eliminate this problem, back up specific tables when creating the ACD data to load onto a pseudo-ACD.
- Data storage allocation for the pseudo-ACD must match or be greater than the ACD where the data was archived. Document the data storage allocation values for the ACD where the data was archived. Verify that the pseudo-ACD configuration matches or is greater than the documented values. If these settings are incorrect, the process of loading data onto the pseudo-ACD might fail.
- Storage intervals for the pseudo-ACD must match the ACD where the data was archived. the values do not match, the process of loading data onto the pseudo-ACD might fail.
- You should be using a network mount point for the backup. Ensure that the backup device path is configured in **Maintenance > Backup/Restore Devices**.

Scenario for backing up data from a real ACD to load on a pseudo-ACD

About this task

Data is loaded from the latest available CMS maintenance backup in the specified backup/restore device. In this high-level procedure, the backup/restore device is a network mount point and the data to be loaded to the pseudo-ACD is a set of specific tables.

Procedure

1. Create a directory for the pseudo-ACD data only.
2. From **Maintenance > Backup/Restore Devices**, configure the backup/restore device you are planning to use to point to the pseudo-ACD directory.
3. From **Maintenance > Back Up Data**, select the specific tables to back up.
To prevent storage issues, ensure that you only back up the data you need. For example, do not back up data for all ACDs if you only need data for the current ACD.
4. From **System Setup > Load Pseudo-ACD Data**, load data onto the pseudo-ACD using the same device that was used to back up data.

This process ensures that the correct data is loaded onto the pseudo-ACD. With this process, the only data that should exist in the directory for the backup/restore device is the data specifically backed up for the pseudo-ACD.

About loading pseudo-ACD data

Loading historical data archived from an existing ACD onto a pseudo-ACD. When the data is available on the pseudo-ACD, historical reports can be run with this information.

Considerations for loading pseudo-ACD data

Consider the following before loading data onto a pseudo-ACD:

- You must create a pseudo-ACD as described in [Pseudo-ACD administration](#) on page 269.
- Before loading data onto a pseudo-ACD, you must back up the data archived from an existing ACD. Review the information in [Considerations for backing up data from a real ACD to load on a pseudo-ACD](#) on page 274.
- Set the pseudo-ACD as the current ACD before attempting to load data into it.
- Loading a pseudo-ACD with data automatically overwrites any existing data currently used by the pseudo-ACD.
- When created, a new pseudo-ACD has historical data storage parameters set to zero. To load data into the pseudo-ACD, the historical data storage allocation values must match or be greater than the values for the ACD from which the data was archived.
- Storage intervals and data collection settings must be configured to match those of the ACD supplying the data. Otherwise, the process of loading data onto the pseudo-ACD might fail.

Verifying that backup data can be read

About this task

Before loading data onto a pseudo-ACD, verify that the backup data can be read.

Procedure

1. Log in to the CMS server with root privileges.
2. Run the `/cms/bin/br_check` command to verify the data source.
3. When prompted to specify the device type, enter `n` for a network mount point device.
4. Enter the device path.

The following is an example of the backup information displayed for a network mount point device:

```
Opening the volume...
Label: CMS-200603-01-LSAC-00-F-01
CMS Database Version: r21Lba.c

Machine name: cmstestsystem
forecasting: n
global dictionary/ACD groups: y
multi-tenancy: y
Dual IP: n
LDAP authentication: y

ACD(s) backed up on the volume:
ACD      Switch  EAS      Vectoring
1        R8      y        y
2        R7      y        y

Enter 'l' to list the tables or 'v' to also verify the volume:
```

5. Enter `v` to verify the backup data and review the output.
6. If the backup data displayed in the output is valid, continue with loading pseudo-ACD data.
If the data is not valid, replace the path with the correct backup data information and repeat the validation process.

Loading pseudo-ACD data in the Web Client

About this task

After backing up archived data from an existing ACD, you can load the data onto a pseudo-ACD. When the loading process starts, the status is displayed along with any errors. Avoid canceling the loading process while it is in progress.

Procedure

1. Navigate to **Administration > System Setup > Load Pseudo-ACD Data**.
2. In the **From ACD** field, enter the ACD number for the source ACD used to back up data.
3. From the **To ACD** list, select the pseudo-ACD that will receive the data.
4. From the **Device Name** list, select the device used for the backup.
Data will be loaded from this backup device.
5. In the **Start Date** and **Start Time** fields, specify the starting point from which historical data will be loaded.

You can leave the start date blank if you want all available historical data from the beginning of the backup to be loaded.

6. In the **Stop Date** and **Stop Time** fields, specify the end point at which CMS will stop loading data from the backup.
7. Click **Run** to start the loading process.

Related links

[Verifying that backup data can be read](#) on page 275

Loading pseudo-ACD data in the PC Client

Procedure

1. From the Controller window, select **Tools > System Setup**.

Supervisor displays the CMS System Setup window.

2. In the **Operations** list, highlight **Load Pseudo-ACD Data**.
3. In the **ACD** field, select the pseudo-ACD that will receive the data.
4. Click **OK**.

CMS Supervisor displays the Load Pseudo-ACD Data window.

5. In the **From ACD** field, enter the ACD number for the source ACD used to back up data.
6. In the **Device Name** field, enter the name of the device used for the backup.

Tip:

To list all the devices on the CMS server, select **Actions > List devices** from the menu bar.

Ensure that the latest CMS maintenance backup on the specified device contains the data you want loaded into the pseudo-ACD.

7. In the **Start Date** field, enter the date representing the first day of historical data to load into the pseudo-ACD.

CMS searches the data backup for this date which serves as the starting point for loading data.

8. In the **Start Time** field, enter the time when CMS will start loading data. The default is 12:00AM.
9. In the **Stop Date** field, enter the last date of historical data that CMS will load into the pseudo-ACD.
10. In the **Stop Time** field, enter the time when CMS will stop loading data from the data backup. The default is 12:00AM.
11. From the menu bar, select **Actions > Run**.

CMS begins loading data from the backup into the pseudo-ACD. The **Status** field at the top of the window displays events in the loading process. The **Errors** field displays any problems encountered during the loading process.

Canceling the load process before it is finished causes the pseudo-ACD to have partial data.

When the data has been loaded, Supervisor displays the Load Pseudo-ACD Data - Acknowledge window.

- If there is no other volume of data to load, select **Actions > Stop**.
- If there are more volumes to load data from, select **Actions > Continue**.

If you log out of CMS before the data is loaded, the process continues to run in the background. You can log back in later to check the status.

Data storage allocation

Data storage parameters are initially set during installation, but you can modify these settings. Use the Data Storage Allocation page to specify the amount of historical data saved by CMS and the duration for which it is saved. The amount of data you can store depends on your server capacity. The type of ACD switch also affects system capacity.

For capacity and scalability specifications, see *Avaya Call Management System Overview and Specification*. You can also find capacity limits for small, medium, large, and extended servers.

Data storage allocation considerations

Consider the following before working with data storage allocation:

- A full maintenance backup should be performed before changing the data storage allocation configuration.
- Before changing data storage allocation values, you must disable data collection and set the CMS state to single-user mode.
- You can make ACD system changes by running the `cms svc` command and selecting the **swsetup** option. If you do this, you must check the data storage allocation settings to ensure that storage is set for any new or modified entities. For example, when activated, the Call Vectoring feature requires data storage space for VDNs and vectors. Changing the release number for the ACD system might change the number of measured entities and affect the storage allocation for each entity.
- When determining the amount of storage space needed, remember that future growth of items, such as trunk groups or splits/skills, need to be taken into account.
- If a Data Storage Allocation window is modifying data in the PC Client, do not open a second Data Storage Allocation window. Wait for the first window to finish the modifications as performing simultaneous modifications through two Data Storage Allocation windows can result in damage to data tables.

- Use the Free Space Allocation page to view the utilization of disk space before making changes to data storage allocation settings. If changes are made to the data storage allocation settings, free space is automatically adjusted.
- The length of the intrahour interval affects the amount of disk space required to store intrahour data. For example, an intrahour interval of 30 minutes requires twice the amount of disk space than an intrahour interval of 60 minutes.
- If the Call Vectoring feature is not enabled, the fields corresponding to call work codes, vectors, and VDNs are not displayed.
- The data storage values determine how much data is available for running historical reports. For example, if weekly and monthly data is not saved, weekly or monthly reports display no data.
- Disk space affects the amount of historical data that can be stored. The following list provides the maximum durations possible when storing historical data:
 - Intrahour - 370 days
 - Daily - 1825 days (5 years)
 - Weekly - 520 weeks (10 years)
 - Monthly - 120 months (10 years)

Viewing data storage allocation in the Web Client

Procedure

1. Navigate to **Administration > System Setup > Data Storage Allocation**.

CMS Supervisor displays the current data storage allocation values.

2. Modify the data storage allocation values as required.

For more information, see [Guidelines for modifying data storage allocation settings](#) on page 280.

Viewing Data Storage Allocation using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Data Storage Allocation**.

3. In the **ACD** field, select the ACD for which the data storage settings will be viewed.

4. Click **OK**.

CMS Supervisor displays the Data Storage Allocation window.

5. To change the Data Storage Allocation values, see [Guidelines for modifying data storage allocation settings](#) on page 280.

Guidelines for modifying data storage allocation settings

Data storage configuration is done on a per-ACD basis. In a multi-ACD environment, data storage allocation should not be set too high as it can exceed the available capacity for other ACDs.

Before modifying data storage allocation settings, consider the following:

- The available capacity for your CMS server.
- The number of ACDs on the CMS system and the information in each ACD. For example, number of agents, trunks, and so on.
- The length of time for data to be stored. For example, 30 days versus 100 days versus two years.

Before modifying data storage allocation settings

Review the following prerequisites before changing the values on the Data Storage Allocation page:

- Navigate to the Maintenance subsystem and perform a full maintenance backup.
- Ensure that data collection is disabled for all ACDs.
- The CMS state must be set to single-user mode.

Description of data storage allocation settings

The following data items are displayed on the Data Storage Allocation page:

- Splits/skills
- Agents
- Trunk groups
- Trunks
- Call work codes
- Vectors
- VDNs

You can set the following values for these data items:

Value	Description
# of Items	Data storage is allocated for the specified number of items. This value is not applicable for the Agents item. When allocating a value, consider the expected growth. For example, 25 splits/skills currently exist, but you enter a value of 30 to account for future growth. A value of 30 indicates that storage space is allocated for 30 splits/skills.

Table continues...

Value	Description
Days of Intrahour	The number of days for which intrahour data is stored. If you enter a value of zero, intrahour data is discarded, which also means that no daily, weekly, or monthly data can be collected. When the specified data collection period elapses, the data is combined, archived, and appended into daily information.
Days of Daily	The number of days for which daily data is stored. If you enter a value of zero, daily data is discarded. When the specified data collection period elapses, the data is combined, archived, and appended into weekly information.
Weeks of Weekly	The number of weeks for which weekly data is stored. If you enter a value of zero, weekly data is discarded. When the specified data collection period elapses, the data is combined, archived, and appended into monthly information.
Months of Monthly	The number of months for which monthly data is stored. If you enter a value of zero, monthly data is discarded. When the specified period of time elapses, the data is deleted.

You can also modify the following fields:

Name	Description
Total split/skill members, summed over all splits/skills	The maximum number of agents or extensions across all splits/skills that are measured or logged in at any one time. This number should include agents or extensions that are members of multiple splits/skills. Each split/skill the agent belongs to counts as a split/skill member. This value represents the maximum agent/skill pairs (skill members) that are logged in.
Number of agent login/logout records	The number of agent login or logout records stored in the system. Each time an agent logs in, CMS creates a record. The subsequent logout of the agent also uses this same record. If the agent logs in again later, another login/logout record is created. The following equation demonstrates how this number is calculated: $(\text{Number of agents}) \times (\text{Number of times each agent logs in each day}) = \text{Number of agent login/logout records}$ If there are 200 agents and each agent logs in three times per day, using the equation above would result in 600 agent login/logout records for this field. When skills for an agent are changed, a new login/logout record is generated if the agent is currently logged in to the system.
Number of agent trace records	The number of agent trace records for the selected ACD. This number is not representative of all ACDs.

Table continues...

Name	Description
Number of unmeasured trunk facilities	The number of trunks not measured by CMS. Unmeasured trunk facilities are used for: • Internal calls (intraswitch) to a measured split or agent. • Internal calls to VDNs. • Calls made by agents to internal destinations or using a trunk group that is not measured. • Transfers and conferences until the transfer/conference is complete. This number should be set high enough to handle the traffic expected over these unmeasured trunks, but cannot exceed the maximum number of trunks minus the number of measured trunks. The default value for this field is 300.
Number of exception records	The total number of exceptions stored for CMS. This total is for each type of exception, such as agents, splits/skills, VDNs, and so on.
Number of call records	The number of call records the system stores for the selected ACD. If the CMS Call History Interface application is installed, another computer can be used for storage and analysis of the call records. This field then represents the amount of buffer space set aside on the CMS server that is used to collect the call records prior to transmission to the other system.

About viewing free space allocation

The Free Space Allocation page displays storage information for each ACD. You see the total allocated space, the amount of space used to date, and the total free space.

If you modify the values on the Data Storage Allocation page, the free space allocation information is automatically adjusted.

Free space allocation considerations

The Free Space Allocation page displays read-only information. Consider the following:

- When CMS data storage parameters are altered, the changes are automatically reflected on the Free Space Allocation page. You can view the allocations for each ACD system and the amount of free space.
- The IDS dbspaces used for free space allocation are created during installation.
- Custom tables increase disk space usage. You see a warning if the dbspace used to store custom tables is close to its maximum capacity.

Permissions required to view Free Space Allocation

To view the Free Space Allocation window, you must have “read” permission for the CMS System Setup features.

Viewing free space allocation information in the Web Client

About this task

The information on the Free Space Allocation page is read only. At the top of the page, high-level information is displayed for the current ACD. Near the bottom of the page, a table shows information for all ACDs. You can view the allocation breakdown for a specific ACD.

Procedure

1. Navigate to **Administration > System Setup > Free Space Allocation**.
2. **(Optional)** Use the drop-down list to change the currently-selected ACD.

CMS Supervisor displays a high-level view of the total free space and the total allocated space for the selected ACD.

3. Use the table near the bottom of the page to view the allocated size and the space used to date for all ACDs.

This table is useful for comparing the space allocation for different ACDs. A **Search** field is also available to search for specific information.

4. Click  next to an ACD to view a detailed allocation breakdown.

A new window shows the allocated size in Kilobytes for each data item. The following example image shows the breakdown for the dads16 ACD:

Agents	5845512
Agent Trace	2744
Call work codes	222384
Agent Login/Logout	135608
Splits/Skills	754344
Trunk groups	168128
Trunks	326192
Other (permissions, etc.)	1051360
VDNs	2275848
Vectors	158440
Total	10940560

When you finish reviewing the breakdown, click **OK** to close the window.

Viewing Free Space Allocation using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Free Space Allocation**.

3. Click **OK**.

Supervisor displays the Free Space Allocation input window for each ACDs:

- **ACD Name** - The name assigned to this ACD.
- **Allocated Size** - The amount of space needed to store data based on the settings in the Data Storage Allocation window
- **Space used to Date** - The amount of data actually stored at this time

The window may take a few minutes to open as CMS is calculating the current free space and other values on the system before the window can be displayed.

Viewing Free Space Allocation detailed values using the PC Client

About this task

This section provides the procedure for viewing the allocations for each call center entity within an ACD.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Free Space Allocation**.

3. Click **OK**.

CMS Supervisor displays the Free Space Allocation input window.

Note:

The window may take a few minutes to open as CMS is calculating the current free space before the window can be displayed.

4. In the **ACD** field, enter the name or number of the ACD to view.
5. From the menu bar, select **Actions > Get contents**.

CMS Supervisor displays a secondary window showing the amount of data currently in use by each call center entity.

Storage interval administration

Storage interval settings affect how and when data for the call center is stored. Any changes you make to these settings impact data storage and report data coverage.

The following is a description of the key settings you can manage on the Storage Intervals page:

Intrahour interval

The intrahour interval is the rate at which CMS archives data within a one-hour time period. You can set the interval to 15, 30, or 60 minutes.

Real-time reports use the intrahour interval when displaying data. Cumulative data is reset to zero at the beginning of each intrahour interval.

Data summarizing

You can modify the times and days for which call center data is recorded and summarized.

ACD switch time zone offset

A setting is available to indicate if the ACD time zone is not aligned with the CMS server time zone. Use this setting if you want the CMS time zone to be displayed instead of the master ACD time. If you leave this setting blank, CMS applications automatically display the master ACD time.

The switch time zone offset setting does not affect:

- The time stamps on CMS reports (realtime or historical).
- The PC Client timetable schedule for timetables set to run at local times for a specific ACD.

Considerations for administering storage intervals

Consider the following when working with the Storage Intervals page:

- Before you can change storage interval settings, CMS must be in single-user mode and data collection must be disabled.
- Perform a full backup of historical data before changing the intrahour interval or data summarizing time settings. After making the changes, perform another backup.
- Free space allocation, data storage allocation, and storage intervals are closely related. When you change storage interval settings, you might also need to adjust the values on the Data Storage Allocation page. The more frequently CMS archives data, the more storage space is required. Keep this in mind before changing the frequency of the intrahour interval.
- Changing the intrahour interval can result in a lengthy process as CMS must make modifications to all previously-collected data.
- In the PC Client, do not open another Storage Intervals window if one is already being used to modify settings. Loss of data tables can result if multiple Storage Intervals windows are used.

Modifying storage interval settings in the Web Client

About this task

Use the Storage Intervals page to:

- Set the intrahour interval at which data is archived.
- Offset time zone differences between the ACD and the CMS server.
- Specify when data is recorded and summarized.

When specifying data collection times, you can use the HH:MM AM/PM format or the 24-hour time format.

Procedure

1. Navigate to **Administration > System Setup > Storage Intervals**.
2. Select one of the following **Intrahour interval** options:
 - **15 minutes**
 - **30 minutes**
 - **60 minutes**

3. In the **Switch time zone offset (-23 to +23)** field, do one of the following to offset the ACD time zone so it matches the CMS server time zone:

- If the ACD time zone is ahead of the CMS server time zone, type + followed by the number of hours the ACD is ahead.
- If the ACD time zone is behind the CMS server time zone, type – followed by the number of hours the ACD is behind.
- If the ACD is connected to a CMS server in the same time zone, type 0 in this field.

For example, if the master ACD is in New York City and the CMS server is in Los Angeles, type +3 because the ACD is 3 hours ahead of the CMS server time.

4. Do the following to manage how data is summarized:

- a. In the **Data Summarizing Time** field, specify the time when CMS will summarize data for the previous day, week, and month.

You can enter the time in one of the following formats:

- HH:MM AM/PM - For example, 12:35 AM
- 24-hour format - For example, 00:35

The value you specify in the **Data Summarizing Time** field must be equal to or greater than the intrahour interval to ensure that data archiving is completed.

- b. From the **Week Start Day** list, select the day that represents the start of the work week for the call center.

The default setting is Sunday. Data collection for the week starts on this day.

- c. From the **Week Stop Day** list, select the day that represents the end of the work week for the call center.

The default setting is Saturday. Data is collected until the end of this stop day and included in the weekly summary.

Avoid changing the start and stop days until the weekly data is archived. When the start and stop days for the week are changed, the current week contains the data item **INCOMPLETE** to indicate that data collection for the week is abnormal because the definition of the week was changed. Note that if the start and stop days are identical, only one day of data is collected for the current week.

- d. In the **Daily Start Time** field, enter the time when data collection will start.

For example, you can set 12:00 AM as the start time.

- e. In the **Daily Stop Time** field, enter the time when data collection for the day will stop.

For example, you can set 11:59 PM as the end of the day. The start time and stop time cannot be the same.

5. Click **Modify** to save your changes.

Managing storage interval settings in the PC Client

Viewing storage interval settings using the PC Client

About this task

This section provides the procedure for viewing the Storage Intervals settings for call center data.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **Storage Intervals**.
3. In the **ACD** field, select the ACD for which settings will be viewed.
4. Click **OK**.

CMS Supervisor displays the Storage Intervals window.

Modifying the intrahour interval using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **Storage Intervals**.
3. In the **ACD** field, select the ACD for which the intrahour interval will be changed.
4. Click **OK**.
CMS Supervisor displays the Storage Intervals window.
5. In the **Intrahour interval (select one)** group, select the option for the rate at which CMS archives call center data.

Caution:

Do not open another **Storage Intervals** window and attempt to change other settings during the following step. Doing so can result in the loss of database tables.

6. From the menu bar, select **Actions > Modify**.

CMS records the setting change and alters all previously recorded data to match this setting. This update process is lengthy and must not be interrupted. The status bar will display a **Successful** message when the operation completes.

7. Restart data collection.

See [Turning data collection on and off using the PC Client](#) on page 296 for information on this procedure.

8. Return CMS to multi-user mode.

See the [Changing the CMS operational state using the PC Client](#) on page 294 for information on this procedure.

Modifying the switch time zone using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Storage Intervals**.
3. In the **ACD** field, select the ACD which will have its time zone offset changed.
4. Click **OK**.

Supervisor displays the Storage Intervals window.

5. In the **Switch time zone offset (-23 to +23)** field, enter the number of hours that will convert the time zone of the ACD so that it matches the time zone of the CMS server.

If the ACD time is ahead of the CMS server time, you must enter a plus sign (+) followed by the number of hours the ACD is ahead. If the ACD time is behind the CMS server time, you must enter a minus sign (-) followed by the number of hours the ACD is behind.

For example, if the master ACD is in New York City and the CMS server is in Los Angeles, you would enter +3 because the ACD is 3 hours ahead of the CMS server time. The time zone offset does not affect the time stamps that are used with historical data.

6. From the menu bar, select **Actions > Modify**.

CMS adjusts the time setting of the ACD by the value specified. The status bar will display a **Successful** message when the operation is complete.

Note:

The CMS time reverts to the operating system (Linux) clock if the link to the ACD that is designated as the master clock stops functioning. Even if the link begins to function normally, the only way CMS will reset back to the master clock is to either turn CMS off and then on or reboot the server.

7. Restart data collection.

See [Turning data collection on and off using the PC Client](#) on page 296 for information on this procedure.

8. Return CMS to multi-user mode.

See [Changing the CMS operational state using the PC Client](#) on page 294 for information on this procedure.

Modifying the data summarizing time settings using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Storage Intervals**.
3. In the **ACD** field, select the ACD which will have its data summarizing settings changed.
4. Click **OK**.

CMS Supervisor displays the Storage Intervals window.

5. In the **Data Summarizing Time** field, enter the time when CMS should summarize data for the previous day, week, and month. The time must be entered in one of the following formats:

- HH:MM PM - For example, 12:35 AM
- 24-hour format - For example, 00:35

If you do not wish to change this field, skip this step and proceed to the next.

The time entered in this field must be equal to or greater to intrahour interval in order to allow CMS to finish archiving data. The default time for this field is 12:35 AM.

Weekly summaries are started on the day following the day specified in the **Week Stop Day** field. Monthly summaries are started on the first day of the next month. For example, the monthly summary for January is done on the first day of February.

To run data summarizing on the day for which data was collected, the **Data Summarizing Time** field must be set for 15 minutes after the **Daily Stop Time** and prior to midnight.

For example, the **Data Summarizing Time** field can be set to 11:59 PM or 23:59. This would require that the **Daily Stop Time** field be set to 11:44 PM or 23:44.

6. In the **Week Start Day** group, select the day that represents the start of the work week for the call center.

If you do not wish to change this field, skip this step and proceed to the next.

The default value for this field is **Sunday**.

7. In the **Week Stop Day** group, select the day that represents the end of the work week for the call center.

If you do not wish to change this field, skip this step and proceed to the next.

The default value for this field is **Saturday**. Data through the end of the stop day is collected and included in the weekly summary.

When the start or stop day is changed for the week, the data from the old start day through the new stop day for the week is archived.

If possible, make any changes to the **Week Start Day** and **Week Stop Day** after CMS performs the weekly archive. This change is not possible for a seven-day week. When the start and stop day for the week are changed, the current week will contain the data item, **INCOMPLETE**, to indicate that the data for this week is peculiar since the definition of that week was changed.

If the **Week Start Day** and **Week Stop Day** are identical, data for only one day will be collected for that week.

8. In the **Daily Start Time** field, enter the time at which data collection should start. Enter the time in one of the following formats:

- HH:MM PM - For example, 12:00 AM
- 24-hour format - For example, 00:00

If you do not wish to change this field, skip this step and proceed to the next.

The default value for this field is 12:00 AM (midnight).

9. In the **Daily Stop Time** field, enter the time at which data collection should stop. Enter the time in one of the formats specified in the previous step.

If you do not wish to change this field, skip this step and proceed to the next.

The default value for this field is 11:59 PM. Data is collected through the end of the minute specified.

Do not enter the same time in this field as in the **Daily Start Time** field. Doing so will result in data being collected for only one minute per day.

10. From the menu bar, select **Actions > Modify**.

CMS updates the data summarizing parameters as specified. A `Successful` message appears in the status bar when CMS completes the operation.

11. Restart data collection.

See [Turning data collection on and off using the PC Client](#) on page 296 for information on this procedure.

12. Return CMS to multi-user mode.

See [Changing the CMS operational state using the PC Client](#) on page 294 for information on this procedure.

Administration of custom menu items

You can create custom menu items in the Web Client or the CMS ASCII interface. You cannot do this from the PC Client. To create custom menu items in the Web Client, navigate to **System Setup > Main Menu Addition**.

You see custom menu items when you run the `cms` command to access the CMS Main Menu. You can do this through Terminal Emulator, a telnet session to the CMS server, or the CMS console. Custom menu items are not displayed in the CMS Supervisor interface.

Adding a custom menu item from the Web Client

Procedure

1. Navigate to **Administration > System Setup > Main Menu Addition**.
2. Click **Add Main Menu Addition**.
3. In the **Menu Item Name** field, enter a name for the new menu item.
4. In the **Description** field, briefly describe the purpose of the menu item.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
5. In the **Full Path Name** field, enter the path to the executable command installed on the CMS server.
6. Click **OK** to save your changes.

Modifying custom menu items using the Web Client

Procedure

1. Navigate to **Administration > System Setup > Main Menu Addition**.
CMS Supervisor displays the Main Menu Addition window.
2. Click  for the menu item you want to change.
The Modify Item window is displayed.
3. **(Optional)** Revise the information in the **Description** field.
You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.
4. In the **Full Path Name** field, update the path to the executable command on the CMS server.
5. Click **OK** to save your changes.

Deleting custom menu items using the Web Client

Procedure

1. Navigate to **Administration > System Setup > Main Menu Addition**.
2. Click  next to the item you want to delete.
The Confirm Delete dialog box is displayed.
3. Click **Yes** to complete the change.

CMS operational states

CMS can run in two operational states:

- Multi-user mode: Any defined user can log on to CMS.
- Single-user mode: Only one user can be logged in to the CMS server at a time.

You must enable single-user mode when making changes to the following systems and procedures:

- Master ACD changes
- ACD group administration
- Data storage allocation
- Storage intervals
- Restore specific types of data
- Migrate specific types of data

The CMS State page can be used to select which ACD serves as the master for time synchronization.

Considerations for changing the CMS operational state

Consider the following before changing the CMS state:

- To change the settings on the Data Storage Allocation, Storage Intervals, and Restore Data pages, you must set the CMS state to single-user mode. This is not required to view information.
- If a user logs out while CMS is still in the single-user state, another user cannot log in for at least ten seconds.
- While in single-user mode, CMS continues to collect data for all ACDs with the data collection feature enabled.

Changing the CMS operational state and master ACD in the Web Client

About this task

Use the CMS State page to change the operational state to single-user mode or multi-user mode. Single-user mode is required to change certain settings.

You can also choose to change the master ACD used for CMS time synchronization.

Before you begin

Disable data collection before changing the master ACD.

Procedure

1. Navigate to **Administration > System Setup > CMS State**.
2. Select one of the following CMS user mode options:
 - **Single-user mode**: Specifies that the CMS state is being set to single-user mode. A message displays to all users indicating that CMS will be brought down in one minute. Users are automatically logged out after one minute.
 - **Multi-user mode**: Specifies that multiple users can be logged in to CMS simultaneously.
3. **(Optional)** In the **Master ACD for clock synchronization** list, select a different ACD to be used for time synchronization.
4. Click **Modify** to save your changes.

Changing the CMS operational state using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **CMS State**.
3. Click **OK**.
Supervisor displays the CMS State window.
4. Under **CMS user mode**, select one of the following options:
 - **Single-user mode** - Specifies that the CMS state is being set to single-user mode. When CMS is set to single-user mode, a message box displays to all users indicating that CMS will be brought down in one minute. Users are automatically logged off after one minute.
 - **Multi-user mode** - Specifies that the CMS state is being set to allow multiple users to log on to CMS.
5. After selecting the CMS user mode, select **Actions > Modify** from the menu bar.
If the CMS user mode is set to single-user, all CMS users are notified to log off. If the CMS user mode is set to multi-user, CMS users can again log on to the system.

Changing the master ACD using the PC Client

Before you begin

Important:

You must turn data collection off before you change the master ACD.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **CMS State**.

3. Click **OK**.

Supervisor displays the CMS State window.

4. In the **Master ACD for clock synchronization** field, select the ACD that will serve as the master for the synchronization of time for CMS .

5. After selecting the master ACD, select **Actions > Modify** from the menu bar.

The selected ACD is set as the master for time synchronization and the status bar displays a **Successful** message.

About turning data collection on and off

Use the Data Collection page to turn data collection on or off for an ACD. When data collection is turned off, no call center data is recorded during the current interval. Reports that are run to include this time period will not accurately reflect call center activities.

Before turning data collection on and off

The following items should be read and understood before working with the data collection feature:

- When data collection is turned on, the connection status of the link should be monitored to ensure data is being transferred. Use the Connection Status feature in the Maintenance subsystem to view this information.
- The data collection feature does not apply for pseudo-ACDs as they do not collect data.
- When changing the data collection status, each ACD must be administered separately.
- Data collection must be disabled when making changes to the following features:
 - Data Storage Allocation
 - Storage Intervals
 - Change Master ACD
 - Restore specific types of data
 - Migrate specific types of data

Viewing data through the features listed above can be done with data collection enabled.

- Data collection must be turned on for the current ACD in order to activate an agent trace or do any switch administration from CMS.
- When data collection is turned off, no new data is collected. If calls are in the system, the data they generate is not recorded in CMS. If data collection is to be turned off, it is best to wait for the current interval to be archived so that data loss is minimized.

Turning data collection on and off in the Web Client

About this task

You can modify the data collection setting for an ACD. You must disable data collection before changing certain settings. When you finish making the required changes, ensure that you re-enable data collection so call center data is accurately recorded.

Procedure

1. Navigate to **Administration > System Setup > Data Collection**.

CMS Supervisor displays the Data Collection window.

2. Click  next to the ACD you want to manage.

The Modify Item window is displayed.

3. From the **Data Collection** drop-down list, select **On** or **Off**.

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

5. **(Optional)** To enable or disable data collection for all ACDs, click from the following options:

- **Enable data collection for all ACDs:** You can then view a message reminding you to check the Connect Status Window to determine when data collection has resumed.

If data collection is enabled for all ACDs, the **Enable data collection for all ACDs** button is disabled.

- **Disable data collection for all ACDs:** You must confirm the operation to disable data collection.

If data collection is disabled for all ACDs, the **Disable data collection for all ACDs** button is disabled.

Turning data collection on and off using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Data Collection**.

3. Click **OK**.

Supervisor displays the Data Collection window.

4. In the **ACD** field, select the ACD which will have data collection turned on or off.

5. Under **Data Collection**, select one of the following options:

- **On** - Enables data collection for the selected ACD.
- **Off** - Disables data collection for the selected ACD.

About running data summarizing

Data is automatically archived based on the entries in the Storage Intervals window. Data Summarizing is used to manually archive data in the daily, weekly, and monthly tables of the historical database.

Before running data summarizing

The following items should be read and understood before working with the Data Summarizing window.

Important:

Since data is automatically archived based on the entries in the Storage Intervals window, this tool *must not* be used unless an archive failed or did not occur.

- Using the Data Summarizing window causes the archiving to happen immediately.
- Automatic and manual data summarizing include time zone archiving when time zones are administered using System Setup Data Summarization Time Zone.
- Multiple data summarizing requests are queued and are run in the order requested.
- Automatic daily, weekly, and monthly data summaries are queued along with manual requests so that just one type of data summarizing occurs at a time.
- Adequate storage space must be made available through the Data Storage Allocation window before archiving can occur.
- Additional storage space is needed for time zone archiving. The maximum amount of additional storage space is twice the size of the storage space of the ACD without time zone archiving. Each ACD time zone requires twice the necessary storage for that ACD. Each tenant time zone occupies a smaller amount of storage space depending upon the resources that are assigned to that tenant. But this amount does not exceed the size of the storage space for the ACD without time zone archiving.
- You can optionally administer a second time zone for an ACD. For that second time zone, the Free Space Allocation feature automatically accounts for the second time zone. This is also true with tenancy. For more information, see About time zone archiving with additional time zones in *Maintaining and Troubleshooting Avaya Call Management System* and [Free Space Allocation](#) on page 282.
- A manual archive cannot be performed unless data exists in the daily, weekly, or monthly tables. If a day of data is missing within the period you are attempting to manually archive, the archive will fail.
- Results of daily, weekly, and monthly archives can be viewed through the Error Log Report or the Archiving Status window.
- If CMS is not operational when an automatic archive should occur, an error message is logged which indicates that a manual archive should be performed using the Data Summarizing window. If time zone archiving has been administered, the result of each time zone archive is viewable.

- If an incomplete week or month is specified as a date, data summarizing will not occur. Partial weekly or monthly data cannot be summarized. A daily archive can run if the date is not in the future.
- For example, if a week is configured in the Storage Intervals window as being Monday through Friday, entering a date which falls on Saturday in the Data Summarizing window results in the week previous to the date specified being archived.

Running data summarizing using the Web Client

Procedure

1. Navigate to **Administration > System Setup > Data Summarizing**.

CMS Supervisor displays the Data Summarizing window.

2. In the **ACD** drop-down list, select the ACD for which you want to archive data.

3. In the **Data Type** field, select the appropriate option:

- **Daily** - Archives data for one day. A daily summary archives a partial day. Daily summaries must be complete for each day of the week or month before CMS archives the data for that week or month.
- **Weekly** - Archives data for one week. A weekly summary must be requested by entering a date that falls within a completed predefined week. See the weekly configuration in the Storage Intervals window.
- **Monthly** - Archives data for one month. Set any day during the month in a completed month for which monthly data should be summarized.

4. Click **Run** to start the data archiving. Click **Reset** to clear the option fields.

CMS Supervisor begins archiving data to the historical database tables.

Running data summarizing using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Data Summarizing**.

3. Click **OK**.

Supervisor displays the Data Summarizing window.

4. In the **ACD** field, select the ACD for which you want to archive data.

5. In the **Data Type** field, select the appropriate option:

- **Daily** - Archives data for one day. A daily summary archives a partial day. Daily summaries must be complete for each day of the week or month before CMS archives the data for that week or month.

- **Weekly** - Archives data for one week. A weekly summary must be requested by entering a date that falls within a completed predefined week. See the weekly configuration in the Storage Intervals window.
- **Monthly** - Archives data for one month. Set any day during the month in a completed month for which monthly data should be summarized.

6. From the menu bar, select **Actions > Run**.

Supervisor displays a warning message stating that data archiving is a lengthy process and cannot be cancelled. Through this window, it is possible to cancel the data archive, otherwise the process continues when the message box is dismissed.

`Archiver started` displays on the status line for the first request and `Archiver request submitted` displays if a data summary is currently in progress.

Administering a data summarization time zone in the Web Client

About this task

To allow for alternative time zone reporting for daily, weekly, and monthly data, a second time zone can be defined to archive the data. This second time zone is in addition to the default ACD time zone. Each time zone is aggregated based on the boundary of a day for the selected time zone. You can choose one time zone from the possible 600+ time zones to use as the second time zone for an ACD.

If tenant partitioning is enabled, you can define a time zone for each tenant within an ACD and choose from those time zones to have the data additionally aggregated. Data is stored in up to three different time zones. With the multi-tenancy feature, one time zone per tenant and one additional time zone for the ACD are supported.

In addition, the agent trace and exception data will be stored in UTC/GMT time enabling filtering and reporting of agent trace and exception data based on the time zone selected on CMS Supervisor.

* Note:

The administration of time zones does not automatically create the time zone data in the daily, weekly, and monthly tables. The Archiver must run after the time zone is administered.

Before you begin

Change the operational state to single-user mode.

Procedure

1. Navigate to **Administration > System Setup > Data Summarization Time Zone**.
2. In the **Current ACD** list, select the ACD for which you want to change the data summarization time zone.
3. Click **Add Data Summarization Time Zone**.
4. Select the time zone to be used for this ACD.
5. Click **OK** to save your changes.

Administering a data summarization time zone using the PC Client

About this task

To allow for alternative time zone reporting for daily, weekly, and monthly data, a second time zone can be defined to archive the data. This second time zone is in addition to the default ACD time zone. Doing this results in aggregating the data for two different time zones. Each time zone is aggregated based on the boundary of a day for the selected time zone. You can choose one time zone from the possible 600+ time zones to use as the second time zone for an ACD.

If tenant partitioning is installed, the user can define a time zone for each tenant within an ACD and choose from those time zones to have the data additionally aggregated. This results in storing the data in up to three different time zones. With the multi-tenancy feature installed, one time zone per tenant and one additional time zone for the ACD are supported.

In addition, the agent trace and exception data will be stored in UTC/GMT time enabling filtering and reporting of agent trace and exception data based on the time zone selected on CMS Supervisor.

* Note:

The administration of time zones does not automatically create the time zone data in the daily, weekly, and monthly tables. The Archiver must run after the time zone is administered.

Before you begin

Change the system to single-user state before you do this task.

Procedure

1. From the Controller window, select **Tools > System Setup**.
2. In the CMS System Setup window, select **Data Summarization Time Zone** in the **Operations** list.
3. In the System Setup Data Summarization Time Zone window, do any of the following operations as explained in the table below:

* Note:

The System Setup Data Summarization Time Zone window displays the tenant option only if the customer has installed the tenancy feature.

Field	Description
Add	Adds the entry for the selected time zone and the associated ACD and tenant (if the tenancy feature is installed) in the current user window to the database. If an entry already exists, the system displays <code>Already exists</code> on the window status line.
Delete	Removes the entry for the selected time zone and the associated ACD and tenant (if the tenancy feature is installed) in the current window from the database. If the database entry does not exist, the system displays <code>Does not exist</code> on the status line.

Table continues...

Field	Description
Find one	Finds an entry in the database that matches the time zone and associated ACD and tenant (if the tenant feature is installed) in the current window. The status line for the current window indicates the total number of matches found.
List all	Lists all the ACDs, tenants and tenant users (if the tenancy feature is installed), and the time zones in the database that match with the values entered in the fields of the current user window.
Next	After doing a Find one search resulting in more than one match, this selection displays the next match.
Previous	After doing a Find one search resulting in more than one match, this selection displays the previous match.

About External Application Status

The External Application Status feature, a separately purchased option for CMS , sends real-time data to an external device or to an external program.

 Note:

External Application Status feature administration is only available from the PC Client.

The types of external devices or programs used with the External Application Status feature can consist of the following:

- A wallboard - This is a large display placed in a call center where all agents can view data. This data can consist of the number of calls in the queue, calls being handled by different splits/skills, and other information.
- An employee scheduler program - This third-party software is used to compare the start and end times for agents with schedules created by management.
- A call center data consolidation program - This third-party software is used to collect data from all call centers for reporting purposes.

Before using External Application Status

The following items should be read and understood before working with the External Application Status feature:

- In the United States, external applications are designed and administered by the Avaya Professional Services Organization. For more information about external applications, call Avaya Contact Center CRM Solutions at 1-877-927-6662. For assistance outside the United States, contact your local Avaya distributor or representative.

Permissions for External Application Status

Depending on the procedure that you want to perform, you need the following permissions:

- To view External Application Status data, the user ID used to log in to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To enable or disable the External Application Status feature, and start or stop external applications, the user ID used to log in to this Supervisor session requires “write” permission for the CMS System Setup feature.

Enabling or disabling the External Application Status feature

About this task

This section provides the procedure for enabling or disabling the External Application Status feature. This feature must be enabled before external applications can be started. Disabling this feature will cause CMS to stop sending data and the external applications cannot be viewed.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **External Application Status**.
3. Click **OK**.
Supervisor displays the External Application Status window.
4. In the **External Application (Select one)** group, select the **External application feature (turns on/off all applications)** option.
5. Select the appropriate option from the **Application status (Select one)** group:
 - **Start** - This option will enable the External Application Status feature.
 - **Stop** - This option will disable the External Application Status feature.
6. From the menu bar, select **Actions > Modify**.

The status bar displays a message indicating if the action succeeded or failed.

Viewing the states of external applications

About this task

This section provides the procedure for viewing the state of one or more external applications through the External Application Status window.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **External Application Status**.

3. Click **OK**.

Supervisor displays the External Application Status window.

4. In the **External Application (Select one)** group, select the **External application feature (turns on/off all applications)** option.
5. From the menu bar, select **Actions > List all**.

Supervisor displays a secondary window displaying one or more applications, their names, and the associated states depending on which option was selected in the step above.

The status of an external application can be one of the following:

- **Starting** - A request to start the external application has been made.
- **Running** - The external application has started and is still running after ten seconds.
- **Stopping** - A request to stop the external application has been made.
- **Stopped** - All processes associated with the external application have stopped.
- **Failed** - The external application has failed repeatedly and is no longer being restarted.

Starting or stopping external applications

About this task

This section provides the procedure for starting and stopping external applications through the External Application Status window.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.
CMS Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **External Application Status**.
3. Click **OK**.
Supervisor displays the External Application Status window.
4. Select the **Application name:** option and enter the name of the application to start or stop in the adjacent field.
5. In the **Application status (Select one):** group, select the appropriate option:
 - **Start** - Supervisor will attempt to start the specified external application.
 - **Stop** - Supervisor will attempt to stop the specified external application.
6. From the menu bar, select **Actions > Modify**.
Supervisor attempts to carry out the specified action. The status bar displays the results of the action.

The information that displays in the status bar after this step can consist of the following.

- **Starting** - A request to start the external application has been made.
- **Running** - The external application has started and is still running after ten seconds.
- **Stopping** - A request to stop the external application has been made.
- **Stopped** - All processes associated with the external application have stopped.
- **Failed** - The external application has failed repeatedly and is no longer being restarted.

Data migration

You can use CMS Supervisor to migrate data from one CMS server onto the database of another CMS server.

 Important:

Do not migrate Agent and Call Center Administration data more than once. If you attempt to perform the migration a second time, data could be corrupted.

Before migrating data

The following items should be read and understood before migrating data:

 Caution:

Attempting to migrate Agent and Call Center Administration data more than once might cause serious errors from which recovery is difficult. Performing the migration of this data a second time can result in the corruption of the password tables. To do a second migration of ACD administration data, do a second setup of the CMS software.

- To migrate System Administration data or Agent and Call Center Administration data, CMS must be in single-user mode.
- Migrations of system administration data cannot be done in phases. Migrating some user IDs at one time and others at a later time result in two separate sets of data. Only one set of data can be used and cannot be migrated into another set.
- When migrating or restoring a non-LDAP user from a maintenance backup, and the “logid” (logon ID) for a user does not exist in `/etc/passwd`, the user is created as a new logid. That logid requires password administration just as if the user was created as described in [User administration](#) on page 173.

When this happens, the migration and restore logs contain messages similar to the following examples:

```
- /cms/maint/r3mig/mig.log
```

```
INFO: New UNIX user normusr1: name, room and telephone will not be
migrated.
```

```
- /cms/maint/restore/rest.log
```

```
Created UNIX login 'normusr1'.
```

```
Warning: Name, Telephone, and Room will not be restored for
normusr1.
```

Migrating data from the Web Client

About this task

You can migrate or merge data from a previous version of CMS to the database of another CMS server that uses the same version or a newer version of the software. For a detailed description of the options on the Migrate Data page, see [Migrate Data page descriptions](#) on page 307.

Important:

Do not attempt to migrate Agent and Call Center Administration data more than once.

Before you begin

To migrate System Administration data or Agent and Call Center Administration data, CMS must be in single-user mode. For more information, see [CMS operational states](#) on page 293.

Procedure

1. Navigate to **Administration > System Setup > Migrate Data**.
2. Select the backup device to use from the **Device Name** drop-down list.
3. Select one of the following data type options:
 - **System Administration data (single-user mode required)**
 - **Agent/Call Center Admin data (single-user mode required)**
 - **Historical data**
4. Enter a value in the **Stop Date** field.
5. Enter a value in the **Stop Time** field.
6. Select one of the following ACD options:
 - **All ACDs**: To migrate data from all ACDs.
 - **Single ACD**: If you select this option, you must specify the ACD you are migrating from and the ACD you are migrating to.
7. Click **Run** to start the migration.

Status information is displayed at the top of the page. The migration process continues if you navigate away from the Migrate Data page.

Migrating data using the PC Client

About this task

Use this procedure to migrate or merge data created using a previous version of CMS to the database of another CMS server using the same version of the software or a newer version of the software.

Before you begin

To migrate System Administration data or Agent and Call Center Administration data, CMS must be in single-user mode. For more information, see [CMS operational states](#) on page 293.

Procedure

1. From the Controller window, navigate to **Tools > System Setup**.

CMS Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **R3 Migrate Data**.
3. Click **OK**.

For a definition of the R3 Migrate Data options, see [Migrate Data page descriptions](#) on page 307.

4. Enter a value in the **Device Name** field.

To list all devices on the system, select **Actions > List devices**.

5. Select one of the following data type options:

Caution:

Attempting to migrate Agent and Call Center Administration data more than once might cause serious errors from which recovery is difficult. Performing the migration of this data a second time can result in the corruption of the password tables. To do a second migration of ACD administration data, do a second setup of the CMS software.

- **System Administration data (single-user required)**
- **Agent/Call Center Admin data (single-user required)**
- **Historical data**

6. Enter a value in the **Stop Date** field.
7. Enter a value in the **Stop Time** field.
8. In the **Specify ACD(s) to migrate** group, select one of the following options:

- **All ACDs**
- **Single ACD**

9. From the menu bar, select **Actions > Run**. The **Run** menu item appears only if the settings for **Data Collection** and **CMS State** are appropriate for the type of migration selected.

CMS begins the migration process. The **Status** field reports the progress of the migration.

Migrate Data page descriptions

The following table describes the key options on the Migrate Data page:

Name	Description
Device Name	The name of the backup device containing the data. Select the device to use for the migration.
Data Type: System Administration data (single-user mode required)	When you select this option, the following data is migrated: • Report GEM files (historical) • Report GEM files (real-time) • Shortcut settings for CMS • CMS users • Timetable settings • Database items • Feature access settings, timetables, schedules, and associated tasks from the User Permissions subsystem • Historical and real-time custom reports • Menu and interface settings for the CMS terminal interface • Printer parameters for the CMS printer
Data Type: Agent/Call Center Admin data (single-user mode required)	When you select this option, the following data is migrated: • ACD profiles - VDN profiles • Agent trace - agents being traced, trace data • Agents - shifts, groups • Dictionary - synonyms • Exceptions - agent admin, link data, malicious call trace, split admin, splits, split profile, trunk group admin, VDN admin, vector admin • User permissions - ACD access, split/skill access, trunk groups access, VDN access, vector access • Forecast - current day report, current day configuration, call handling profiles, costs profiles, data storage allocation, special day admin, manager status, trunk group profiles

Table continues...

Name	Description
Data Type: Historical data	When you select this option, the following data is migrated: • Exceptions - agent data, split access, trunk groups, trunk group access, VDN data, vector data • Historical reports - agent activity, agent login/logout, daily agent data, daily call work codes data, daily splits data, daily trunk groups data, daily trunk groups data, daily trunks data, daily VDN data, daily vector data, intrahour agent data, intrahour agent login-logout data, intrahour call work code data, intrahour split data, intrahour trunk group data, intrahour trunk data, intrahour VDN data, intrahour vector data, monthly agent data, monthly call work code data, monthly split data, monthly trunk group data, monthly trunk data, monthly VDN data, monthly vector data, weekly agent data, weekly call work code data, weekly split data, weekly trunk group data, weekly trunk data, weekly VDN data, weekly vector data • Forecast - daily split data, daily trunk group data, special day split data, interval split data, interval trunk group data
Stop Date	Migration data is recorded until this date. The migration process does not migrate data collected after the date specified.
Stop Time	Migration data is recorded until the time specified. Data is not collected after the specified stop date and time. The default stop time is 11:59 PM.
Specify ACD(s) to migrate: All ACDs	Data is migrated for each ACD. For example, data for ACD1 on the backup device is used for ACD1 on the new CMS.
Specify ACD(s) to migrate: Single ACD	You must specify the ACD you want to migrate from and the ACD you want to migrate to. For example, to migrate data from ACD1 on the backup device to ACD4 on the new CMS, enter 1 in the from field and 4 in the to field.

Chapter 11: Maintaining CMS

Maintaining a CMS server consists of routine tasks such as backing up data, checking the connection to the ACD switch, and viewing the maintenance error log.

 Note:

Some CMS maintenance operations are done using the `cmsadm` or `cmssvc` commands, and some are available when using the CMS Supervisor interface.

This chapter describes how to do the following:

- Reboot your CMS server regularly
- Back up your data
- Restore your data
- Administer backup and restore devices
- Administer printer names and options
- Administer report properties
- Monitor the data connection between the CMS server and the switch
- View the measurement status of an ACD
- View the status of archiving
- View the status of a firewall if administered
- View the status of feature licensing
- Administer LDAP integration

Periodic reboot best practices

Avaya recommends that you reboot your CMS server once every three months for preventative maintenance reasons. This periodic reboot helps to minimize the risk of a system failure. It lessens the possibility of your system being adversely impacted by anomalies such as memory leaks, packet loss, unreleased file locks, data inconsistency, data corruption, and storage space fragmentation. Rebooting your CMS server should not take longer than 10 minutes and should be done when the CMS server load is low.

CMS supports HA, which provides an uninterrupted data stream between the communication server and two CMS servers. If you use HA, reboot each CMS server at a different time to prevent data loss.

Data backups

There are two types of data backup available for CMS:

- CMSADM backup
- Maintenance backup

CMS supports backups to multiple backup devices. You cannot run simultaneous backups of any type, even if multiple backup device types are administered.

CMS can back up data and restore data while data collection remains on. Backups help to minimize data loss. When a CMSADM backup starts, new login attempts from CMS Supervisor or the ASCII interface are blocked.

CMSADM backups save all local file systems, including system files and programs and CMS programs. Perform CMSADM backups after provisioning CMS or after performing an upgrade.

CMS maintenance backups save administration and historical data and the CMS data for each ACD. Avaya recommends that you do full maintenance backups weekly and incremental maintenance backups daily. You can perform maintenance backups in CMS Supervisor. A maintenance restore of CMS system administration data or ACD administration data requires CMS to be in single-user mode.

Caution:

If you do not perform regular backups of your data and you have a system failure, data is lost and cannot be recovered. More frequent backups increase your chances of not losing data. It is up to you to determine how much data loss you can tolerate if you choose not to back up your data more frequently.

CMSADM backups

Perform a CMSADM backup from the command line interface. You cannot perform CMSADM backups from CMS Supervisor.

Back up your system data onto a network mount point. Note that other backup options, such as a USB storage device, are not supported in virtual environments. The CMSADM backup process backs up the following data:

- Operating system files and programs.
- CMS programs.
- Non-CMS customer data on the computer.

The CMSADM backup does not save CMS database tables. For complete data recovery, both CMSADM and maintenance backups are required.

Calculating data space requirements for CMSADM backups

About this task

The command described in this procedure provides a snapshot of the current CMS disk space usage. Run additional checks periodically to see if your storage needs have changed to ensure you have enough backup space.

Procedure

1. Log in to the CMS command line interface with root privileges.
2. Run `df -Th` to get a snapshot of the current disk space usage on the CMS server.

Information such as the following is displayed:

Filesystem	Type	Size	Used	Avail	Use%	Mounted on
devtmpfs	devtmpfs	7.7G	0	7.7G	0%	/dev
tmpfs	tmpfs	7.7G	4.0K	7.7G	1%	/dev/shm
tmpfs	tmpfs	7.7G	105M	7.6G	2%	/run
tmpfs	tmpfs	7.7G	0	7.7G	0%	/sys/fs/cgroup
/dev/sda2	ext4	9.8G	2.4G	6.9G	26%	/
/dev/sda12	ext4	16G	540M	15G	4%	/tmp
/dev/sda8	ext4	2.9G	268M	2.5G	10%	/var
/dev/sda1	ext4	545M	187M	319M	37%	/boot
/dev/sda13	ext4	12G	1.1G	11G	10%	/opt
/dev/sda3	ext4	9.8G	971M	8.3G	11%	/cms
/dev/sda7	ext4	32G	96K	30G	1%	/export/home
/dev/sda9	ext4	2.0G	36K	1.9G	1%	/var/tmp
/dev/sda10	ext4	2.0G	22M	1.8G	2%	/var/log
/dev/sda6	ext4	86G	5.5G	77G	7%	/storage
/dev/sda11	ext4	9.8G	4.5M	9.3G	1%	/var/log/audit
tmpfs	tmpfs	1.6G	0	1.6G	0%	/run/user/0

3. Add the disk space from the Used column for all `ext4` file systems, except for the `/storage` and `/tmp` directories.
4. Calculate the space you need.

The example in the following table shows the used space for the relevant `ext4` file system directories:

Directory	Used space
/	1.6 GB
/boot	106 MB
/var	240 MB
/export/home	49 MB
/opt	1.8 GB
/cms	354 MB
Total: 4.15 GB	

Performing a CMSADM backup

About this task

A file system backup option is available when you run the `cmsadm` command. Ensure that you back up your CMS data to a network mount point. Tape drives are not supported with the latest CMS releases and USB storage device backups are not supported in virtual environment deployments.

Procedure

1. Log in to CMS with root privileges.
2. Run `who -r` to verify that your operating system is in multi-user mode.
The command output should display run-level 2 or 3.
3. Run `cmsadm` to display the CMS Administration Menu.
4. Enter the number associated with the **backup** option.
5. When prompted to choose a backup device, enter the number associated with the **Other** option.
Do not select the tape option. You should use a network mount point for the backup process.
6. Enter the directory path for the network mount point you are using for the backup.

After the backup has been written, it is verified and CMS displays a message such as the following:

```
xxxxxxx blocks
Backup Verification
xxxxxxx blocks
WARNING: A CMS Full Maintenance Backup in addition to this cmsadm backup
must be done to have a complete backup of the system. . . . .
Backup file is located at /xxx/CMSADM-<CMS load name>-<date-time>-<machine name>
```

Maintenance backups

Maintenance backups are used to back up and restore CMS data, including database tables that are not backed up with the CMSADM backup process.

To perform a maintenance backup, navigate to **Administration > Maintenance** in CMS Supervisor. You can do full and incremental backups of CMS historical and administration data.

You can back up the data immediately or you can set up scheduling.

Scheduling for backing up data

You can set up scheduling to back up data in the Web Client. Scheduling is useful if you want to back up the data at a particular time.

Maintenance backup considerations

The maintenance backup process does not back up CMS software, operating system files, or non-CMS customer data on the system. For complete data recovery, both CMSADM and maintenance backups are required.

Consider the following before performing a maintenance backup:

- Backups run in the background. You can navigate away from the Backup Data page without affecting the backup.
- Running backups during archiving can cause performance problems. Run backups before or after the archiving process.

Calculating data space requirements for CMS full maintenance backups

Procedure

1. Log on to Linux as *root*.

Important:

- If using a remote connection, you cannot directly log on as *root*. Instead, log on using an administered CMS user ID and then use `su - root` to log on with root privileges.

2. Run the following command to set the Informix environment: `./opt/informix/bin/setenv`

3. Run `onstat -d`

4. Use the output generated from running this command to estimate how much database space is required for a CMS full maintenance backup. The data in this table is dynamic and changes as database space is used.

Note:

- Bytes to GB conversion factor = 1,073,741,824.
- Full Maintenance Backup compression ratio = 30 (approximation). The `onstat -d` command gives a current snapshot of disk space usage of the CMS server.
- You must run additional checks periodically to see if your storage needs have changed to ensure that you have enough backup space.

Performing a maintenance backup in the Web Client

About this task

When performing a maintenance backup in CMS Supervisor, you can choose which data you want to back up. You can perform the backup for all real ACDs or for the current ACD only. Note that this procedure does not apply to pseudo ACDs.

Procedure

1. Navigate to **Administration > Maintenance > Back Up Data**.

2. Select the backup device you want to use from the **Device Name** list.
3. Select one of the following ACD options:
 - **All ACDs**: To back up data from all ACDs.
 - **Current ACD**: To back up data for the current active ACD.
4. Use the check boxes to specify the data to back up. From the Data to back up area, The **Data to back up** check boxes, by default, are all selected. If you do not want to back up all data types, clear the types of data you do not want to be backed up.

By default, all check boxes in the Data to back up area are selected. If you do not want to back up all data, you can clear some of the check boxes. For a description of the available check boxes, see [Backup Data page descriptions](#) on page 315.

5. Do one of the following:
 - Click **Run** to start the backup immediately.
 - Click **Schedule** to set up scheduling. For more information about scheduling, see the sections under [Scheduling for administration jobs](#) on page 403.

At the top of the page, you see the estimated size of the backup. The status indicates what is currently being backed up.

Doing a maintenance backup using the PC Client Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
2. Click the **Operations** tab.
3. Depending on if you want to back up a single ACD or all ACDs, choose one of the following steps:
 - To back up a single ACD, enter the ACD identification in the **ACD** field.
 - To back up all ACDs, make sure no ACDs are selected in the **ACD** field.
4. Select **Backup Data** in the **Operations** list.
5. Click **OK**.
Supervisor displays the Backup Data window.
For a definition of the Backup Data options, see [Backup Data page descriptions](#) on page 315.
6. In the **Device Name** field, verify that the correct backup device is displayed. If you need to select another device, select **List devices** from the **Actions** menu.
7. If your device is tape, ensure that the **Verify tape can be read after backup?** check box is selected.

It is recommended that you check the tape backup for readability. When the tape is verified, a message displays in the **Status** field. If the tape cannot be read, a message

displays in the **Error name** field. See [Common backup and restore error messages](#) on page 316 for information on additional error messages you may receive. If your device is a non-tape device (USB storage device or network), this check box is ignored.

8. In the **ACD(s) to back up** field, select one of the following options:

- The **All ACDs** option backs up data from all real ACDs (that is, not pseudo-ACDs).
- The **Current ACD** option backs up data from the ACD that is displayed in the bottom right corner of the Backup Data window.

9. The **Data to back up** check boxes, by default, are all selected. If you do not want to back up all of these data types, clear the types of data you do not want to be backed up.

10. From the **Actions** menu, select **Run**.

The backup process begins. When the backup process is complete, CMS Supervisor displays an acknowledgment window.

If you have selected “Tape” as your backup device and your backup requires more than one tape, you receive a message telling you to mount another tape to complete the backup.

11. When the backup completes, remove and label the tape(s) if your backup device is tape.

Backup Data page descriptions

To perform a maintenance backup, navigate to **Maintenance > Back Up Data**. This page displays status information and provides options for setting up the backup. Check boxes are also available to specify the data you want to back up. The following table describes the options on the Backup Data page:

Option	Description
Status information fields:	
Backups completed today	This status information field shows the number of backups completed for the current day.
Status	This status information field shows the status of the current or most recent backup and what is currently being backed up.
Errors	This status information field shows any errors found in the backup.
Device and ACD options:	
Device Name	Use this drop-down list to change the backup device.
ACD(s) to back up	Specify whether you want to perform a backup for all ACDs or for the current active ACD only.
Check boxes to select data to back up:	

Table continues...

Option	Description
Local System administration data	Select this check box to back up IP addresses, port numbers, and other data configured during installation.
CMS System administration data	Select this check box to back up user permissions, feature access permissions, additional main menu data, timetables, printer administration, default values, color choices, and custom report definitions. Note that custom report definitions does not include the data associated with custom reports.
ACD-specific administration data	Select this check box to back up call work code administration data, VDN administration data, data storage allocation information, exception administration data, agent trace data (historical list of agents traced), and ACD-specific Dictionary names.
Historical data	Select this check box to back up the historical data stored in the CMS database. If you select this check box, you must specify whether you want to perform a full or incremental backup. • Full: Includes data for all periods in the historical database. You must perform a full backup before the first incremental backup. Avaya recommends that you perform a full backup of your system periodically (for example, once a week). • Incremental: Includes the CMS data recorded since the last backup (incremental or full) was completed. Only the historical data can be stored incrementally. Administration data is stored in full.
Non-CMS data	Select this check box to include all data from Informix tables with names that start with "c_". The table definitions for non- CMS Informix tables are not backed up because a CMSADM backup captures these tables.
Specific tables	Select this check box to back up data from specific data tables. When you select this check box, you see table names and descriptions. Select the check boxes next to the tables you want to include in the backup.

Common backup and restore error messages

Common error messages and their solutions are described as follows.

CMS cannot access the specified device**Solution**

Enter a new device name.

The volume mounted is bad (corrupt)**Solution**

If the mounted volume is corrupt, mount a new volume.

The volume mounted contains CMS data that you might not want to overwrite**Solution**

Mount a different volume if you do not want to overwrite the data on the volume in the drive.

The volume mounted is the last backup volume**Solution**

Mount a different volume. CMS does not let you overwrite your last backup.

The volume mounted has errors**Solution**

Mount another volume.

A table cannot be backed up**Solution**

You must either skip the table and continue or cancel the backup.

Considerations when backing up or restoring data

Avaya recommends that you back up your CMS system data monthly and your CMS ACD data daily. Running system backups is not service affecting, but the backups impact the performance of the CMS system. Therefore, ensure that you run backups when CMS system activity is low.

** Caution:**

If you do not perform regular backups of your data and you have a system failure, data is lost and cannot be recovered. More frequent backups increase your chances of not losing data. It is up to you to determine how much data loss you can tolerate if you choose not to back up your data more frequently.

CMS Supervisor provides options for restoring or migrating data. You can restore data from **Maintenance > Restore Data** when the CMS version on the backup media is the same as the CMS version installed on the system. If the CMS versions are different, you must migrate data instead. To migrate data, navigate to **System Setup > Migrate Data**. For example, if the CMS version on the backup media is r21ab.g and the CMS version installed on the system is r21ab.g, the data can be restored. If the CMS version on the backup media is r21ab.c and the CMS version installed on the system is r21ab.g, the data must be migrated.

Factors that impact backup and restore times

The amount of time it takes to back up or restore data depends on various factors. These factors include:

- Amount of data: An increase in the amount of data causes an increase in the amount of time it takes to back up or restore the data. Some factors that increase the amount of data being stored are:
 - Number of items being measured: More data is generated if you measure 100,000 agent skill pairs instead of 10,000.
 - Number of days information is stored: The greater the data storage time, the greater the amount of data to be backed up or restored. When CMS reaches the threshold for data storage, the system deletes the oldest record to accommodate the newest record. You can store the data for 370 days.
 - Interval size: Shorter intervals generate more data. A 15-minute interval generates significantly more data than a 60-minute interval.
- System load: Processes that require a large number of system resources slow down the CMS system. Backing up data requires a large amount of system resources. Additional processes that require a large amount of system resources are:
 - Running reports: Running a single large report or multiple smaller reports uses a large amount of system resources.
 - Archiving data: Archiving a large amount of data uses a large amount of system resources.
- The device you are backing up to can also affect the time the backup takes. For the latest CMS releases, you should be using a network mount point for backups. Consider a backup strategy such as the following:
 - Perform full backups only once a week.
 - Perform incremental backups every other day, three or four times a week.

For example, you might want to perform your full backup on Saturday nights, and your incremental backups on Mondays, Wednesdays, and Fridays.

Best practices for reducing backup and restore times

If you do not take steps to optimize your CMS backup and restore times, you might experience performance issues. Your CMS system performance drops if the backup continues to run when call center activity increases. Due to higher capacity limits and fewer database restrictions, the maintenance backup time can take longer with each new CMS release. In rare extreme cases, maintenance backups could take more than 24 hours.

To reduce the amount of time it takes to backup or restore data, you can:

- Select the maximum interval time that meets your data collection needs.
- Select the minimum data storage times that meets your data collection needs for all the historical database tables.

- Run reports when the CMS system is not actively backing up or restoring data.
- Schedule each ACD to back up at a different time.
- Schedule routine backups to occur at a different time than data archiving.
- Schedule routine backups to occur when CMS system activity is low.
- Use the binary backup method. A binary backup does not support table level restore and data migration. This backup method is also a good alternative for disaster recovery.
- Upgrade your CMS system to add additional memory and CPUs.

Best practices for maintaining your storage device

Tape drives are no longer supported with the latest CMS releases and USB storage devices are not supported in a virtual environment. Therefore, you should be using a network mount point as your backup device. You must keep enough free space on your device for scheduled maintenance backups. This means that you must periodically check the network mount point for available space and remove older backup files to increase the storage space. Ensure that you include the network directory in the system backups of your company's non-CMS servers.

Consider the following best practices for maintaining your backup storage device:

- Do not store CMSADM and maintenance backup files on the same network mount point. Create separate network directories for your CMSADM backups with adequate storage for at least two backups.
- Ensure that your network directory has enough storage for at least two full maintenance backups and the accompanying week's worth of incremental backups. If you are backing up multiple servers, increase the storage accordingly.

Backup file used to restore data

On the Restore Data page in the Maintenance subsystem, you can choose to restore from the last backup. CMS uses the following logic to determine which backup to use:

- If found, CMS uses the backup file labeled with the latest full backup for the given server.
- If the latest cannot be found, the previous full backup is used.
- If no full backups can be located for the given server, the latest incremental backup is used.

List to manage which backup is used

To control which backup file is used, do not enable the option to restore from the last backup. Instead, create a file called "restore_list" on your storage device. Ensure that it contains the names of the files you want to restore from. These files must be listed in order, starting with the first backup file you want to restore from.

You can run a command to see the CMS maintenance backups on your server. For example, if maintenance backups on server "finch" begin on October 4 with a full backup followed by an incremental backup on October 6, October 8, and October 10, you can run the `ls -rt *finch*` command to see the backup files in your backup storage area. To create a list of these file names in the "restore_list" file, run the `ls -rt *finch* > restore_list` command.

Performing a binary database backup to a network device

About this task

You can back up the entire database in binary form. If you perform a binary backup, you cannot restore system data, call center administration data, or historical data individually.

The CMS server can be configured to use a network mount point for the binary backup and restore. The binary backup writes backup data to the network device. The speed of the network backup depends on your network bandwidth.

This procedure requires knowledge and experience with network file system mounts. You can find information about extracting data to a network mount point in *Upgrading Avaya Call Management System*. Additional information is also available in *Maintaining and Troubleshooting Avaya Call Management System*.

Procedure

1. Create a mount point and mount the network file system to the CMS server.
2. Modify `/etc/vfstab` to make sure your network file system can survive a reboot.
3. Run the following `touch` command to create an empty file:

```
touch /<mount_point_path>/<binary_backup_filename>
```

For example, run the following command:

4. Run the following command to perform the backup:

```
/cms/install/bin/db_backup /<mount_point_path>/<binary_backup_filename>
```

Example

The following example shows the commands for mounting an NFS on Linux:

```
mkdir /nfs
mount -o vers=3 <machine_name>:/cms_db_backup /nfs
touch /nfs/cms_db_backup
/cms/install/bin/db_backup /nfs/cms_db_backup/<binary_backup_filename>
```

Adding a full maintenance backup timetable for an ACD in the PC Client

About this task

Timetables are supported in the PC Client. You can set up a full maintenance backup timetable for a specific ACD.

Procedure

1. Log in to CMS.
2. From the **Main Menu**, press F4 to access CMS timetables.
3. Select **Timetable**.
4. Press **Ctrl+Z** to clear out the entries in the form.
5. Enter `fullBackup` in the **Timetable** name field.

6. Press `Enter`.
7. Select **Find one**.
8. Press `Enter`.
9. Rename the full backup timetable to identify the ACD being backed up.
For example, enter the name `acd1fullBackup` for ACD 1.
10. Press `Enter`.
11. Enter the letter `a` to highlight the **Add** item.
12. Press `Enter`.
13. Press `F3` to access the **Options** menu.
14. Enter the letter `o` to highlight the **Options** item.
15. Press `Enter`.
16. Enter the letters `cu` to highlight the **Current ACD** item.
17. Press `Enter`.
18. Enter the number of the ACD for which the timetable is being created.
19. Press `Enter`.
20. Enter the letter `m` to highlight the **Modify** item.
21. Press `Enter`.
22. Press `F5` to exit the **Options** menu.
23. Enter the letter `m` to highlight the **Maintenance** item in the main menu.
24. Press `Enter`.
25. Ensure that the **Back Up Data** item is highlighted and then press `Enter`.
26. Use the down arrow key to move to the **ACD(s) to back up** field.
27. Enter `x` in the **Current ACD** field.
28. Press `Enter`.
29. Enter the letter `r` to select the **Run** option.
30. Press `Enter`.
31. Press `F5` to exit the **Timetable** menu.
32. Press `F4` to open the **Timetable/Shortcut** item.
33. Ensure that **Stop** is highlighted and press `Enter`.
If **Stop** is not highlighted, enter the letters `st` to highlight it.
34. Enter `y` when prompted to save the changes and then press `Enter`.

The timetable is created and the Timetable page is displayed.

35. **(Optional)** Update the dates and times when the timetable will run and select **Modify** to save your changes.
36. Press **F5** to exit the **Timetable** menu.

Options for restoring data

Navigate to **Maintenance > Restore Data** to restore CMS data that has been lost due to system failure, disk crashes, or power outages. You can restore all CMS data files that you previously backed up. Alternatively, you can select which ACDs and CMS data to restore.

An automatic and manual restore process is available:

- The automatic process restores all CMS data files from your last backup.
- The manual process restores specific CMS data files. You can control which data is restored. This is useful when only a select number of database tables need to be restored.

Before restoring data

Data must be backed up before it can be restored. To ensure the safety of your data, you should frequently back up your system.

Consider the following before restoring data:

- Ensure that the data collection and CMS states are set as follows:

Data backup type	Data collection (on or off)	CMS state (user mode)
Local system administration data	Turn off	Single-user mode
CMS system administration data	On or off	Single-user mode
ACD system administration data	On or off	Single-user mode
Historical data	On or off	Single-user mode or multi-user mode
Non-CMS data		
Specific tables		

- The restore process is run in the background. The Restore Data page shows the status of the restore process as it is performed.
- When migrating or restoring a non-LDAP user from a maintenance backup, and the “logid” (logon ID) for a user does not exist in `/etc/passwd`, the user is created as a new logid. That logid requires password administration just as if the user was created as described in [User administration](#) on page 173.

When this happens, the migration and restore logs contain messages similar to the following examples:

```
- /cms/maint/r3mig/mig.log
```

```
INFO: New UNIX user normusr1: name, room and telephone will not be
migrated.
```

```
- /cms/maint/restore/rest.log
```

```
Created UNIX login 'normusr1'.
```

```
Warning: Name, Telephone, and Room will not be restored for
normusr1.
```

Automatically restoring data in the Web Client

About this task

Use the automatic restore process to restore all CMS data files from your last backup.

Procedure

1. Navigate to **Administration > Maintenance > Restore Data**.
2. Select the restore device from the **Device Name** list.
3. Under the Restore from last backup area, select **Yes**.
4. Click **Run** to start the restore process.

The status of the restore process is displayed. You see which database tables are being restored.

Manually restoring data in the Web Client

About this task

Use the manual restore process to specify the data to restore. In this procedure, you will not restore data from the latest backup. The manual restore process stops if severe errors occur. Do not click **Cancel** during the restore process. Canceling a restore leaves the already restored data in the tables, which can result in an abnormal database state.

Note that you can only restore local system administration data once. A second attempt corrupts the data.

Procedure

1. Navigate to **Administration > Maintenance > Restore Data**.
2. Select the restore device from the **Device Name** list.
3. Under the Restore from last backup area, select **No**.
4. In the **Start Date** field, enter the oldest date to be included in the restore.
5. In the **Start Time** field, enter the time to start restoring data.

Use the format HH:MM and specify AM or PM.

6. In the **Stop Date** field, enter the end date to be included in the restore.
7. In the **Stop Time** field, enter the time to stop restoring data in the HH:MM format.
8. In the **ACD(s) to restore** options, select **All ACDs** or **Current ACD**.
9. Select the check boxes corresponding to the data you want to restore.

If you select **Specific tables**, you cannot restore any other information simultaneously. This includes:

- Local system administration data: This data can only be restored once.
- CMS system administration data
- ACD system administration data
- Historical data

10. Click **Run** to start the restore process.

Doing an automatic restore using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Select **Restore Data** in the **Operations** list.
4. Click **OK**.

Supervisor displays the Restore Data window.

The **Status** field shows the status of the current restore or a previous restore if one has taken place.

The **Error name** field shows any errors found during the restore.

5. Check the **Device Name** field to make sure the correct backup/restore device is selected.

If you want to use another backup/restore device, select **Actions > List devices**. Enter the correct backup/restore device name in the **Device Name** field.

This field defaults to the device named during installation.

6. Select the **Restore from the latest backup?** check box.
7. From the **Actions** menu, select **Run**.

The system notifies you which volumes to mount to restore the data. At the end of every restored volume, the tables that have been fully or partially restored are displayed. If your device is "Other", then the backup file is automatically located for you. You only need to press the **Continue** key to perform the requested restore.

If the system asks for a tape that you cannot provide, you must cancel the restore process. The restore can be rerun if the tape is found.

Doing a manual restore using the PC Client

About this task

Important:

The manual restore stops when severe errors occur or when you tell it there are no more volumes to restore. Select **Stop** to tell the restore process that you are finished. Do not select **Cancel** since it implies an abnormal termination. Canceling a restore leaves the data that has already been restored in the tables, which may result in the database being in an abnormal state. You receive an acknowledgment window asking if you are sure you want to cancel the restore.

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Select **Restore Data** in the **Operations** list.
4. Click **OK**.

Supervisor displays the Restore Data window.

The **Status** field shows the status of the current restore or a previous restore if one has taken place.

The **Error name** field shows any errors found during the restore.

5. Check the **Device Name** field to ensure that the correct backup/restore device is selected.

If you want to use another backup/restore device, select **Actions > List devices**. Enter the correct backup/restore device name in the **Device Name** field.

This field defaults to the device named during installation.

Important:

If your backup device is tape, do not select the **Restore from the latest backup?** check box. A manual restore accepts any tape you mount as long as the data on the tape corresponds with the requested data.

6. In the **Start Date** field, enter the oldest date to be included in the restore by using one of the following methods:
 - Enter the date in the mm/dd/yy format.
 - Use the drop-down calendar to select a date.
 - Enter the date in relative format; for example, 0 for today and -1 for yesterday.
7. In the **Start Time** field, enter the time you want to start restoring data. Use the format of hh:mm XM when entering the time where hh is hours, mm is minutes, and XM is AM or PM.

If you wanted to restore data starting at 1:15 AM, you would enter 01:15 AM

If AM or PM is not specified, a 24-hour clock is assumed.

8. In the **Stop Date** field, enter the most recent date to be included in the restore.
9. In the **Stop Time** field, enter the time you want to stop restoring data. Use the format of hh:mm XM when entering the time.
10. In the **ACD(s) to restore** options, select either **All ACDs** or **Current ACD**.
11. In the **Data to restore** group, select the types of data you want to restore.
12. If you do not select **Specific tables**, go to Step [16](#) on page 326. Otherwise, select **Actions > Select tables**.

Supervisor displays the Restore Data - Select tables window.

If you are performing the **Specific tables** restore, you cannot restore any other information at the same time. This includes:

- Local system administration data - This data can only be restored once. A second attempt corrupts the data.
- CMS system administration data
- ACD system administration data
- Historical data

13. Select the tables you want to restore.
14. From the **Actions** menu, select **Modify**.
15. Close the Restore Data - Select tables window to return to the Restore Data window.
16. From the **Actions** menu, select **Run**.

The system notifies you which volumes to mount to restore the data. At the end of every restored volume, the tables that have been fully or partially restored are displayed. If your device is "Other", then the backup file is automatically located for you. You only need to press the **Continue** key to perform the requested restore.

If the system asks for a tape that you cannot provide, you must cancel the restore process. The restore can be rerun if the tape is found.

Restoring the database from a binary backup

The binary backup does not back up the CMS software, operating system files or non-CMS customer data on the system. For complete data recovery, both a CMSADM restore and a binary restore are required. See *Maintaining and Troubleshooting Avaya Call Management System* for instructions on how to perform a CMSADM restore and a binary restore.

Backup and restore devices

You can add and manage backup and restore devices from the Backup/Restore Devices page. Assign a name and description to the full device path. The device name is used for data backup, data migration, data restore, and for loading a pseudo-ACD.

Tape backups are no longer supported and USB storage devices are not supported in a virtual environment. Therefore, you should be using an NFS mount point.

Adding a backup and restore storage device in the Web Client

About this task

For the latest CMS releases, use a network mount point to extract data. After setting up this storage device, use this procedure to add it to CMS Supervisor. You must add a storage device to perform backup, restore, and migration procedures.

Before you begin

You must configure the network mount point device and ensure that it is accessible from the CMS server.

Procedure

1. Navigate to **Administration > Maintenance > Backup/Restore Devices**.
2. Click **Add Backup/Restore Device** to add a new storage device.
3. In the **Device Name** field, enter a name for the backup/restore device.

You will select this device name when performing backup, restore, and migration procedures in CMS Supervisor.

4. In the **Path** field, enter the full path to access the device.

The device path for the network mount point must exist on the CMS server and the device must be mounted.

5. In the **Description** field, enter any additional information to help identify the device.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

6. In **Device Type**, select **Other** for the network mount point device.

Tape is no longer supported in the latest CMS releases.

7. Click **OK** to save your changes.

Modifying a backup and restore storage device in the Web Client

About this task

You can modify the path and description for an existing backup/restore device. The device name is read only and cannot be changed.

Ensure that you provide the full path for the device. When using a network mount point, the device path must exist on the CMS server and the device must be mounted.

Procedure

1. Navigate to **Administration > Maintenance > Backup/Restore Devices**.

CMS Supervisor displays the backup and restore devices currently administered.

2. Click  next to the item you want to modify.

The Modify Item window is displayed.

3. In the **Path** field, enter the full path for the device.

4. **(Optional)** Revise the information in the **Description** field.

You can enter up to 50 characters. This field cannot contain the pipe (|) symbol, a semicolon, or double quotes.

5. Administer the following options:

- The **Device Name** field is display-only. You cannot change the name.
- In the **Path** field, enter the full operating system path to access the device.

See the “Accessing devices” section in your operating system’s Administrator’s Guide for more information about devices and paths. If the device type is **Other**, its system path cannot be located on the CMS disk. In addition, the USB storage device or network must be mounted.

- In the **Description** field, enter any additional information to help identify the device.
- For **Device Type**, select either **Tape** or **Other**. **Tape** includes all currently supported tape drives. **Other** includes the USB and network type backup devices.

6. Click **OK** to save your changes.

7. Click **OK**.

CMS Supervisor displays an updated list of items.

Deleting a backup/restore storage device in the Web Client

About this task

When you delete a storage device, you can no longer use it to perform backup, restore, and migration procedures in CMS Supervisor.

Procedure

1. Navigate to **Administration > Maintenance > Backup/Restore Devices**.

CMS Supervisor displays the backup and restore devices currently administered.

2. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

3. Click **Yes** to complete the change.

Viewing backup or restore devices using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
2. Click the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Click **OK**.
Supervisor displays the Backup/Restore Devices window.
5. From the **Actions** menu, select **Find one**.
Supervisor displays the information for the first device.
6. If more than one match is found, go to the **Actions** menu, and select **Next**. Repeat this step until all devices have been displayed.

Listing all backup and restore devices using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
2. Click the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Click **OK**.
Supervisor displays the Backup/Restore Devices window.
5. From the **Actions** menu, select **List all**.
Supervisor displays a list of all devices.

Adding a backup or restore device using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
2. Click the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Click **OK**.
Supervisor displays the Backup/Restore Devices window.

5. In the **Device Name** field, enter the name of the backup/restore device.

If you want to refer to your backup/restore device as `ddrive1`, enter `ddrive1` in the **Device Name** field.

6. In the **Path** field, enter the full operating system path to access the device.

See the “Accessing devices” section in your operating system’s Administrator’s Guide for more information about devices and paths. If the device type is **Other**, its system path cannot be located on the CMS disk. In addition, the USB storage device or network must be mounted.

7. In the **Description** field, enter any additional information to help identify the device.

The **Device Name** field now has the option of **Tape** and **Other**. **Tape** includes all currently supported tape drives. **Other** includes the USB and network type backup devices.

8. From the **Actions** menu, select **Add**.

The device is defined through CMS and can be used for backup and restore operations.

Modifying a backup or restore device using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.

3. Select **Backup/Restore Devices** in the **Operations** list.

4. Click **OK**.

Supervisor displays the Backup/Restore Devices window.

5. Perform one of the following procedures to select the correct backup/restore device:

- If you know the name of the device, enter the name of the device in the **Device Name** field and then press the `Enter` key.
- If you do not know the name of the device, select **Find one** from the **Actions** menu. If more than one match is found, go to the **Actions** menu, and select **Next**. Repeat this step until the device you want to delete is displayed in the dialog box.

6. Enter the new information in the fields that require modification.

7. From the **Actions** menu, select **Modify**.

The changes made to the device definition are saved.

Deleting a backup or restore device using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Click **OK**.

Supervisor displays the Backup/Restore Devices window.

5. Perform one of the following procedures to select the correct backup/restore device:
 - If you know the name of the device, enter the name of the device in the **Device Name** field and then press the `Enter` key.
 - If you do not know the name of the device, select **Find one** from the **Actions** menu. If more than one match is found, go to the **Actions** menu, and select **Next**. Repeat this step until the device you want to delete is displayed in the dialog box.
6. From the **Actions** menu, select **Delete**.

The specified backup/restore device definition is deleted from the CMS server.

Printer administration

Use the Printer Administration page to set up a printer that can be used by terminals connected to a CMS server. When adding a printer, you can assign a name, description, and other print settings.

Note:

Printers directly connected to CMS servers is a legacy feature that is not supported with new installations.

CMS Supervisor users must use printers that are associated with their own computers.

Considerations for administering a printer

Consider the following items before you administer a printer:

- Printers directly connected to CMS servers is a legacy feature that is not supported with new installations.
- Before you can assign a printer on the Printer Administration page, it must already be set up on the operating system.
- The printer set up as the default printer will receive all terminal requested print jobs, unless otherwise specified.
- If jobs are sent to a printer that is no longer administered, the print job will be sent to the default printer and an error will be logged in the Maintenance Error Log.
- The name of a printer administered on the Printer Administration page can be used by terminal users as the default destination when printing historical reports.

Adding a printer in the Web Client

About this task

After setting up a printer on

Procedure

1. Navigate to **Administration > Maintenance > Printer Administration**.
CMS Supervisor displays the printers currently administered.
2. Click **Add Printer**.
3. In the **CMS printer name** field, enter the name of the new printer.
The name assigned to the printer must be unique from all other installed printers, but it can be assigned the same name it was given during the operating system administration.
4. In the **LP printer name** field, enter the name assigned to the printer when it was administered for the operating system.
5. In the **Description** field, enter any additional information to identify the printer.
6. From the **IBM graphic characters** list, select **Yes** if the printer uses IBM graphic characters.
Otherwise, ensure that **No** is selected.
7. In the **Lines per page** field, enter the number of lines that fit on a page.
The default is 66 lines. CMS formats reports to correspond to the value in this field.
8. From **Print type**, select one of the following options:
 - **Normal**: This is the default setting.
 - **Other**: Select this option to customize the print type. In the corresponding field, enter the specific print type; for example, `pica`, `elite`, or `compressed`.
9. From the **Banners** list, select **Yes** if you want a banner to be printed for every job.
A banner is a cover sheet that identifies the user who requested the print job.
10. Click **OK** to save your changes.

Modifying printer options using the Web Client

Procedure

1. Navigate to **Administration > Maintenance > Printer Administration**.
CMS Supervisor displays the printers currently administered.
2. Click  next to the item you want to modify.
The Modify Item window is displayed.
3. Update one or more of the printer settings.

For a description of the available options, see [Adding a printer in the Web Client](#) on page 332.

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

Deleting a printer using the Web Client

Procedure

1. Navigate to **Administration > Maintenance > Printer Administration**.

CMS Supervisor displays the printers currently administered.

2. Click  next to the item you want to delete.

The Confirm Delete dialog box is displayed.

3. Click **Yes** to complete the change.

Listing all printers using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.

3. Select **Printer Administration** in the **Operations** list.

4. Click **OK**.

Supervisor displays the Printer Administration window.

5. From the **Actions** menu, select **List all**.

Supervisor displays the Printer Administration - List All window.

Adding a printer using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.

3. Select **Printer Administration** in the **Operations** list.

4. Click **OK**.

Supervisor displays the Printer Administration window.

5. In the **CMS printer name** field, enter the name of the new printer.

The name assigned to the printer must be unique from all other installed printers; however, it can be assigned the same name it was given during the operating system administration.

6. In the **LP printer name** field, enter the name assigned to the printer when it was administered in the operating system.
7. In the **Description** field, enter any additional information to identify the printer.
8. If the printer uses IBM graphic characters, select the **IBM graphic characters** check box. Otherwise, leave the check box cleared.
9. In the **Lines per page** field, enter the number of lines that fit on a page.
The default is 66 lines. CMS formats reports to correspond to the value in this field.
10. In the **Print type** options select one of the following choices:
 - Select **Normal** (default setting)
 - Select **Other**. Then, in the corresponding field, enter the specific print type such as `pica`, `elite`, or `compressed`.
11. If you want a banner to be printed for every print job, select the **Banners** check box.
A banner is a cover sheet that identifies the user who requested the print job.
12. From the **Actions** menu, select **Add**.

Modifying printer options using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
 2. Click the **Operations** tab.
 3. Select **Printer Administration** in the **Operations** list.
 4. Click **OK**.
Supervisor displays the Printer Administration window.
 5. Perform one of the following procedures to select the correct printer:
 - If you know the name of the printer, enter the name of the printer in the **CMS printer name** field, and then press `Enter`.
 - If you do not know the name of the printer, select **Find one** from the **Actions** menu. If more than one match is found, go to the **Actions** menu, and select **Next**. Repeat this step until the printer you want to delete is displayed.
-  **Important:**
- You cannot modify the name of a CMS printer. If you want to change a printer name, you must delete the printer and add it again with a new name. See [Deleting a printer using the PC Client](#) on page 335, and [Adding a printer using the PC Client](#) on page 333 for more information.
6. Make changes to any of the fields in the Printer Administration window, except the **CMS printer name** field

7. From the **Actions** menu, select **Modify**.

Deleting a printer using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Select **Printer Administration** in the **Operations** list.
4. Click **OK**.

Supervisor displays the Printer Administration window.

5. Perform one of the following procedures to select the correct printer:

- If you know the name of the printer, enter the name of the printer in the **CMS printer name** field, and then press **Enter**.
- If you do not know the name of the printer, select **Find one** from the **Actions** menu. If more than one match is found, go to the **Actions** menu, and select **Next**. Repeat this step until the printer you want to delete is displayed.

6. From the **Actions** menu, select **Delete**.

If you try to delete a printer that is assigned to users, you will receive a message asking if you still want to delete the printer.

Users assigned to this printer will not have another printer assigned when it is deleted.

Report properties

You can configure report properties in CMS Supervisor or from the ASCII (text) interface.

From the Report Administration page in CMS Supervisor, you can set a timeout value for historical report queries and limit the size of agent groups. These options enable you to impose a system-wide limit on report queries.

The following is a more detailed description of the report properties you can set:

- **Timeout value:** You can impose a specific time limit, in 1 second increments, on historical report queries. If a report query takes more than X seconds to return data from the Informix database, it times out. You can set the timeout range to a value between 3 and 999 seconds. Alternatively, you can select **Never timeout** to enable all historical report queries to run for an unlimited amount of time.
- **Agent group size:** A check box is available to limit the size of an agent group for realtime or historical queries. Clear the check box if you do not want to restrict agent group sizes. If you select this option, the agent group limit is 99 members or less. When this limit is enabled,

you cannot run a realtime or historical report that uses an agent group with 100 or more members.

If you change a setting or set a limitation, the change takes effect the next time a report is run and the limit is imposed on all users.

Report limits apply to standard reports, custom reports, designer reports, and reports run from PC Client timetables. In the case of a report running from a timetable, if the report fails due to the set limits, the error is recorded in the elog. If you want to limit the properties of report queries during certain times of the day, you can create two timetables.

Before administering report properties

- Examine the reports in your query log. Check for historical or realtime reports that use agent groups. Determine whether there are any reports that affect system performance due to the time spent on the Informix database query.
- Decide if you want to limit your historical report queries and what the limit, in seconds, should be.
- Decide if you want to limit the size of agent groups used in agent group reports.

Modifying report properties using the Web Client

About this task

Use this procedure to manage report property settings. No limits are configured by default.

Procedure

1. Navigate to **Administration > Maintenance > Report Administration**.
2. Clear the **Agent groups > 99 members allowed in queries** check box to limit agent group sizes for report queries.

When the check box is selected, there is no limit. When the limit is enforced, you cannot run reports that use an agent group with 100 or more members.

3. Do one of the following depending on whether you want to set a time limit for historical report queries:
 - To set a time limit after which the report query will time out, select **Timeout value for historical report queries** and then enter a timeout value between 3 and 999 seconds.
 - If you do not want to set a time limit, select **Never timeout historical report queries**.
4. Click **Modify** to save your changes.

Modifying report properties from the command line interface

About this task

You can use the ASCII (text) client or command line interface to manage report properties.

Procedure

1. Run the `cms` command to display the Main Menu.
2. Select **Maintenance** and press `Enter`.
3. Select **Report Administration** and press `Enter`.
4. In the **Agent groups > 99 members allowed in queries** field, do one of the following:
 - Enter `n` to limit agent group reports to groups of 99 members or less.
 - Enter `y` to allow all sizes of agent groups in reports.
5. In the **Timeout value for historical report queries** field, do one of the following:
 - Enter `never` if you do not want to impose a time limit.
 - Enter the number of seconds from 3 to 999 to limit historical report queries to a specific time length.

ACD connection status

You can use the Connection Status page to monitor the data link between the CMS server and the ACD system. Communication Manager is an example of an ACD system. You can also view the current status of the application, session, and connection layers of the link between the ACD system and the CMS server.

Viewing connection status in the Web Client

About this task

You can view the connection status for all ACD systems connected to CMS. For a description of the available connection status information, see [Connection status descriptions](#) on page 338.

Procedure

1. Navigate to **Administration > Maintenance > Connection Status**.
CMS Supervisor displays the current connection status for all ACD systems.
2. **(Optional)** Click **Refresh** to update the current connection status.

Viewing connection status of an ACD using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
2. Click the **Operations** tab.
3. Select **Connection Status** in the **Operations** list.

4. Click **OK**.

CMS Supervisor displays the Connection Status window.

5. In the **ACDs** field, enter the name or number of the ACD or ACD Group.

For a description of the connection status information, see [Connection status descriptions](#) on page 338.

6. From the **Actions** menu, select **Find one**.

CMS Supervisor displays the Connection Status window for the selected ACD.

Listing connection status of all ACDs using the PC Client Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.

3. Select **Connection Status** in the **Operations** list.

4. Click **OK**.

CMS Supervisor displays the Connection Status window.

For a description of the connection status information, see [Connection status descriptions](#) on page 338.

5. If the **ACDs** field is not clear, select **Edit > Clear All**.

6. From the **Actions** menu select **List all**.

CMS Supervisor displays the Connection Status - List All window.

Connection status descriptions

The Connection Status page displays the following:

Field	Description	Status Messages
ACD	Displays the number or name of the ACD.	-

Table continues...

Field	Description	Status Messages
Application	Displays status for the application layer of the link between the ACD system and CMS .	waiting session - The application layer is inactive: This is the state of the application layer when the system is first powered on. translation pumpup: CMS is receiving translations from the ACD system. Translations are needed for CMS to correctly track the ACD calls coming from the switch. data transfer: The application layer can receive and transmit data successfully. not collecting data: Data collection has been turned off. You can turn data collection back on from System Setup > Data Collection. CMS System Setup - The link has gone down: The connection link is down. busied out (switch): The link between CMS and the ACD system has been busied out from the switch side, usually to change switch translations.
Session	Displays status for the session layer of the link between the Communication Manager system and CMS.	quiescent: The session layer is inactive. This is the state of the session layer when the system is first powered on. waiting acceptance: The session layer is waiting for the connection layer to become operational and for the remote session layer to accept the session. data transfer: The session layer can now transmit and receive data from the ACD.
Connection	Displays status for the connection layer of the link between the ACD and CMS. Next to the connection status, you see which server is connected (primary or secondary). This information is useful in an HA environment where a secondary server is deployed.	operational: The connection is operational and can transmit information between the ACD and CMS. quiescent: The connection is inactive. This is the state of the connection when the system is first powered on. out of order: Something is wrong with the connection to the ACD. For example, the network connection between the ACD and CMS is not working. waiting session accept: The link is down.
Date/Time	Displays the date/time for the ACD, unless the link to the ACD is down when CMS is brought up. If this happens, CMS uses the operating system time until the link is reestablished.	-

Table continues...

Field	Description	Status Messages
Error	Displays any errors found.	-

About viewing ACD status

The ACD Status page displays information about the current selected ACD, including the number of splits/skills, agents logged in, trunk groups, trunks, VDNs, and vectors (if Call Vectoring is enabled).

Prerequisites for viewing ACD status

To view the ACD status, consider the following:

- The link must be up between the ACD system and the CMS server if you want to view the status of a specific ACD.
- Data collection must be on for the specific ACD.

Viewing ACD status using the Web Client

Procedure

Navigate to **Administration > Maintenance > ACD Status**.

CMS Supervisor displays the status of all connected ACDs.

For information about the fields in the ACD Status window, see [ACD status field descriptions](#) on page 341.

Viewing ACD status using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Highlight **ACD Status** in the **Operations** list.
4. Click **OK**.

Supervisor displays the ACD Status window.

For information about the fields in the ACD Status window, see [ACD status field descriptions](#) on page 341.

5. Perform one of the following steps to enter information in the **ACDs** field:
 - Enter the name or number of the ACD directly into the field.

- Use the history list to select an ACD.
- Use the Browse button to select an ACD.

 Note:

You can also select an ACD Group which will return all the members of that group.

6. From the **Actions** menu, select **Find one**.

Supervisor displays the ACD Status window for the selected ACD.

If you selected an ACD Group, the first member of the group is displayed. View any other member ACDs by using the **Next** and **Previous** buttons.

Listing ACD status using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Highlight **ACD Status** in the **Operations** list.
4. Click **OK**.

Supervisor displays the ACD Status window.

5. From the **Edit** menu, select **Clear All**.
6. From the **Actions** menu select **List all**.

Supervisor displays the ACD Status - List All window.

For information about the fields in the ACD Status window, see [ACD status field descriptions](#) on page 341.

ACD status field descriptions

The ACD Status page displays the following information:

Information	Description
ACD	The ACD name.
Skills	The skills measured by CMS.
Skill members in use	The agent/skill pairs that are currently logged in.
Trunk Groups	The trunk groups measured by CMS.
Trunks	The trunks measured by CMS. Unmeasured trunks are not included.
VDNs	The VDNs measured on the selected ACD.
Vectors	The vectors available for use in the selected ACD.

Table continues...

Information	Description
Agents	The number of agents.
Error name	The errors encountered by the ACD if applicable.

About viewing archiving status

The Archiving Status page shows the status, date, and time of the last archive. You can sort by the archive type (Interval, Daily, Weekly, and Monthly). This page also shows when the next archive is scheduled.

You can use the archiving status information to decide when to turn off data collection or change your archiving times to minimize data loss.

* Note:

The Archiving Status window displays the status for the default time zone archiving for each ACD and the archiving of each time zone set up with Data Summarization Time Zone. If the tenancy feature is turned on and the user has permissions for the given tenant, the user sees the status of the tenant time zone archiving for each ACD.

Viewing archiving status using the Web Client

Procedure

1. Navigate to **Administration > Maintenance > Archiving Status**.

CMS Supervisor displays the current data archiving status for all archiving types, Interval, Daily, Weekly, and Monthly.

2. Change the **Archiving type** options to narrow or widen your view of the archiving status.

Viewing archiving status of a single ACD using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Select **Archiving Status** in the **Operations** list.
4. Click **OK**.

CMS Supervisor displays the Archiving Status window.

5. Perform one of the following steps to enter information in the **ACDs** field:
 - Enter the name or number of the ACD directly into the field.
 - Use the history list to select an ACD.

- Use the **Browse** button to select an ACD.
6. In the **Archiving type** check boxes, clear the archives you do not want to view. If you want to view all archive types, leave the check boxes as check marked and proceed to the next step.
 7. From the **Actions** menu, select **List all**.

CMS Supervisor displays the Archiving Status - List All window.

For more information about the Archiving Status window, see [Archiving status field descriptions](#) on page 343.

 Note:

It is also possible to view the archiving status of all members of a single ACD Group using this procedure. Instead of the name or number of a single ACD, enter the name or number of the ACD Group in the **ACD** field.

Viewing archiving status of all ACDs using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Click the **Operations** tab.
3. Select **Archiving Status** in the **Operations** list.
4. Click **OK**.

CMS Supervisor displays the Archiving Status window.

5. If the **ACDs** field is not clear; go to the **Edit** menu, and select **Clear All**.
6. Select the type of archives you want to view in the **Archiving type** check boxes.
7. From the **Actions** menu, select **List all**.

CMS Supervisor displays the Archiving Status - List All window.

For more information about the Archiving Status window, see [Archiving status field descriptions](#) on page 343.

Archiving status field descriptions

The following table describes the information displayed on the Archiving Status page:

Information	Description
ACD	The name of the ACD.

Table continues...

Information	Description
Tenant	When tenancy is enabled, you see “all” or a specific number. This information indicates whether archiving is done for all tenants or for individual tenants.
Archive Type	Check boxes are available to sort the archive types you want to display. The available archive types are: • Interval (intrahour interval) • Daily • Weekly • Monthly Note that information about the next scheduled archive is not displayed for the Interval archive type.
Status	The archiving status indications are: • Finished: The last archive is complete. • Running: The archive is currently running. • Not Run: The archive has never run.
Date	The date the last archive was completed.
Time	The time the last archive was completed.
Next Scheduled	The date and time of the next scheduled archive. Dates and times will not appear for Interval archiving, which occurs at the end of each intrahour interval. The interval settings are 15, 30, or 60 minutes.
Time Zone	The time zone used for the archiving period. When you see “default”, the master ACD time zone is used.
Tenant Name	This information is displayed for tenancy. It shows the name of the tenant or “all” if archiving is done for all tenants.

Viewing firewall status information in the Web Client

About this task

You can view firewall status information for the IPv4 or IPv6 protocol. Status information is only displayed if the firewall is running.

Procedure

1. Navigate to **Administration > Maintenance > Firewall Status**.
2. From the **Interface Type** drop-down list, select **IPv4** or **IPv6**.

CMS Supervisor displays the firewall status for the selected protocol.

Example

The following example image shows a snippet of the type of information displayed:

Firewall Status

Contact you system administrator for firewall changes

Interface Type

IPV6

IPV6

Chain INPUT (policy ACCEPT)

num	target	prot	opt	source	destination
1	ACCEPT	all		::/0	::/0 state RELATED,ESTABLISHED
2	ACCEPT	all		::/0	::/0
3	ACCEPT	tcp		::/0	::/0 tcp dpt:22
4	ACCEPT	tcp		::/0	::/0 tcp dpt:8443
5	ACCEPT	tcp		::/0	::/0 tcp dpt:50000
6	ACCEPT	tcp		::/0	::/0 tcp dpt:50001
7	ACCEPT	tcp		::/0	::/0 tcp dpt:1556
8	ACCEPT	tcp		::/0	::/0 tcp dpt:13724
9	ACCEPT	tcp		::/0	::/0 tcp dpt:22
10	ACCEPT	tcp		::/0	::/0 tcp dpt:162
11	ACCEPT	tcp		::/0	::/0 tcp dpt:3076
12	ACCEPT	tcp		::/0	::/0 tcp dpt:3077

Viewing CMS licensing information in the Web Client

About this task

In the Web Client, you can view CMS licensed features and the licensing status for each. The status refers to the licensing state. For example: Normal or Error. When the Error status is displayed, you also see information about when the violation first occurred and the latest violation. For general information about CMS licensing and a more detailed description of license modes, see *Avaya Call Management System Overview and Specification*.

Note that you cannot view the license status in the PC Client.

Procedure

Navigate to **Administration > Maintenance > License Status**.

For each license, you see the current status, what features are licensed, along with the quantities of the license, and any license violations.

Example

The following is an example of the type of licensing status information displayed:

License Status					
Latest Update: 10/10/2024 7:57 pm					
WebLM: https://148.147.177.245:52233/WebLM/LicenseServer					
Status: Normal 07/11/2024 8:05 am					
	Status	Licensed	Current	Initial Violation	Latest Violation
WebLM	Normal		connected		
Licensing	Normal	CMS	obtained		
Expiration	Normal	11/19/24	10/10/24		
Version	Normal	R21	R21		
ACDs	Normal	8	3		
Agents	Normal	30000	0		
Logins	Normal	1999	1		
ODBC/JDBC	Normal	5	0		
CLInt int	Normal	on	0		
CLInt ext	Normal	5	0		
RT Conn	Error	5	0	07/20/23	6:25
HR Conn	Normal	5	0		
OT Conn	Normal	5	0		

Support for LDAP integration

CMS supports LDAP Active Directory for user management. You can integrate CMS with Active Directory on Windows Server. CMS can only integrate with a single Active Directory system. Azure Active Directory is not supported.

You can administer traditional CMS Linux users and LDAP-authenticated users with CMS. When LDAP is enabled, the CMS User Data page provides an option to identify LDAP-authenticated users. When logging in to CMS, users are authenticated with the LDAP server. Linux password administration is not required for LDAP-authenticated users.

With LDAP integration, you can log in to all CMS interfaces, including:

- CMS Supervisor Web Client
- CMS Supervisor PC Client
- CMS ASCII

You can encrypt the Active Directory server connection to avoid exposing personal data. Data encryption with LDAP is an optional feature you can enable when installing the LDAP authentication feature package. Certificate setup is required to encrypt the LDAP connection.

*** Note:**

The CMS user ID maps to the Active Directory user or person **objectClass: sAMAccountName** field. The CMS user ID field supports 31 characters. However, for LDAP-authenticated users, you are limited to 20 characters. You cannot use special characters including hyphens, underscores, punctuation, and any diacritical, accented, special characters or blanks (for example, á, ñ, ç, |).

Verify that the username is configured in a user or person **objectClass** and that the username is in the **sAMAccountName** field. Verify that the names match exactly (spelling, capitalization, no unexpected spaces, and so on.)

Use the descriptions in this table to help you gather the information you need for LDAP integration:

Active Directory Server information	Example	Your Value
Enable optional encrypted LDAP connection (TLS/SSL)	yes, no	
Path to certificate exported from LDAP server – must be provided when LDAP encryption=yes	/tmp/my_AD_cert.cer	
Windows Active Directory server IP Address or Fully Qualified Domain Name An FQDN must be provided when LDAP encryption=yes	10.20.30.40 or ADServer.company.com	
Port number for the Active Directory server	389 (default for TCP) 689 (default for TLS/SSL) Or specific value from your AD server	

The installation log file for LDAP is in the CMS security log located at `/cms/install/logdir/security/cms_sec.log`.

Configuring LDAP in the command line interface

About this task

Configure LDAP Active Directory server integration with CMS. You must provide information about the LDAP server, including the IP address or FQDN and the domain connection string. This information is used to establish a connection.

Before you begin

Before configuring LDAP, ensure that the LDAP package is installed. If it is not installed, use the feature package installation procedures in *Maintaining and Troubleshooting Avaya Call Management System*.

Procedure

1. Log in to the CMS server with root privileges.
2. Run the `cmsadm` command to display the **cmsadm**.
3. Enter the number that corresponds with the option to configure the LDAP feature.
4. Enter `1` to configure the LDAP directory server and then press `Enter`.
5. Modify the following information if required and then press `Enter`:

- IP address or FQDN of the LDAP server.

IP address of the LDAP domain connection string. For example, type `DC=com` as the domain connection string value.

CMS verifies the information and establishes a connection with the LDAP server.

The system updates NSS-PAM-LDAPD configuration files, such as `nsld.conf` and `nsswitch.conf`. In the PAM file (for example, `cs-auth`), the PAM stack is updated to authenticate with LDAP first and then fall through to Linux authentication.

Chapter 12: Using administration and maintenance reports

This chapter describes the various administration and maintenance reports you can run using CMS Supervisor. The reports include:

- Exception reports
- Trunk Group Members reports
- Vector Configuration reports
- Tenant administration reports
- Maintenance reports
- Dictionary reports (PC Client only)

Related links

[About Dictionary reports](#) on page 349

[About exception reports](#) on page 352

[About Trunk Group Members reports](#) on page 369

[About Vector Configuration reports](#) on page 371

[About tenant administration reports](#) on page 372

[About maintenance reports](#) on page 374

About Dictionary reports

In the Dictionary window of the PC Client, use the Reports tab to generate reports on most sections of the Dictionary. These reports can be printed, sent to a file, or displayed on the screen.



Note:

Dictionary reports only work using the PC Client. Information you would see in the Dictionary reports is automatically displayed on the Dictionary windows used with the Web Client.



Note:

Dictionary reports are not available to tenant users. Tenant users are unable to see these reports in the user interface.

Permissions required to run Dictionary reports

To obtain a report, you need to read the permissions for the Dictionary subsystem.

Types of Dictionary reports

This section provides a description of each of the Dictionary reports.

Dictionary ACDs Report

This report gives you a report of the ACD names you have assigned in the Dictionary ACDs Operation input window and the corresponding ACD number.

Dictionary Agent Groups Report

You can generate reports of the groups(s) you created using the Dictionary Agent Groups Operation input window.

Dictionary Call Work Codes Report

The names you add in the Dictionary Call Work Codes Operation input window are displayed on the Dictionary Call Work Codes report.

Dictionary Custom Items Report

This report gives you a report of all the custom items in the database on the Avaya CMS server.

Dictionary Login Identifications Report

This report gives you a report of the names of agents that you have assigned to Login IDs in the Dictionary Login IDs Operation input window. If you assign names to the login IDs, agent names appear on all reports. However, if you make any additions or changes to login IDs, the changes do not appear on any real-time report that is currently running. You must exit the report and rerun it to see the new agent names.

Dictionary Splits/Skills Report

This report provides the names that have been assigned to splits/skills using the Dictionary Splits/Skills Operation input window. When you assign a split/skill name, that name appears on all split/skill windows and real-time and historical split/skill reports. However, if you make any additions or changes to split/skill names, the changes do not appear on any real-time report that is currently running. You must exit the report and rerun it to see the new split/skill names.

Dictionary Standard CMS Items Report

This report provides a list of all the Standard CMS database items on the Avaya CMS server.

Dictionary Tenants Report

This report displays the tenants defined on the system. You can access this report just like the other dictionary reports.

Dictionary Trunk Groups Report

This report provides the names that have been assigned to trunk groups using the Dictionary Trunk Groups Operation input window. When you assign a trunk group name, that name appears on all trunk group windows and real-time and historical reports. If you make any additions or changes to trunk group names, the changes do not appear on any real-time report that is currently running. You must exit the report and rerun it to see the new trunk group names.

Dictionary VDNs Report

Important:

If you have not purchased the Vectoring feature, this window is not available.

This report provides the names that have been assigned to VDNs in the Dictionary VDNs Operation input window. When you assign a VDN name, that name appears on all real-time and historical reports that include that VDN. However, if you make any changes to VDN names, the changes do not appear on any real-time report that is currently running. You must exit the report and rerun it to see the new VDN names.

Dictionary Vectors Report

Important:

If you have not purchased the Vectoring feature, this window is not available.

This report provides the names that have been assigned to vectors in the Dictionary Vectors Operation input window. When you assign a vector name, that name appears on all real-time and historical reports that include that vector. However, if you make any additions or changes to the vector names, the changes do not appear on any real-time report that is currently running. You must exit the report and rerun it to see the new vector names.

Printing dictionary reports

Procedure

1. From the Controller window, select **Commands > Dictionary**.
CMS Supervisor displays the Dictionary window.
2. Select the **Reports** tab.
CMS Supervisor displays the Reports window.
3. In the **Reports** list, select the Dictionary item on which you want to generate a report.
4. Select **OK**.
CMS Supervisor displays the Reports window.
5. Select one of the following options:
 - **View Report on Screen**
 - **Print Report on**

To send the report to a printer other than the default printer in the report window, select **Print Report on** and then select the printer button on the right side of the report window. Select the new printer from the Print window.

6. Select **OK**.

Depending on the option that you selected, the report is either sent to a printer or displayed on the screen.

Running an agent group members report

Procedure

1. From the Controller window, select **Commands > Dictionary**.

CMS Supervisor displays the Dictionary window.

2. Select the **Reports** tab.

CMS Supervisor displays the Reports window.

3. In the **Reports** list, select **Agent Group Members**.

4. Select **OK**.

CMS Supervisor displays the Dictionary Agent Groups window.

5. In the **Agent group name** field, enter the name of the agent group, and then press the **Enter** key.

6. Select one of the following options:

- **View Report on Screen**
- **Print Report on**

7. Select **OK**.

Depending on the option that you selected, the report is either sent to a printer or displayed on the screen.

About exception reports

Use the exception reports to view information about exceptions that occur on your system.

Running the Agent Exceptions by Location report using the Web Client

About this task

Use the Agent Exceptions by Location report to view exceptions that have occurred for the selected agents. For each agent exception, the report shows the time, agent, and type of exception.

Before you begin

To be able to view data for an agent exception report, the following events must have occurred:

- One or more agent exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. Navigate to **Administration > Exceptions > Reports > Agent Exceptions by Location**.

CMS Supervisor displays the Agent Exceptions by Location window.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. In the **Order by** field, select one of the following sorting options:
 - **Time** - The report results are sorted by the time that the exceptions occurred.
 - **Agent** - The report results are sorted by agent name or number.
4. In the **Split/Skill** field, select a split/skill using the drop-down list or search on the name or number of a split/skill.
5. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.

Click **Reset** to blank out the **Date** field.

6. Click **Agents** to select the agents to display in the report.

You can enter agent names or login IDs separated by a semicolon (;), or you can use the **Search Results** shuttle to move agents to the **Selected Agents** area. You can add up to 1,000 agents for the report.

7. Click **OK** to use the selected options.
8. Click **Exceptions** to select one or more exceptions to include in the report.

Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.

9. Click **OK** to use the selected options.
10. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Data Collection Exceptions report using the Web Client

About this task

Use the Data Collection Exceptions report to view any event that affects the storage of call center data. This includes the following:

- Starting or stopping data collection
- Resetting the clock
- A session (link) is down

Before you begin

The following items should be read and understood before working with the Data Collection Exceptions report:

- Exceptions must have occurred for the exception type that you want the report to cover. Otherwise, the report is blank.
- User IDs must have the “exception” permission for the ACD in order to be notified of a “link-down” exception.

Procedure

1. Navigate to **Administration > Exceptions > Reports > Data Collection Exceptions**.
CMS Supervisor displays the Data Collection Exceptions window.
2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.Click **Reset** to blank out the **Date** field.
4. Click **OK** to run the report.
CMS Supervisor displays the report.

Running the Malicious Call Trace report using the Web Client

About this task

The Malicious Call Trace feature provides a way for a terminal user to notify a predefined set of users that the user be party to a malicious call, such as bomb threats, hackers, and so forth.

The following actions occur when the Malicious Call Trace feature is activated:

- The inbound phone line is prevented from “hanging up”.
- Management is immediately alerted.
- The call is recorded (with an additional Communication Manager feature).

- All data regarding the call is stored.

The Malicious Call Trace report is used to view detailed information on the occurrences of these calls. The report shows the date and time when each call occurred, the agent who received the call, and the involved split/skill. If the automatic number identification/station number identification (ANI/SID) network feature has been purchased and implemented, the report also shows where the call originated. This report is only available with CMS Supervisor.

Before you begin

The following items should be read and understood before working with the malicious call trace report:

- To view the Malicious Call Trace report, the user ID used to log in to this CMS Supervisor session requires the “exception” permission for the split/skill that received the malicious call.

Procedure

1. Navigate to **Administration > Exceptions > Reports > Malicious Call Trace by Location**.

CMS Supervisor displays the Malicious Call Trace by Location window.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.

Click **Reset** to blank out the **Date** field.

4. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Split or Skill Exceptions report using the Web Client

About this task

The Split/Skill Exceptions report is used to view exceptions that have occurred for the selected splits/skills. For each split/skill exception, the report shows the time and type of exception.

Before you begin

To be able to view data for a Split/Skill Exceptions report, the following events must have occurred:

- One or more split/skill exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.
- The user ID used to run the report must have the “read” permission for the Exceptions subsystem and the affected splits/skills as well as the “exceptions” permission for all affected splits/skills.

Procedure

1. Navigate to **Administration > Exceptions > Reports > Split/Skill Exceptions**.

CMS Supervisor displays the Split/Skill Exceptions window.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.

3. In the **Order by** field, select one of the following sorting options:

- **Time** - The report results are sorted by the time that the exceptions occurred.
- **Split/Skill** - The report results are sorted by the split/skill number.

4. In the **Date** field, specify the date for the report using one of the following methods:

- Enter MM/DD/YY format; for example, 10/06/20.
- Select a date or range of dates using the calendar icon.

Click **Reset** to blank out the **Date** field.

5. Click **Split/Skill** to select the split/skill to display in the report.

Enter a split/skill number or a series of split/skill numbers separated by semicolons to display the results in the **Search Results** shuttle. Move the split/skill to the **Selected Split(s)/Skill(s)** area. You can add up to 1000 splits/skills for the report.

6. Click **OK** to use the selected options.

7. Click **Exceptions** to select one or more exceptions to include in the report.

Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.

8. Click **OK** to use the selected options.

9. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Trunk Group by Location Exceptions report using the Web Client

About this task

Use the Trunk Group by Location Exceptions to view exceptions that have occurred for the selected trunk groups. For each trunk group exception, the report shows the time and type of exception.

To be able to view data for a Trunk Group by Location Exceptions report, the following events must have occurred:

- One or more trunk group exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. Navigate to **Administration > Exceptions > Reports > Trunk Group Exceptions by Location**.

CMS Supervisor displays the Trunk Group Exceptions by Location window.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. In the **Order by** field, select one of the following sorting options:
 - **Time** - The report results are sorted by the time that the exceptions occurred.
 - **Trunk Group** - The report results are sorted by the trunk group.
 - **Trunk Location** - The report results are sorted by trunk location.
4. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.

Click **Reset** to blank out the **Date** field.

5. Click **Trunk Groups** to select the trunk groups to display in the report.

Enter a trunk group number or a series of trunk group numbers separated by semicolons (;) to display the results in the **Search Results** shuttle. Move the trunk groups to the **Selected Trunk Group(s)** area. You can add up to 1,000 trunk groups for the report.

6. Click **OK** to use the selected options.
7. Click **Exceptions** to select one or more exceptions to include in the report.

Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.

8. Click **OK** to use the selected options.
9. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the VDN Exceptions report using the Web Client

About this task

Use the VDN Exceptions report to view exceptions that have occurred for the selected VDN. For each VDN exception, the report shows the time and type of exception.

Before you begin

To be able to view data for a VDN exception report, the following events must have occurred:

- One or more VDN exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.

- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. Navigate to **Administration > Exceptions > Reports > VDN Exceptions**.
CMS Supervisor displays the VDN Exceptions window.
2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. In the **Order by** field, select one of the following sorting options:
 - **Time** - The report results are sorted by the time that the exceptions occurred.
 - **VDN** - The report results are sorted by the VDN.
 - **Vector** - The report results are sorted by vector.
4. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.

Click **Reset** to blank out the **Date** field.

5. Click **VDNs** to select the VDNs to display in the report.
Enter a VDN or a series of VDNs separated by semicolons (;) to display the results in the **Search Results** shuttle. Move the VDNs to the **Selected VDN(s)** area. You can add up to 1,000 VDNs for the report.
6. Click **OK** to use the selected options.
7. Click **Exceptions** to select one or more exceptions to include in the report.
Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.
8. Click **OK** to use the selected options.
9. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Vector Exceptions report using the Web Client

About this task

Use the Vector Exceptions report to view exceptions that have occurred for the selected vectors. For each vector exception, the report shows the time and type of exception.

Before you begin

To be able to view data for a Vector Exceptions report, the following events must have occurred:

- One or more vector exceptions must have been activated at some time in the past.

- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. Navigate to **Administration > Exceptions > Reports > Vector Exceptions**.
CMS Supervisor displays the Vector Exceptions window.
2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. In the **Order by** field, select one of the following sorting options:

- **Time** - The report results are sorted by the time that the exceptions occurred.
- **Vector** - The report results are sorted by vector.

4. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.

Click **Reset** to blank out the **Date** field.

5. Click **Vectors** to select the vectors to display in the report.

Enter a vector or a series of vectors separated by semicolons (;) to display the results in the **Search Results** shuttle. Move the vectors to the **Selected Vector(s)** area. You can add up to 1,000 vectors for the report.

6. Click **OK** to use the selected options.
7. Click **Exceptions** to select one or more exceptions to include in the report.

Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.

8. Click **OK** to use the selected options.
9. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Agent Exceptions by Location report using the PC Client

About this task

Use the Agent Exceptions by Location report to view exceptions that have occurred for the selected agents. For each agent exception, the report shows the time, agent, and type of exception.

Before you begin

To be able to view data for an agent exception report, the following events must have occurred:

- One or more agent exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. Select the **Reports** tab.
3. In the **ACD** field, select the ACD that contains the agents on which to run the report.
4. In the **Reports** list, highlight **Agent Exceptions by Location**.
5. Click **OK**.

CMS Supervisor displays the Agent Exceptions window.

6. In the **Date** field, specify the date for the report in one of the following date formats:

- Enter MM/DD/YY format; for example, 10/06/20.
- Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
- Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
- Select a date from the drop-down list.
- Select a date by using the Browse button.

This is a required field.

7. In the **Skill State** field, enter the name or number of the split/skill to display in the report.

This is a required field.

8. In the **Agents** field, specify the name or number of the agents to display in the report. This field accepts the specification of multiple agents. Multiple values must be separated by a semicolon (;).

This is a required field.

9. In the **Order by** field, select one of the following sorting options:

- **Agent** - The report results are sorted by agent name or number.
- **Time** - The report results are sorted by the time that the exceptions occurred.

10. In the **Exceptions** field, select one or more exceptions to include in the report.

Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.

11. In the **Destination** group, select the output option of the report:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

12. Click **OK**.

CMS Supervisor sends the report to the specified output option.

Running the Data Collection Exceptions report using the PC Client

About this task

Use the Data Collection Exceptions report to view any event that affects the storage of call center data. This includes the following:

- Starting or stopping data collection
- Resetting the clock
- A session (link) is down

Before you begin

The following items should be read and understood before working with the Data Collection Exceptions report:

- Exceptions must have occurred for the exception type that you want the report to cover. Otherwise, the report is blank.
- User IDs must have the “exception” permission for the ACD in order to be notified of a “link-down” exception.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. Select the **Reports** tab.

3. In the **Reports** list, highlight **Data Collection Exceptions**.

4. Click **OK**.

CMS Supervisor displays the Data Collection Exceptions window.

5. In the **ACD** field, select the ACD that contains the vector on which to run the report.

This field accepts multiple values. Multiple ACDs must be separated by a semicolon (;).

6. In the **Date** field, specify the date to view for the report. Entry of the date can be done through the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
 - Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
 - Select a date from the drop-down list.
 - Select a date by using the Browse button.

This is a required field.

7. In the **Destination** group, select one of the following output options:
 - **View Report on Screen** - The report is displayed on the screen.
 - **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.
8. Click **OK**.

CMS Supervisor sends the data collection exceptions report to the specified output option.

Running the Malicious Call Trace report using the PC Client

About this task

The Malicious Call Trace feature provides a way for a terminal user to notify a predefined set of users that the user may be party to a malicious call, such as bomb threats, hackers, and so forth.

The following actions occur when the Malicious Call Trace feature is activated:

- The inbound phone line is prevented from “hanging up”.
- Management is immediately alerted.
- The call is recorded (with an additional Communication Manager feature).
- All data regarding the call is stored.

The Malicious Call Trace report is used to view detailed information on the occurrences of these calls. The report shows the date and time when each call occurred, the agent who received the call, and the involved split/skill. If the automatic number identification / station number identification (ANI/SID) network feature has been purchased and implemented, the report also shows where the call originated. This report is only available with CMS Supervisor.

Before you begin

The following items should be read and understood before working with the malicious call trace report:

- To view the Malicious Call Trace report, the user ID used to log in to this CMS Supervisor session requires the “exception” permission for the split/skill that received the malicious call.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. Select the **Reports** tab.
3. In the **ACD** field, select the ACD that contains the vector on which to run the report.
4. In the **Reports** list, highlight **Malicious Call Trace by Location**.
5. Click **OK**.

CMS Supervisor displays the Malicious Call Trace window.

6. In the **Date** field, specify the date to view for the report. Entry of the date can be done through the following methods:

- Enter MM/DD/YY format; for example, 10/06/20.
- Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
- Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
- Select a date from the drop-down list.
- Select a date by using the Browse button.

This field can accept multiple date values, but the dates must be separated by a semicolon. This field is required.

7. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

8. Click **OK**.

CMS Supervisor sends the report to the specified output option.

Running the Splits/Skills Exceptions report using the PC Client

About this task

The Splits/Skills Exceptions report is used to view exceptions that have occurred for the selected split/skill. For each split/skill exception, the report shows the time and type of exception.

Before you begin

To be able to view data for a Splits/Skills Exceptions report, the following events must have occurred:

- One or more split/skill exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.

- Active exceptions must be specified in the input window so that they are included in the report.
- The user ID used to run the report must have the “read” permission for the Exceptions subsystem and the affected splits/skills as well as the “exceptions” permission for all affected splits/skills.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. Select the **Reports** tab.
3. In the **ACD** field, select the ACD that contains the split/skill on which to run the report.
4. In the **Reports** list, highlight **Split/Skill Exceptions**.
5. Click **OK**.

CMS Supervisor displays the Split/Skill Exceptions window.

6. In the **Date** field, specify the date to view for the report. Entry of the date can be done through the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
 - Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
 - Select a date from the drop-down list.
 - Select a date by using the Browse button.

This is a required field.

7. In the **Splits/Skills** field, specify the name or number of one or more split/skill to run the report against. Entry of the split/skill can be done through the following methods:
 - Enter the name or number of the split/skill.
 - Select the split/skill from the drop-down list.
 - Select the split/skill by using the Browse button.

Multiple split/skill can be entered in this field, but must be separated by a semicolon. This is a required field.

8. In the **Order by** field, select one of the following sorting options:
 - **Split/Skill** - The report results are sorted by split/skill name or number.
 - **Time** - The report results are sorted by the time the exceptions occurred.
9. In the **Exceptions** field, select one or more exceptions to include in the report.

Only those exceptions that have been activated in the past should be selected. Selecting exceptions that have not been activated will not return any data in the report.

10. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

11. Click **OK**.

CMS Supervisor sends the report to the specified output option.

Running the Trunk Group by Location Exceptions report using the PC Client

About this task

Use the Trunk Group by Location Exceptions to view exceptions that have occurred for the selected trunk groups. For each trunk group exception, the report shows the time and type of exception.

To be able to view data for a Trunk Group by Location Exceptions report, the following events must have occurred:

- One or more trunk group exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. Select the **Reports** tab.

3. In the **ACD** field, select the ACD that contains the trunk group on which to run the report.

4. In the **Reports** list, highlight **Trunk Group Exceptions by Location**.

5. Click **OK**.

CMS Supervisor displays the Trunk Group Exceptions window.

6. In the **Date** field, specify the date to view for the report. Entry of the date can be done through the following methods:

- Enter MM/DD/YY format; for example, 10/06/20.
- Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
- Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
- Select a date from the drop-down list.

- Select a date by using the Browse button.

This is a required field.

7. In the **Trunk Groups** field, specify the name or number of one or more trunk groups to run the report against. Entry of the trunk group can be done through the following methods:

- Enter the name or number of the trunk group.
- Select the trunk group from the drop-down list.
- Select the trunk group by using the Browse button.

Multiple trunk groups can be entered in this field, but must be separated by a semicolon (;).

This is a required field.

8. In the **Order by** field, select one of the following sorting options:

- **Trunk Groups** - The report results are sorted by trunk group number.
- **Trunk Location** - The report results are sorted by individual trunks.
- **Time** - The report results are sorted by the time the exceptions occurred.

9. In the **Exceptions** field, select one or more exceptions to include in the report.

Select only those exceptions that are or have been activated during the date specified. If you select exceptions that have not been active during the date specified, the report does not display any data in the report.

Audio difficulty is a trunk group exception that can be requested on a report even though it cannot be administered in trunk group exception operations.

10. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

11. Click **OK**.

CMS Supervisor sends the report to the specified output option.

Running the VDN Exceptions report using the PC Client

About this task

Use the VDN Exceptions report to view exceptions that have occurred for the selected VDN. For each VDN exception, the report shows the time and type of exception.

Before you begin

To be able to view data for a VDN exception report, the following events must have occurred:

- One or more VDN exceptions must have been activated.
- The exceptions must have occurred at some point. Otherwise, the report is blank.

- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.
CMS Supervisor displays the Exceptions window.
2. Select the **Reports** tab.
3. In the **ACD** field, select the ACD that contains the VDN on which to run the report.
4. In the **Reports** list, highlight **VDN Exceptions by Location**.
5. Click **OK**.

CMS Supervisor displays the VDN Exceptions window.

6. In the **Date** field, specify the date to view for the report. Entry of the date can be done through the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
 - Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
 - Select a date from the drop-down list.
 - Select a date by using the Browse button.

This is a required field.

7. In the **VDNs** field, specify the name or number of one or more VDNs to run the report against. Entry of the VDN can be done through the following methods:
 - Enter the name or number of the VDN.
 - Select the VDN from the drop-down list.
 - Select the VDN by using the Browse button.

Multiple VDNs can be entered in this field, but must be separated by a semicolon (;). This is a required field.

8. In the **Order by** field, select one of the following sorting options:
 - **Time** - The report results are sorted by the time the exceptions occurred.
 - **VDNs** - The report results are sorted by VDN name or number.
 - **Vectors** - The report results are sorted by vector.
9. In the **Exceptions** field, select one or more exceptions to include in the report.

Select only those exceptions that have been activated at some point in the past. Selecting exceptions that have not been activated will not return any data in the report.

10. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

11. Click **OK**.

CMS Supervisor sends the report to the specified output option.

Running the Vector Exceptions report using the PC Client

About this task

Use the Vector Exceptions report to view exceptions that have occurred for the selected vectors. For each vector exception, the report shows the time and type of exception.

Before you begin

To be able to view data for a Vector Exceptions report, the following events must have occurred:

- One or more vector exceptions must have been activated at some time in the past.
- The exceptions must have occurred at some point. Otherwise, the report is blank.
- Active exceptions must be specified in the input window so that they are included in the report.

Procedure

1. From the Controller window, navigate to **Commands > Exceptions** on the menu bar.

CMS Supervisor displays the Exceptions window.

2. Select the **Reports** tab.

3. In the **ACD** field, select the ACD that contains the vector on which to run the report.

4. In the **Reports** list, highlight **Vector Exceptions**.

5. Click **OK**.

CMS Supervisor displays the Vector Exceptions window.

6. In the **Date** field, specify the date to view for the report. Entry of the date can be done through the following methods:

- Enter MM/DD/YY format; for example, 10/06/20.
- Enter the relative day; for example, 0 for today, -1 for yesterday, or -7 for one week ago.
- Enter a relative range; for example, -9-0 causes the report to display data for the past ten days including today.
- Select a date from the drop-down list.
- Select a date by using the Browse button.

This is a required field.

7. In the **Vectors** field, specify the name or number of one or more vectors to run the report against. Entry of the vector can be done through the following methods:

- Enter the name or number of the vector.
- Select the vector from the drop-down list.
- Select the vector by using the Browse button.

Multiple vectors can be entered in this field, but must be separated by a semicolon (;). This is a required field.

8. In the **Order by** field, select one of the following sorting options:

- **Time** - The report results are sorted by the time the exceptions occurred.
- **Vectors** - The report results are sorted by vector name or number.

9. In the **Exceptions** field, select one or more exceptions to include in the report.

The exceptions selected in this field should be those that have been activated at some point in the past. Selecting exceptions that have not been activated will not return any data in the report.

10. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

11. Click **OK**.

CMS Supervisor sends the report to the specified output option.

About Trunk Group Members reports

The Trunk Group Members report is used to view the equipment locations of all the trunks that are in a particular trunk group. The report lists the selected trunk groups in numerical order, each trunk group's assigned name, and the equipment location of each trunk in the trunk group. If the trunk group does not have an assigned name, the **Trunk Group Name** field shows the trunk group number. Also, if the trunk group has no trunks assigned to it, the equipment location field is blank.

Before using the Trunk Group Members report

The following items should be read and understood before working with the Trunk Group Members report:

- Custom or designer reports cannot be created from the Trunk Group Members report.
- The link to the Communication Manager system must be active in order to run this report.

Permissions required to use the Trunk Group Members report

To run a Trunk Group Members report, the user ID used to log in to this session requires “read” permission for the Call Center Administration subsystem and all affected trunk groups.

Running the Trunk Group Members report using the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Reports > Trunk Group Members**.

CMS Supervisor displays the Trunk Group Members window.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. Click **Trunk Group** to select the trunk groups to display in the report.

Enter a trunk group number or a series of trunk group numbers separated by semicolons (;) to display the results in the **Search Results** shuttle. Move the trunk groups to the **Selected Trunk Group(s)** area. You can add up to 32 trunk groups for the report.

4. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Trunk Group Members report using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. On the Call Center Administration window, select the **Reports** tab.
3. In the **ACD** field, select the ACD for which the report will run.
4. In the **Reports** list, highlight **Trunk Group Members**.
5. Click **OK**.

Supervisor displays the Trunk Group Members window.

6. In the **Trunk Groups** field, enter the numbers or names of the trunk groups that are to be used in the report.

Multiple trunk groups must be separated by a semicolon (;).

7. In the **Destination** group, select the output option of the report:
 - **View Report on Screen** - The report is displayed on the screen.
 - **Print Report on** - Sends the report to the printer that is specified in the associated field. To change the specified printer, select the **Select printer** button located on the right side of this group.
8. Select **OK**.

Supervisor runs the report and sends it to the specified destination.

About Vector Configuration reports

Vector Configuration reports display the following items that are associated with a vector:

- Trunk group
- Trunk group name
- VDN
- VDN name
- Vector
- Vector name
- 1st, 2nd, and 3rd skill preferences
- 1st, 2nd, and 3rd skill names

Before using the Vector Configuration report

The following items should be read and understood before running Vector Configuration reports:

- A vector may appear in a report even if it is not associated with a trunk group or VDN.
- A vector may appear in a report even if it does not contain any steps.
- A custom or designer report cannot be created from a vector configuration report.
- A `go to vector` step can cause a trunk group or VDN to carry calls to another vector to which the VDN being used is not assigned. Trunk groups and VDNs that carry calls to a secondary vector in this manner do not appear in the vector configuration report for those secondary vectors.

Permissions required to use the Vector Configuration report

Depending on the procedure that you want to perform, you need the following permissions:

- To view a Vector Configuration report, the user ID used to log in to this session requires “read” permission for the Call Center Administration subsystem and all vectors to be listed on the report. Permissions are not required for the trunk groups and VDNs that are associated with the specified vectors.

Running the Vector Configuration report using the Web Client

Procedure

1. Navigate to **Administration > Call Center Administration > Reports > Vector Configuration**.

CMS Supervisor displays the Vector Configuration window.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.
3. Click **Vectors** to select the vectors to display in the report.

Enter a vector or a series of vectors separated by semicolons (;) to display the results in the **Search Results** shuttle. Move the vectors to the **Selected Vector(s)** area. You can add up to 1000 vectors for the report.

4. Click **OK** to run the report.

CMS Supervisor displays the report.

Running the Vector Configuration report using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Call Center Administration**.

CMS Supervisor displays the Call Center Administration window.

2. Select the **Reports** tab.
3. In the **ACD** field, select the ACD containing the vector on which the report will be run.
4. In the **Reports** list, highlight **Vector Configuration**.
5. Click **OK**.

Supervisor displays the Vector window.

6. In the **Vectors** field, enter the name or number of the vector for which the report will be run.

Multiple vectors can be entered in this field but must be separated by a semicolon (;).

7. In the **Destination** group, select the output option of the report:
 - **View Report on Screen** - The report is displayed on the screen.
 - **Print Report on** - Sends the report to the printer that is specified in the associated field. To change the specified printer, select the **Select printer** button located on the right side of this group.
8. Select **OK**.

Supervisor runs the report and sends it to the specified destination.

About tenant administration reports

Use the Tenant Agent Group Members report to view all of the administered tenants, tenant agent groups, agents, and agent login IDs.

Running the Tenant Agent Group Members report using the Web Client

Procedure

1. Navigate to **Tenant Administration > Reports > Tenant Agent Group Members**.

CMS Supervisor displays the Tenant Agent Group Members window showing the report data for the current ACD.

2. In the **Current ACD** drop-down list, select the ACD for which you want to run a report.

CMS Supervisor displays the Tenant Agent Group Members window showing the report data for the selected ACD.

Running the Tenant Agent Group Members report using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Tenant Administration**.

CMS Supervisor displays the Tenant Administration window.

2. Click the **Reports** tab.

3. Select **Tenant Agent Group Members**.

CMS Supervisor displays the Tenant Administration Agent Group Members window.

4. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.
- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

5. Click **OK**.

CMS Supervisor sends the report to the specified output option.

Running the Tenant Agent Groups report using the PC Client

Procedure

1. From the Controller window, navigate to **Commands > Tenant Administration**.

CMS Supervisor displays the Tenant Administration window.

2. Click the **Reports** tab.

3. Select **Tenant Agent Groups**.

CMS Supervisor displays the Tenant Administration Agent Groups window.

4. In the **Destination** group, select one of the following output options:

- **View Report on Screen** - The report is displayed on the screen.

- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

5. Click **OK**.

CMS Supervisor sends the report to the specified output option.

About maintenance reports

This section provides information about setting up and running maintenance reports. CMS administrators and users with read permission for the Maintenance subsystem can display the maintenance reports.

Maintenance reports:

- Identify problems and facilitate the work necessary to fix problems.
- Aid Services personnel in clearing problems in your system.
- Track changes made to the system by administrative users.

About the ACD Administration Log report

The ACD Administration Log provides an audit trail for all administrative changes made to an ACD by CMS administrative users. The administrative changes include changes to agents, skills, and any other ACD-related features. The ACD Administration Log records real-time administrative changes made by a user through CMS Supervisor or the CMS ASCII interface. The log also records the administrative changes made by a user through a scheduled timetable or a CMS Supervisor script. You can view all of these log entries using the ACD Administration Log report.

Before using the ACD Administration Log report

The following items should be read and understood before working with the ACD Administration Log report:

- The maximum capacity for the log is set at 30,000 records and cannot be changed. When the table size exceeds 30,000 records, the 100 oldest records will be deleted.
- This report can be scheduled through a CMS timetable or a CMS Supervisor script.
- The historical database items of the CMS ACD Administration Log are not available for use with the CMS Supervisor Report Designer tool. The menu option for this report will not display the Designer option. It will, however, behave in the same manner as drill-down reports.

Permissions required to use the ACD Administration Log report

To view the ACD Administration Log report, the user ID must have “read” permission for the Maintenance subsystem.

! Important:

If the ACD Administration Log report is run to display all 30,000 records, your PC should have no less than 200 MB of free disk space to allow for the caching of this data.

Running the ACD Administration Log report using the Web Client

Procedure

1. Navigate to **Administration > Maintenance > Reports > ACD Admin Log Report**.

CMS Supervisor displays the ACD Admin Log Report window.

2. In the available fields, enter the data to use in the report. For a description of the ACD Administration Log window fields, see [ACD Administration Log report field descriptions](#) on page 376 for additional information.
 3. Click **Run** to run the report. Click **Clear** to discard the selected report parameters.
- CMS Supervisor displays the report data. Since there can be up to 30,000 rows of data, the report might take several minutes to display on the screen.

Running the ACD Administration Log report using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.

CMS Supervisor displays the Maintenance window.

2. Select the **Reports** tab.
3. In the **Reports** list, select **ACD Administration Log Report**.

It is not necessary to select an ACD in the **ACD** field as this feature allows ACD specification in a subsequent dialog.

4. Click **OK**.

Supervisor displays the ACD Administration Log window.

The height of this dialog box varies according to the current screen resolution of your PC. A higher screen resolution results in more fields being displayed.

For a description of the ACD Administration Log window fields, see [ACD Administration Log report field descriptions](#) on page 376 for additional information.

5. In the available fields, enter the data to use in the report.

The data can also be selected through the drop-down history lists or through the Browse buttons.

The more fields that you specify, the more restricted the data will be that is used in the report. If all of the input fields are left blank, all records will be displayed.

6. In the **Destination** group, select one of the following output options:
 - **View Report on Screen** - The report is displayed on the screen.

- **Print Report on** - The report is sent to the specified printer. Any printer available to the PC can be used and selected through the button at the right of the field.

7. Select **OK**.

Supervisor displays the ACD Administration Log with the specified data.

ACD Administration Log report field descriptions

Name	Description
CMS User IDs	The user IDs to display in the report. If changes were made to the ACD with the specified user IDs, those user IDs and the associated changes are displayed.
Dates	The date or range of dates to be covered in the report. Only those administrative changes made on or within the date(s) specified will be present in the report.
Times	A range of time for which log entries are to be displayed. Only those administrative changes made within this time range will be present in the report.
ACDs(n)	The ACDs to include in the report.
VDNs(n)	The VDNs on the ACD to include in the report.
Vectors(n)	The Vectors on the ACD to include in the report.
Agents(n)	The login IDs on the ACD to include in the report.

About the Maintenance Error Log report

Use the Maintenance Error Log report to help you in working on system problems and to help Services personnel in clearing problems from your system. The Maintenance Error Log report displays a chronological list of warnings, information, and errors detected by CMS .

Before using the Maintenance Error Log report

The following items should be read and understood before working with the Maintenance Error Log report:

- The Maintenance Error Log report can contain 500 entries. When the log reaches 500 records, the next record will overwrite the oldest record.
- The entries in the Maintenance Error Log report are displayed in chronological order, starting with the most recent entry.
- You can search the log by error severity or by error code
- The results of all archives and backups are written to the Maintenance Error Log.
- If you have the CMS Forecast feature, the results of the Forecast Manager are written to the Maintenance Error Log report.

Running the Maintenance Error Log report using the Web Client

Procedure

1. Navigate to **Administration > Maintenance > Reports > Data Collection Exceptions**.
CMS Supervisor displays the Error Log Report window.
2. In the **ACD** drop down list, select **All ACDs** or select an individual ACD for which you want to see an error log report. Selecting an ACD Group shows the error logs for only the member ACDs of that group.
3. In the **Error codes** field, leave it blank if you want to display all error codes in the error log report. If you only want the report to include specific error codes, enter the codes in the **Error codes** field.
4. In the **Severities** drop down list, select **All Severities** to include errors of any severity level, or select the severity level you want to see in the report.
See [Severity of errors](#) on page 378 for additional information on error code classifications.
5. In the **Date** field, specify the date for the report using one of the following methods:
 - Enter MM/DD/YY format; for example, 10/06/20.
 - Select a date or range of dates using the calendar icon.
 Click **Reset** to blank out the **Date** field.
6. Click **Run** to run the report. Click **Clear** to discard the selected report parameters.
CMS Supervisor displays the report data.
See [Maintenance Error Log messages](#) on page 378 for additional information about the error messages.

Running the Maintenance Error Log report using the PC Client

Procedure

1. From the Controller window, navigate to **Tools > Maintenance**.
CMS Supervisor displays the Maintenance window.
2. Select the **Reports** tab.
3. Select **Error Log Report** in the **Reports** list.
4. Click **OK**.
Supervisor displays the Maintenance Error Log window.
5. In the **ACD** drop down list, select **All ACDs** or select an individual ACD for which you want to see an error log report. Selecting an ACD Group shows the error logs for only the member ACDs of that group.
6. In the **Error codes** field, leave it blank if you want to display all error codes in the error log report. If you only want the report to include specific error codes, enter the codes in the **Error codes** field.

7. In the **Severities** drop down list, select **All Severities** to include errors of any severity, or select the severity level you want to see in the report.

See [Severity of errors](#) on page 378 for additional information on error code classifications.

8. In the **Date** field, enter the amount of time that the report will include through one of the following methods:

- Enter the date(s) in the MM/DD/YY format.
- Use the history list to select the dates.
- Use the Browse button to select the dates
- Enter the date in relative format; for example, 0 for today, -1 for yesterday.

9. Select one of the following **Destination** options:

- To display the Maintenance Error Log on the monitor, select **View Report on Screen**.
- To send the Maintenance Error Log to a printer, select **Print Report on**.

10. Select **OK**.

CMS Supervisor displays the report data.

See [Maintenance Error Log messages](#) on page 378 for additional information about the error messages.

Severity of errors

The following list describes the error classifications in the Maintenance Error Log:

- **ALARM** - This type of entry could cause the system to crash or fail. You must work with Avaya Services to avoid the possibility of system failure.
- **ERROR** - This type of entry needs immediate action. For example, a backup may not be working properly.
- **INFO** - This type of entry does not need immediate action but is listed either to let you know that some aspect of the system is not operating correctly or to indicate the status of an operation. For example, *Successful*.

Maintenance Error Log messages

The Maintenance error codes and related messages are organized by error code number. If any of the solutions do not resolve the problem you are experiencing, contact your CMS services representative. If a reference to a task number is shown in the Maintenance Error Log, give the number to the CMS services personnel.

The following table lists the possible error codes as well as the related information.

Error Code	Message	Reason/Action
500	UNIX error on OPEN, file: <filename>	Could not write a file which is part of a timetable. One or more timetable tasks may be corrupted.
505	UNIX error on WRITE, file: File system may be out of space.	Error in writing the file. Potential file space problem.
505	The following two errors are found together: UNIX error on WRITE, file: SIGPIPE signal caught during printing, print request is incomplete or failed UNIX error on WRITE, file: lp. The user may have no default printer assigned and the UNIX(r) system administration for a default system line printer has not been done.	Could not print a file. The CMS server probably does not have a default system line printer assigned, and the user probably does not have a CMS default printer assigned. Using the operating system documentation, administer a default printer. Select the <F3> key -> Options > Default printer to assign a default printer to a user. Ensure that the user has the appropriate permissions to the printer in the User Permissions subsystem.
555	UNIX error on EXEC: Couldn't execute the following command: <user command>	System is too busy for command to be processed.
555	UNIX error on EXEC: CMS couldn't run because crt_io_man wouldn't execute	System is too busy for command to be processed.
556	UNIX error on FORK: CMS couldn't run because the system was too busy.	System is too busy for command to be processed.
556	UNIX error on FORK: UNIX process limit exceeded, system is too busy	CMS was unable to start a process. This occurs most likely if a user is logged into CMS through multiple terminals. Make sure each user logs in on only one CMS terminal/session at a time. If this message occurs when timetables are running, try adjusting the starting times of the timetables so that fewer are running simultaneously. If it occurs when running , try rewriting the Main Menu Addition to use fewer simultaneous operating system processes.
556	UNIX error on FORK: Call records not being sent. Call Services.	The process for transferring external call records could not be started. Call Services.
557	UNIX call error: UNIX process limit exceeded. System is too busy	This error could occur for multiple reasons. Call services for assistance.

Table continues...

Error Code	Message	Reason/Action
557	UNIX call error: uucp failed	The uucp file transfer mechanism for the External Call Records feature has failed. The system will automatically retry the transfer. If it fails repeatedly, call Services.
1001	UNIX error on NEW Agent upper bound has been reached. You have administered more Agent Exceptions than are allocated. You must either delete unneeded exceptions or allocate more space in System Setup: Data Storage Allocation.	The exception distributor process (ED) is attempting to log more agent exceptions than will fit in the storage space allocated for them. Delete unneeded exceptions or allocate more space in Data Storage Allocation > System Setup .
1001	UNIX error on NEW Split upper bound has been reached. You have administered more Split Exceptions than are allocated. You must either delete unneeded exceptions or allocate more space in System Setup: Data Storage Allocation.	The exception distributor process (ED) is attempting to log more Split exceptions than will fit in the storage space allocated for them. Delete unneeded exceptions or allocate more space in Data Storage Allocation > System Setup .
1001	UNIX error on NEW Trunk group upper bound has been reached. You have administered more Trunk Group Exceptions than are allocated. You must either delete unneeded exceptions or allocate more space in System Setup: Data Storage Allocation.	The exception distributor process (ED) is attempting to log more Trunk Group exceptions than will fit in the storage space allocated for them. Delete unneeded exceptions or allocate more space in Data Storage Allocation > System Setup .
1001	UNIX error on NEW VDN upper bound has been reached. You have administered more VDN Exceptions than are allocated. You must either delete unneeded exceptions or allocate more space in System Setup: Data Storage Allocation.	The exception distributor process is attempting to log more VDN exceptions than will fit in the storage space allocated for them. Delete unneeded exceptions or allocate more space in Data Storage Allocation > System Setup .

Table continues...

Error Code	Message	Reason/Action
1001	UNIX error on NEW Vector upper bound has been reached. You have administered more Vector Exceptions than are allocated. You must either delete unneeded exceptions or allocate more space in System Setup: Data Storage Allocation.	The exception distributor process is attempting to log more Vector exceptions than will fit in the storage space allocated for them. Delete unneeded exceptions or allocate more space in Data Storage Allocation > System Setup .
1050	INFORMIX SQL syntax error:	The given SQL command is syntactically incorrect. Usually more details of the error are included. For customers, this error is reported via their custom report and is corrected there. For CMS , this is usually a software problem which may need reporting. Correct the SQL statement in the custom report.
1053	INFORMIX insert error	An internal error or a full ACD dbspace is preventing data from being inserted into the ag_actv database table. Make sure that there is enough room in the ACD dbspace that holds the table.
1100	IPC error on messages: message queue queue is NN% full	This message is logged when a message queue is more than 75 percent full. Each message queue is checked approximately once every two minutes. If this message is repeatedly logged, CMS is in danger of losing messages that may result in loss of customer data. Single occurrences of this message can be ignored. If it happens repeatedly, contact services for assistance. Try reducing your CMS usage while this message is being logged to reduce the chances of losing data. If this message occurs while you are doing a CMS backup, try doing the backup during a less busy period.

Table continues...

Error Code	Message	Reason/Action
1302	PROCESS COMMUNICATIONS (PO) library error, function: ERROR - <HARCH> receiving too many exceptions too fast. Some exceptions have been discarded. Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered.	Exceptions are being generated faster than interval archiver process can handle them. This is the result of having too many exceptions activated, or having thresholds set to produce too many exceptions. Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered.
1302	PROCESS COMMUNICATIONS (PO) library error, function: ERROR - <IDBM> receiving too many exceptions too fast. Some exceptions have been discarded. Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered.	Exceptions are being generated faster than intermediate database manager interface process can handle them. This is the result of having too many exceptions activated, or having thresholds set to produce too many exceptions. Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered.
1302	PROCESS COMMUNICATIONS (PO) library error, function: ERROR - <SPI> receiving too many exceptions too fast. Some exceptions have been discarded. Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered.	Exceptions are being generated faster than the switch interface process can handle them. This is the result of having too many exceptions activated, or having thresholds set to produce too many exceptions. Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered.
1350	GENERAL error internal to process: Unable to successfully complete archiving.	Unable to initialize CMS environment. Re-initiate Data Summarizing.
1350	GENERAL error internal to process: Failure in agent exception database table. Agent exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the agent exception table. The error can occur when the ACD dbspace holding the agent exception table becomes full. No more agent exceptions can be recorded until the problem is corrected.
1350	GENERAL error internal to process: Failure in link exception database table. Link exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the link exception (linkEx) table. The error can occur when the disk partition holding the link exception table becomes full. No more link exceptions can be recorded until the problem is corrected.

Table continues...

Error Code	Message	Reason/Action
1350	GENERAL error internal to process: Failure in malicious call trace exception database table. MCT exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the malicious call trace exception (mctEx) table. The error can occur when the disk partition holding the malicious call trace exception table becomes full. No more malicious call exceptions can be recorded until the problem is corrected. Call Services.
1350	GENERAL error internal to process: Failure in split exception database table. Split exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the split exception (spEx) table. The error can occur when the disk partition holding the split exception table becomes full. No more split exceptions can be recorded until the problem is corrected. Call Services.
1350	GENERAL error internal to process: Failure in trunk group exception database table. Trunk group exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the trunk group exception table. The error can occur when the disk partition holding the trunk group exception table becomes full. No more trunk group exceptions can be recorded until the problem is corrected. Call Services.
1350	GENERAL error internal to process: Failure in VDN exception database table. VDN exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the VDN exception (vdnEx) table. The error can occur when the disk partition holding the VDN exception table becomes full. No more VDN exceptions can be recorded until the problem is corrected. Call Services.
1350	GENERAL error internal to process: Failure in vector exception database table. Vector exception data not being stored. Call Services.	This error message is logged when the exception distributor process is unable to insert rows in the vector exception (vecEx) table. The error can occur when the disk partition holding the vector exception table becomes full. No more vector exceptions can be recorded until the problem is corrected. Call Services.

Table continues...

Error Code	Message	Reason/Action
1350	GENERAL error internal to process: CMS task limit exceeded, system is too busy	This message means that a CMS task cannot be created because CMS is already running the maximum number of tasks. Make sure each user logs in to CMS only once. If this message occurs when timetables are running, try adjusting the starting times of the timetables so that fewer are running simultaneously. If it occurs when running Main Menu Addition, try rewriting the Main Menu Addition to use fewer simultaneous operating system processes.
1350	GENERAL error internal to process: Update failure for <item searched> Too much data. Try again with a more restrictive search.	Item searched for is too large. The search needs to be restricted further. Restrict the search to a smaller amount of data.
1350	GENERAL error internal to process: disk may be full.	Error in searching for item. Disk may be full. Clean up unnecessary files from disk.
1350	GENERAL error internal to process: Failure in removing data from database table: ag_actv. Agent Trace data not being stored. Call Services.	An internal error occurred that prevents data from being deleted from the ag_actv database table. Call Services.
1351	GENERAL error in process interface: Invalid action request.	Something is corrupted with the window interface. Exit and re-enter the data summarizing window. Attempt to initiate data summarizing again.
1351	GENERAL error in process interface: Cannot archive a day which interval data does not exist for.	Interval data does not exist for the requested day or any day prior to the requested day. The number of days of interval data saved is based on the Days of Intrahour field set on the Data Storage Allocation window. Re-initiate Data Summarizing for a day that is within the number of Days of Intrahour saved. For future reference, the number of Days of Intrahour data can be increased. Disk space must be considered before changing this parameter.

Table continues...

Error Code	Message	Reason/Action
1351	GENERAL error in process interface: Cannot archive the requested week/month. Daily data does not exist for all tables for the week/month beginning xx/xx/xx.	Daily data does not exist for the requested week/month or any week/month prior to the requested day. The number of days of interval data saved is based on the Days of Daily field set on the Data Storage Allocation window. Re-initiate Data Summarizing for a week/month that is within the number of Days of Daily saved. For future reference, the number of Days of Daily data can be increased. Disk space must be considered before changing this parameter. If the number of Days of Daily is changed and intrahour daily data is present for the days of the requested week/month, those days can be archived and the week/month can then be archived.
1351	GENERAL error in process interface: ERROR - <ARCH> receiving too many archive requests too fast. Some requests have been discarded.	Too many data summarizing requests (more than 25) have been initiated in a short period of time (approx. 1/2 hour) and cannot all be processed. Determine all data summarizing requests that have been initiated. Once all requests have been processed, verify the requests against the completed archives (as reported in /cms/dc/archive/arch.log). Re-initiate archive for the date and archive (daily/weekly/monthly) for the archives not initiated. In the future, do not initiate all requests at once.
1351	GENERAL error in process interface: Cannot archive a day in the future.	The date of the requested archive has not happened yet. Re-initiate the daily archive for a date prior to today.
1351	GENERAL error in process interface: Cannot archive a partial weeks/months data.	The last day for the week/month has not been archived yet. Verify that a weekly/monthly archive is not being requested for the current week/month. That is, the end of the week/month has not been reached yet. Re-initiate the weekly/monthly archive for a week/month in which the last day has already been archived.

Table continues...

Error Code	Message	Reason/Action
1351	GENERAL error in process interface: stopping task id to free up message queue	A message queue is more than 85 percent full and the task that should be reading from the queue is apparently stuck. This message is logged when CMS restarts the task to attempt to clear the error condition. Depending on which task has been stopped, it is likely that some customer data has been lost. Report the problem to services. If this error is logged repeatedly, try reducing your CMS usage while this message is being logged to reduce the chances of losing data. If this message occurs while you are doing a CMS backup, try conducting the backup during a less busy period.
1351	GENERAL error in process interface: External applications not started. Set to OFF	When the External Application feature was started, there was some general error. The feature was turned back off because of this error. Request help from your External Application provider (Avaya Professional Services Organization).
1351	GENERAL error in process interface: Activate Agent Trace request failed. Try again.	This error is logged when the agent activity recorder process (AAR) has too many messages in its message queue to accept any more. This can occur when many very active agents are being traced, keeping aar's queue full. Trace fewer agents or try this request again later.
1351	GENERAL error in process interface: Task < task_num> of timetable <name> may not have completed, window status was: <status>	Timetable ran and has a status other than Successful. Based on what the timetable was, examine the state of things (database, ACD administration, etc) to see if the request completed. If desired, complete the action manually by running CMS now.

Table continues...

Error Code	Message	Reason/Action
1400	SPI session error: data collection session is down	An error has occurred in the X.25 connection to the switch. CMS data is not being collected. CMS will automatically try to restore the link. If the link does not re-establish by itself within five minutes, check the cables, modems, and other hardware between the CMS and the switch for any obvious loose connections.
1404	SPI configuration error: Insufficient unmeasured trunks allocated. To avoid further data loss, go to Data Storage Allocation and administer more unmeasured trunk facilities.	There are not enough unmeasured trunks allocated in the CMS realtime database to track all calls. This message is logged once during each data collection interval when the error condition occurs. When this message appears, some call data has already been lost. Data will continue to be lost until more trunk facilities have been allocated. Allocate more unmeasured trunk facilities in the Data Storage Allocation screen.
1404	SPI configuration error: Switch and UNIX clocks differ by more than 24 hours. Switch clock is <nn:nn:nn nn/nn/nn> UNIX clock is <mm:mm:mm mm/mm/mm> Data collection will remain down until switch or UNIX clock is reset so they agree.	CMS requires that the times on the Communication Manager and operating system remains within 24 hours of each other. This is done to prevent an accidental deletion of all historical data if someone were to inadvertently change the clock to a date far into the future. If the operating system clock is correct but the Communication Manager clock is incorrect, reset the clock at the switch. CMS will bring the link up automatically within five minutes after correcting the switch clock.
1404	SPI configuration error: Extension <number> has been staffed by two different login IDs: <first> and <second>. Data will be tracked only for the last login ID. Ask the agent to log off and log in again with a single login ID.	Protocol error as explained in the message. Ask the agent to log off and log in again with a single login ID.

Table continues...

Error Code	Message	Reason/Action
1404	One of the following messages will be displayed depending on the switch configuration: Two agents at extensions <ext>in split <num> and <ext>in split <num> are logged in with the same login ID: <id> This may indicate table corruption on the switch. Contact Services to repair table as soon as possible. Two agents at extensions <ext> and <ext>are logged in with the same login ID: <id>. This may indicate table corruption on the switch. Contact Services to repair table as soon as possible.	Protocol violation or switch corruption. Try requesting new translations in ACD Status screen. If the problem persists, call Services.
1404	One of the following messages will be displayed depending on the switch configuration: SPI configuration error: Agent <logid> at extension <ext>has logged into too many splits: <sp1>, and <sp2>. Data will only be tracked for the last split. This may indicate incorrect switch type on CMS for G3. SPI configuration error: Agent <logid> at extension <ext> has logged into too many splits: <sp1>, <sp2>, <sp3>, and <sp4> . Data will only be tracked for the last split. This may indicate incorrect switch type on CMS for G3. SPI configuration error: Agent <logid> at extension <ext> has logged into too many splits: <sp1>, <sp2>, <sp3>, <sp4>, and <sp5>. Data will only be tracked for the last split. This may indicate incorrect switch type on CMS for G3.	Switch type mismatch, protocol violation or switch table corruption. Try requesting new translations in Data Storage Allocation screen. If the problem persists, call Services.

Table continues...

Error Code	Message	Reason/Action
1406	SPI data message error: ERROR can't new a message (or got illegal opcode)	This generally indicates that there is a mismatch between the administered CMS type on the Communication Manager system and the actual CMS or there is a mismatch between the administered switch type and feature set of the switch on the CMS . This results in message formats being of unexpected lengths. Data is lost since the remainder of the buffer is discarded after the unknown message. Determine if the problem happens more than once. Call Services.
1407	SPI timer expired error: there is no response from the switch	CMS has stopped receiving messages from the Communication Manager system. CMS data is not being collected. CMS will automatically try to restore the link. At the switch, perform a busy out and release the MIS connection.
1409	SPI ACD administration error: switch was unable to logon agent <logid> with skill <num>	For some reason the login failed on the switch. This login may have been part of a Move Agent or Change Agent Skills request which was pending. Have the agent try to log in to the skill again. Or put the agent in the AUX workmode for all skills and have no calls on their set. Repeat the administration request. If the request fails again, collect the information from the status window for Services.
1409	One of the following messages will be displayed: SPI ACD administration error: switch unable to move ext <ext> from split <num> to <num> SPI ACD administration error: switch unable to move ext <ext> from split <num>	Previous ACD administration request for moving an agent or changing an agent's skills was pending. When the pending was resolved, the agent could not be moved for some reason. Put the agent in the AUX workmode for all split/skills and have no calls on their set. Repeat the administration request. If the request fails again, collect the information from the status window for Services.
1501	SCREEN MANAGER error: system may be overloaded by real time reports behind by XX seconds.	CMS is behind on refreshing the real-time reports currently running. Run fewer real-time reports or lengthen refresh rates for the reports currently running.

Table continues...

Error Code	Message	Reason/Action
1600	FORECAST status: Forecast Manager failed for mm/dd/yy	Forecast Manager failed in its attempt to perform the daily data collection and/or the current day report for mm/dd/yy. If the date is invalid, correct the date and rerun the report. If it is not a problem with the date, call Services for assistance.
1600	FORECAST status: Forecast Manager failed for mm/dd/yy - mm/dd/yy	Forecast Manager failed in its attempt to perform the recollect data for a range of dates mm/dd/yy - mm/dd/yy. The first date is the start date and the second date is the stop date. If the dates are invalid, correct the date and rerun the report. If it is not a problem with the date, call Services for assistance.
1700	BACKUP Process out of sync. Contact Services.	A bad message was received from the backup screen. If this occurs, some sort of interference may have occurred in the message queue between the backup process and backup screen. If the problem re-occurs, something is impacting the communication between the processes. Further investigation is necessary to determine the source of the problem. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.
1701	BACKUP Process out of memory. Contact Services.	If this error occurs, it is when the tape is being verified, but after the backup has already completed successfully. If tape verification is not essential, no further action is necessary. This error indicates a problem with memory allocation. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.

Table continues...

Error Code	Message	Reason/Action
1702	BACKUP Process startup failed. Contact Services	Any number of startup activities could cause this problem. Most are message and database activities that should never be encountered. If the problem re-occurs, something is peculiar in the environment of the backup process and further investigation is necessary to determine the source of the problem. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.
1703	BACKUP Volume access failed. Retry Backup.	A problem accessing the backup device has occurred. This problem could range from an invalid backup device to the tape drive requiring cleaning. Verify the following: • The backup device is administered properly (name corresponds with the operating system administered device) • The tape compatibility is correct (320 meg tape for 320 meg drive, etc.). • The tape drive is clean.
1704	BACKUP Volume check failed. Retry Backup.	Either the inserted tape is a recent backup and backup was initiated in timetable or backup had difficulty determining the most recent backup (either full or incremental) volume. Determine if the inserted tape is associated with the most recent backup (full or incremental). Replace the tape and re-execute backup (or services run <code>br_check</code>).
1705	BACKUP Volume verification failed. Retry Backup.	A problem reading the tape exists. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.

Table continues...

Error Code	Message	Reason/Action
1706	BACKUP Table backup failed. Retry Backup. Table=	A problem was encountered either reading the indicated table or writing that table to tape. Replace the tape with a new tape (after verifying no problems with the indicated table) and re-execute the backup process. Verify that the problem does not re-occur.
1707	BACKUP Volume span failed. Retry Backup	When verifying the backup tape, a problem was discovered between the current volume and the previous volume. Most likely, the blocks are out of sequence. More specifically, at least 1 block is missing. Re-execute the backup process. Verify that the problem does not re-occur.
1708	BACKUP Error in process communication. Retry Backup.	This should never be encountered. A bad message was received from the backup screen (or erroneously from another process). If this occurs, some sort of interference occurred in the message queue between the backup process and backup screen. If the problem re-occurs, something is impacting the communication between the processes. Further investigation is necessary to determine the source of the problem. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.
1709	BACKUP Backup history update failed. Retry Backup.	This should never be encountered. The backup was completed successfully. A problem exists with the update tables or the process to update the tables. Verify that the next backup does not encounter this problem.
1710	BACKUP Process in need of service. Please check the Backup screen.	An acknowledgement window is requiring a response. Respond to the backup acknowledgement window.

Table continues...

Error Code	Message	Reason/Action
1711	INFO Warning backup waited 210/7200 seconds before archive completed.	The backup process waited 210 seconds for the current archiving process to finish. Backups should not be run during the archiving process. If this occurs consistently, consider rescheduling your archiving and backup processes so that overlap does not occur.
1711	ERROR backup terminated because archive did not complete within 2 hours.	The backup process waited two hours for the archiving process to be completed and was terminated as a result. Backups should not be run during the archiving process. Reschedule the backup and archiving processes so that simultaneous processing does not occur.
1711	BACKUP INFO:	Backup was initiated through a timetable and information is reported (number of volumes and backup completed) simply for information purposes. No action required
1750	BACKUP Screen startup failed. Contact Services.	Any number of startup activities could cause this problem. Most problems deal with accessing screen entries and database activities that should never be encountered. If the problem re-occurs, something is peculiar in the environment of the backup process. Further investigation is necessary to determine the source of the problem. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.
1751	BACKUP Screen execution failed. Retry Backup.	Any number of startup activities could cause this problem. Most problems deal with accessing screen entries and database activities that should never be encountered. If the problem re-occurs, something is peculiar in the environment of the backup process. Further investigation is necessary to determine the source of the problem. Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur.

Table continues...

Error Code	Message	Reason/Action
1800	RESTORE Process out of sync. Contact Services.	A bad message was received from the restore screen. If this occurs, some sort of interference occurred in the message queue between the restore process and restore screen. If the problem re-occurs, something is impacting the communication between the processes. Further investigation is necessary to determine the source of the problem. Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur.
1801	RESTORE Process out of memory. Contact Services.	A problem with memory allocation exists. Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur.
1802	RESTORE Process startup failed. Contact Services	Any number of startup activities could cause this problem. If the problem re-occurs, something is peculiar in the environment of the restore process and further investigation is necessary to determine the source of the problem. Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur.
1803	RESTORE Volume access failed. Retry Restore.	A problem exists accessing the restore device. This could be an invalid restore device, the tape drive requiring cleaning, or a table header format problem (internal error). Verify the following: • The backup/restore device is administered properly (name corresponds with the operating system administered device). • The tape compatibility is correct (320 meg tape for 320 meg drive, etc.). • The tape drive is clean.

Table continues...

Error Code	Message	Reason/Action
1804	RESTORE Error in process communication. Retry Restore.	A bad message was received either by the restore screen or the restore process. If this occurs, some sort of interference occurred in the message queue between the restore process and the restore screen. If the problem re-occurs, something is impacting the communication between the processes. Further investigation is necessary to determine the source of the problem. Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur.
1805	RESTORE Table restore failed. Retry Restore. Table=	A problem was encountered either reading the indicated table from tape or writing that table into the database. Perform a specific table restore for the indicated table. Verify that the problem does not re-occur.
1806	RESTORE INFO: Volume contains no data for ACD=X	This is an Information message indicating that the current table for the indicated ACD does not have data. No action required.
1850	RESTORE Screen startup failed. Contact Services.	Any number of startup activities could cause this problem. Most problems result from accessing screen entries that should never be encountered. If the problem re-occurs, something is peculiar in the environment of the restore process and further investigation is necessary to determine the source of the problem. Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur.
1851	RESTORE Screen execution failed. Retry Restore.	Updating the status on the screen could cause this problem (although extremely rare). If the problem re-occurs, something is peculiar in the environment of the restore process and further investigation is necessary to determine the source of the problem. Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur.

Table continues...

Error Code	Message	Reason/Action
1900	SYSTEM ME SSA GE OVERLOAD: Agent Trace (AAR) is overloaded, some agent trace data lost. Turn off traces for some agents to prevent possible further overloading.	AAR is receiving messages faster than it can process them. Turn off traces for some agents.
1900	SYSTEM ME SSA GE OVERLOAD: Call History Recorder (ch_rec) overloaded, some call record data lost.	Data is being sent faster than it can be processed. This usually indicates that the system as a whole is overloaded. Stop some reports or applications so that the system capacity is increased.
1901	FULL DISK ERROR: Out of disk space. Data Collection failed (Archiver).	Enough disk space is not available for the insertion of daily/weekly/monthly archive data. Free up disk space or add more disk space in the form of additional hard disks.
1901	FULL DISK ERROR: Out of disk space. Harchiver could not write to <TABLENAME>.	Enough disk space is not available for the insertion of agent login/logout or interval archive data. Free up disk space or add more disk space in the form of additional hard disks. If the problem persists, call Services.
1901	FULL DISK ERROR: cannot write to xxx.	The filesystem or ACD dbspace is out of disk space. Use Data Storage Allocation to adjust the amount of space available to the ACD.
1901	FULL DISK ERROR:	There is no more disk space to load the data for this pseudo-ACD. The load ACD process cannot continue. Delete the pseudo-ACD and start over again using a later "Start date" for the pseudo-ACD and load less data. Reduce the amount of historical data kept in other ACDs.

Table continues...

Error Code	Message	Reason/Action
1901	FULL DISK ERROR: Automatically turning off data collection and bringing CMS to single user mode	All ACD dbspaces are checked for free space every 10 minutes. By turning off data collection and going to single user mode, CMS prevents corruption of the data that may occur if IDS tries to write data to a full ACD dbspace. CMS cannot be returned to its normal operational state until space has been made available in the ACD dbspace. Use Data Storage Allocation to adjust the amount of space available to the ACD.
1901	FULL DISK ERROR: WARNING: File system <filesys> is <NN> percent full.	This message is logged once each day near midnight and whenever CMS is started. The message is logged once for each file system or ACD dbspace that is at or beyond 80 percent of maximum capacity. This message is intended as an early warning that disk space may need to be reallocated. No immediate action is necessary.
1901	FULL DISK ERROR: Storage Interval Migration failed migrating	The disk or ACD dbspace is out of space. Use Data Storage Allocation to adjust the amount of space available to the ACD.
1901	FULL DISK ERROR	The dbspace containing the ag_actv database table is full. Change the allocation of disk space for the various classes of data to accommodate storage of more agent trace records.
1901	FULL DISK ERROR: Out of disk space. Call Records not recorded.	The dbspace containing the call_rec database table is full. Change the allocation of disk space for the various classes of data to accommodate storage of more internal call records.
1901	FULL DISK ERROR: Call Records not being stored. Call Services.	The dbspace containing the external call records files is full. Call Services.
1902	CALL RECORD ERROR: Call Records not being stored. Call Services.	An error was encountered in writing call records to a disk file. Call Services
1902	ALL RECORD ERROR: Call Records are being collected again.	Previous errors writing files have been cleared and records are again being stored. No action necessary.

Table continues...

Error Code	Message	Reason/Action
1902	CALL RECORD ERROR: Call Records not being stored, buffer area is full. Call Services	Files containing call records have not been successfully transferred. All storage space has been used and new records cannot be added. Call Services.
1902	CALL RECORD ERROR: Call rate exceeded capacity: xxx calls not transmitted	The internal Call History feature is activated but the call rate exceeds the maximum capacity handled by this feature; therefore, call records are not being sent to the Call History feature. This message indicates how many calls were not sent in the past data collection interval. This has no effect on the collection of regular data. Call Services.
2000	Could not run timetable: - Aborting Timetable. <timetable name>	Something is wrong with the timetable which is not allowing properly functionality. Try rescheduling the timetable. Consult the section on using timetables to see if there are erroneous tasks in the timetable.
2000	Could not run timetable: <timetable name> Task <number> of <total> was unable to complete. Reason: <reason>	A timetable task is in error. One common possibility is that the user does not have permissions for the split, vdn, etc. for which they are running reports.
2000	Could not run timetable: don't run timetable, in single user timetable = <timetable_name> <user_name>	Timetables cannot run when CMS is in single user mode. An administrator has put CMS in single user mode as required by some special administrative tasks. The severity of the problem is that the user's timetables are not being run when expected. Schedule the timetables that should have run to be performed as soon as possible and then reschedule those timetables back to their original times. Schedule their timetables to run at a time that does not conflict during the time when CMS needs to be in single user mode.
2000	Could not run timetable: sorry post office open of timetable crt_io_man was not successful for timetable - <timetable name> and <cms id> - <user name>.	Communications cannot be established with a crt_io_man in order to run the timetable. Try rescheduling the timetable.

Table continues...

Error Code	Message	Reason/Action
2000	Could not run timetable: -- Archiver <timetable name> did not run on <date> for the user - <user name>. Please schedule it to rerun using the Data Summarizing screen.	The Archiver has a problem in moving historical data into tables for the timetable to use. Call Services.
2000	Could not run timetable: -- Archiver <timetable name> did not run on <date> for the user - <user name>. To schedule a timetable to run as soon as possible, enter a cms start time that is two minutes into the future, and a start date of 0.	A user scheduled a timetable to run in less than two minutes into the future. Reschedule the timetable for at least two minutes into the future.
2100	Unable to execute <process>. <Impact-description>. Call Services.	The specified process could not be executed. The impact is usually the failure of a major component of CMS such as Agent Trace, Exceptions, or Data Collection. This problem can usually be repaired by stopping CMS and restarting it. Call Services.
2200	Sometimes the problem can be repaired by stopping CMS and restarting it. <table>	An error was encountered during migration. Call services for assistance.
2300	INTERVAL MIGRATION: Interval migration was canceled before it completed. Restart it from the Storage Intervals screen to complete the migration	The migration was canceled manually before it completed. Restart the migration from the Storage Intervals screen.
2300	INTERVAL MIGRATION: Migrating intrahour historical data for ACD xx from xx to yy minute interval is complete.	This message indicates when intrahour migration is complete. No action required.
2400	FREE SPACE ALLOCATION: <error message>	This type of error message specifies that the Free Space Allocation feature has suffered a problem in locating or updating database tables. Contact services.
2500	STORAGE INTERVALS: Weekly start/ stop day(s) have been changed from xx to yy.	This is an informational message indicating that the Storage Interval days have changed. Verify that the new days are correct.

Table continues...

Error Code	Message	Reason/Action
2600	ARCHIVER status: Daily/Weekly/Monthly Archive not executed for xx/xx/xx due to Data Storage Allocation administration.	Data Storage Allocation indicates 0 days/weeks/months are to be saved; therefore, no reason to archive data exists. This is most commonly a result of an error in user input. If daily archives are desired, Days of Daily/Weeks of Weekly/Months of Monthly entries must be changed to allow an archive to take place. Disk space must be considered before changing these fields.
2600	ARCHIVER status: Daily/Monthly/Weekly Archiver for xx/xx/xx Successful.	Indicates successful completion of the daily/weekly/monthly archive. The status of previous and current archives also exists in /cms/dc/archive/arch.log. No action necessary.
2600	ARCHIVER status: Daily/Monthly/Weekly Archiver for xx/xx/xx Failed.	Indicates failure of the daily/weekly/monthly archive. The status of previous and current archives also exists in /cms/dc/archive/arch.log. Re-initiate an archive for the same date and archive type (daily/weekly/monthly) using the Data Summarizing screen.
2700	MIGRATE DATA Process out of sync. Call Services.	A bad message was received from the R3 Migrate Data screen. If this occurs, some sort of interference occurred in the message queue between the R3 Migrate process and the associated screen. If the problem re-occurs, something is impacting the communication between the processes. Further investigation is necessary to determine the source of the problem. Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not re-occur.
2701	MIGRATE DATA Process out of memory. Contact Services.	A problem with memory allocation has occurred. Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not re-occur.

Table continues...

Error Code	Message	Reason/Action
2702	MIGRATE DATA Process startup failed. Contact Services	Any number of startup activities could cause this problem. If the problem re-occurs, there is an error in the environment of the migrate process and further investigation is necessary to determine the source of the problem. Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not re-occur.
2703	MIGRATE DATA Volume access failed. Retry Restore.	A problem exists accessing the migration device. This could range from: • Invalid migration device • Tape drive needs cleaning • Table header format problem (internal error). Verify the following: • The backup/restore device is administered properly (name corresponds with the operating system administered device) • The tape compatibility is correct (320 meg tape for 320 meg drive, etc.). • The tape drive is clean.
2706	MIGRATE DATA Table migration failed. Retry Migrate. Table=	A problem was encountered either reading the indicated table from tape or writing that table into the database. Stop the migration and call Services for help with the table that failed. After the problem is fixed, restart the migration.
2708	MIGRATE DATA Error in process communication. Retry Restore.	A bad message was received either by the R3 Migrate Data screen or the migration process. If this occurs, some sort of interference occurred in the message queue between the migration process and the R3 Migrate Data screen. If the problem re-occurs, something is impacting the communication between the processes. Further investigation is necessary to determine the source of the problem. Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not re-occur.

Table continues...

Error Code	Message	Reason/Action
2750	MIGRATE DATA Screen startup failed. Contact Services.	Any number of startup activities could cause this problem. Most can be attributed to accessing screen entries that should never be encountered. If the problem re-occurs, something is in error in the environment of the migrate process and further investigation is necessary to determine the source of the problem. Exit the current instance of the R3 Migrate Data screen and re-initiate the migrate. Verify that the problem does not re-occur.
2751	MIGRATE DATA Screen execution failed. Retry Migrate.	This error can result when an update to the R3 Migrate Data screen fails. If the problem re-occurs, something is in error in the environment of the migrate process and further investigation is necessary to determine the source of the problem. Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not reoccur.

Chapter 13: Scheduling for administration jobs

Scheduling is available in the Web Client. Use this chapter to set up an administration scheduling job. For information about setting up scheduling for reports, see *Avaya CMS Supervisor Reports*.

You can schedule an administration job from the Change Agent Skills and Multi-Agent Skill Change pages under the Agent Administration subsystem and the Back Up Data page under the Maintenance subsystem. Set up scheduling if an agent needs to handle different types of calls at different times. Scheduling is not currently available for other administration menus.

After setting up scheduling, you can view and manage all your scheduling jobs from the Scheduler page. For example, you can modify a scheduling job, pause it, or cancel it. You can also view the status of each job to see if it succeeded or failed.

Related links

[Agent skill changes](#) on page 151

[Multi-agent skill changes](#) on page 160

Setting up scheduling

About this task

After you click **Schedule** on the Change Agent Skills, Multi-Agent Skill Change, or Back Up Data page, the Schedule Administration window is displayed. Use this window to set up scheduling.

Procedure

1. In the **Job Name** field, type a name for the job you are scheduling.
2. Select one of the following **Schedule Type** options:
 - **Once**: To schedule a single job for a specific date and time. For example, you can use this option before a unique, one-time event to ensure that agents can focus on calls for the event.
 - **Daily**: To schedule a job at the same time every day or every few days. For example, you can configure the job to run every two days.
 - **Weekly**: To schedule a job for specific days every week. You can select one or more days.

- **Monthly:** To schedule a job on the months and days you specify. For example, you can set up scheduling for the last Friday in September and December.
3. If you set **Schedule Type** to **Once**, do the following:
 - a. In the **Date** and **Time** fields, specify when the job will run.
 - b. In the **Retain results for** field, type the number of days for which job results will be retained in the database.
 - c. Click **Schedule** to complete the scheduling process.
 4. If you set **Schedule Type** to **Daily**, do the following:
 - a. Under the First Run heading, complete the **Date** and **Time** fields to specify when the job will run for the first time.
 - b. In the **Run every** field, type a number to specify how many days apart the job will run.
You can specify any number of days. For example, if you type 1, the job will run every day. If you type 3, it will run every 3 days.
 - c. Under the Expire heading, specify an end date and time after which the job will no longer run.
 - d. In the **Retain results for** field, type the number of days for which job results will be retained in the database.
 - e. Click **Schedule** to complete the scheduling process.
 5. If you set **Schedule Type** to **Weekly**, do the following:
 - a. Under the First Run heading, complete the **Date** and **Time** fields to specify when the job will run for the first time.
 - b. Under the Run on heading, select one or more days of the week.
For example, you can select the check boxes for Tuesday, Thursday, and Friday. Jobs run every week on the specified days.
 - c. Under the Expire heading, specify an end date and time after which the job will no longer run.
 - d. In the **Retain results for** field, type the number of days for which job results will be retained in the database.
 - e. Click **Schedule** to complete the scheduling process.
 6. If you set **Schedule Type** to **Monthly**, do the following:
 - a. Under the First Run heading, complete the **Date** and **Time** fields to specify when the job will run for the first time.
 - b. Under the Months heading, select one or more months.
For example, you can select the check boxes for February, June, and September.

- c. Select one of the following options:
 - Select **Days** to select one or more dates. For example, select **2** and **Last** to run the job on the second and last days of the specified months.
 - Select **On** to specify which week and day the job will run. For example, you can run the job on the second Friday of the specified months.
- d. Under the **Expire** heading, specify an end date and time after which the job will no longer run.
- e. In the **Retain results for** field, type the number of days for which job results will be retained in the database.
- f. Click **Schedule** to complete the scheduling process.

Next steps

After setting up scheduling, navigate to the Scheduler page to view and manage your scheduled jobs.

Scheduler page descriptions

After setting up scheduling in the Web Client, click **Scheduler** to view and manage your scheduled jobs. You can view report jobs, administration jobs, or all jobs. This section is focused on administration jobs.

The Jobs table on the Scheduler page displays information about each job. It also provides actions that you can perform to manage each job.

When you click a job in the table, historical data is displayed in the Job Detail area. You see information about each scheduled run for the job. For each item displayed, you can view results or delete the item.

The Jobs table displays the following information:

Job information	Description
Job Name	Displays the name of the scheduled job.
Action	Displays recent actions. For example, "Suspend" indicates that you temporarily suspended the job.
State	Displays the status of the job. For example: • "Active" indicates that the job is active and will continue to run as scheduled. • "Complete" indicates that the job is complete. For example, this status is displayed if you scheduled a one-time job that has already run. • "Suspended" indicates that you temporarily suspended the job.
Last Run	Displays the date and time for the previous run.

Table continues...

Job information	Description
Result	Indicates whether the last run was successful.
Next Run	Displays the date and time for the next scheduled job run. This information is displayed for active jobs.
Type	Displays the schedule type for the job. For example: Once, Daily, Weekly, or Monthly.
Interval	Displays the interval at which the job is scheduled. For example, if a Daily job is scheduled to run every day, the interval is 1.
ID	Displays the job ID. CMS generates this ID automatically.
Expire	Displays the end date and time when the job will run for the last time.
Retention	Displays the number of days the scheduled job is stored in the database. The number of days job results can be retained for depends on the maximum retention setting, which varies based on the schedule type. For example, by default, Daily jobs can be retained for up to 10 days. The maximum retention settings are customizable.

Action icons are available in the main Jobs table and the Job Details area:

Action	Available in main Jobs table	Available in Jobs Details area	Description
	Yes	No	In the main Jobs table, click to resume a suspended job. The job continues to run as scheduled.
	Yes	No	In the main Jobs table, click to suspend the job temporarily. The scheduled job will not run until you resume it.
	Yes	No	In the main Jobs table, click to cancel the job. You cannot resume the job after canceling it.
	Yes	No	In the main Jobs table, click to run the job immediately. You can view the results when they are ready. After this, the job continues to run as scheduled.
	Yes	Yes	In the main Jobs table, click to view results for the latest available job. If there are any errors, you can view the same. In the Job Details area, this option is displayed next to each available item. Click it to view specific job results. If there are any errors, you can view the same. This option is grayed out if results are not available to view.

Table continues...

Action	Available in main Jobs table	Available in Jobs Details area	Description
	Yes	No	In the main Jobs table, click to edit the job name and scheduling options. For example, you can change the days when the job is run. Note that this icon might not be available depending on the job status. • If the job details are available when you edit the job schedule, the Schedule Administration window displays the Schedule and the Job Detail tabs. • If the job details are unavailable when you edit the job schedule, the Schedule Administration window displays the job schedule.
	Yes	No	In the main Jobs table, click to view the jobs that are either canceled or expired. • If the job details are available when you view the job schedule, the Schedule Administration window displays the Schedule and the Job Detail tabs. • If the job details are unavailable when you view the job schedule, the Schedule Administration window displays the job schedule.
	Yes	Yes	In the main Jobs table, click to delete the job and all associated details. In the Job Details area, this option is displayed next to each available item. Click it to delete an entry.

To refresh the page after making changes, you can click  at the top of the page.

Customizing the maximum retention settings

About this task

Use the command line interface to configure the maximum number of days that data can be stored in the database. You can set different retention values for one-time, daily, weekly, and monthly data.

Before increasing the maximum data retention period, ensure that you have enough free space on your server. Do not retain data for longer than you need.

Procedure

1. Log in to the CMS server with root privileges.
2. Edit `/opt/cmsweb/data/system.properties` to customize the maximum retention values.

The retention values are displayed in the following format, where each number represents the maximum number of days for which data can be retained:

```
OnceMaxRetention=10  
DailyMaxRetention=10  
WeeklyMaxRetention=30  
MonthlyMaxRetention=70
```

You can change one or more numbers. For example, if you want to retain Daily data for up to 15 days, you can change the `DailyMaxRetention` value from 10 to 15.

Chapter 14: Scripting CMS operations

Scripting CMS operations

Scripting enables the automation of tasks such as running reports, exporting report data, and other operations.

 Note:

CMS scripting is available only using the PC Client.

Before you begin scripting CMS operations

Before a script can be run through CMS Supervisor, the following conditions must be met:

- The username associated with an automatic script must be assigned all the permissions required for all operations specified by the script.
- No more than four scripting CMS Supervisor sessions, including background sessions initiated by automatic scripts, can be run simultaneously on a PC.

 Caution:

When using scripts to change VDNs, verify that only one script is running at a time. If multiple scripts execute in parallel that are all changing VDNs, some VDN changes may not finish.

- The PC must be running at the time when an automatic script is scheduled to run.
- Once a script is created, it can be started by accessing the script file directly from a Microsoft Windows Explorer window.
- You must schedule mission-critical activities, such as backups, through Timetables on the CMS Supervisor server. For more information about Timetable scheduling, see [Creating and scheduling a timetable](#) on page 425.

Tasks scripts can automate

Scripts can be used to automate several CMS tasks, such as:

- Running reports
- Exporting data from reports
- Performing Dictionary operations and reports

- Administering Exceptions and requesting Exception reports
- Performing Agent Administration operations
- Performing Call Center Administration operations and reports
- Performing System Setup operations
- Performing Maintenance operations and viewing the Error Log
- Administering User Permissions

Interactive and automatic scripts

Each script is designated to be either interactive or automatic, as defined below:

- An interactive script runs in the current CMS Supervisor session and the actions display on the PC. If the CMS Supervisor session is disconnected from the CMS server, the script will not run.
- An automatic script launches a new Supervisor session that logs into CMS and runs the requested tasks as a background process. Script actions are not displayed on the screen. Although CMS Supervisor provides the ability to create automatic scripts, a third-party scheduling program must be used in order to run the scripts automatically on a regular schedule.

Script creation

This section describes how to create interactive or automatic scripts used to run reports. Interactive and automatic scripts used to run reports have the following differences:

- An *interactive* script runs in the current Supervisor session and the actions display on the PC. If the CMS Supervisor session is disconnected from the CMS server, the script will not run.
- An *automatic* script launches a new Supervisor session that logs into CMS and runs the requested tasks as a background process. Script actions are not displayed on the screen. Although Supervisor provides the ability to create automatic scripts, a third-party scheduling program must be used in order to run the scripts automatically on a regular schedule.

Accessing scripts

Procedure

Scripts can be created and accessed through the **Scripts** button found on several dialog boxes. Dialog boxes containing the **Scripts** button can be accessed through the following menu selections:

- **Commands > Reports**
- **Commands > Dictionary**
- **Dictionary > Exceptions**
- **Commands > Agent Administration**
- **Commands > Call Center Administration**

- **Tools > System Setup**
- **Tools > Maintenance**
- **Tools > User Permissions**

Scripts can also be accessed from agent administration windows or once a report is run. The **Scripts** button is also available when you use any other Supervisor command or tool that allows you to add or change objects.

Accessing the script options

About this task

Before you create scripts, you should be aware of the different options and behaviors available for scripts.

Procedure

Select **Tools > Options > Scripting**.

The Scripting dialog provides the fields required to set the scripting options, which are described in [Scripting options description](#) on page 411.

Scripting options description

Name	Description
User ID	This read only ID allows automatic scripts to make their connection to the CMS server. The login ID and password are not validated until an automatic script is run.
Set User	You must specify a CMS user ID and password before you can run any automatic scripts. For more information, see Setting user ID and password on page 412
Logging Level	The extent to which script-related activities and outputs are logged, according to the following criteria: • Minimum - Logged activities are limited to those errors and messages from CMS Supervisor which would otherwise be displayed when the scripts are run manually. • Normal - Logged activities include those recorded at the Minimum setting, plus the following information: task start time; task end time; name of the script. • Maximum - Logged activities include all those recorded at Minimum and Normal settings, plus additional error messages which may be useful for debugging a script.

Table continues...

Name	Description
Log File Path	Allows you to specify a non-default file directory path. Selecting the folder icon to the right of this field also lets you browse the file system to select a log file directory.
Log File Size	Allows you to specify the size of the log file before it rolls over and begins to overwrite itself.

Setting user ID and password

Before you create an automatic script, you must set a user ID and password to allow the script to log into CMS. If you do not set the ID and password beforehand, you are prompted to do so the first time you save an automatic script.

Setting users procedure

Procedure

1. Select **Tools > Options > Scripting**.
2. Select **Set User**.
3. Enter your CMS login ID in the **User ID** field.
4. Enter your password in the **Password** field.
5. Enter your password again in the **Confirm Password** field.
6. Select **OK**.

The two password entries are checked to make sure they match. If they do not, the message `Passwords do not match` appears and you remain in the window. If they match, your user ID and password are encrypted and saved and are used to log in when this or any automatic script is run.

Your user ID and password are not verified with the server at this time. The only way to check if they are correct is to attempt to run an automatic script and check the script log to see if the script ran successfully.

Scripting reports

Creating an interactive report script

Procedure

1. Select **Commands > Reports** from the Controller window menu bar.

CMS Supervisor displays the Reports window.

2. Select the tab associated with the type of report you want to run (Real-Time, Historical, or Integrated), and then highlight the report from the categories and listings which are displayed.
3. Select the **Script** button on the report selector window.

CMS Supervisor displays the Save as Script window.

4. Select a directory and file name for the script and select **Save**.

CMS Supervisor closes the Save as Script window and returns you to the report selector window.

Creating an automatic report script

Procedure

1. Select **Commands > Reports** from the Controller window menu bar.

CMS Supervisor displays the Reports window.

2. To select a report for scripting, select the appropriate report type from the dialog box tabs, highlight the report, and select **OK**.

CMS Supervisor displays the input window for the selected report.

3. Enter the appropriate data in the input window and run the report by selecting **OK**.

CMS Supervisor displays the selected report.

Note:

If a historical report was selected, set the **Destination** controls to **View Report on Screen**.

4. In the dialog displayed for the report, select **Reports > Commands > Script** from the main menu.

CMS Supervisor displays the Save as Script window.

5. Select a directory and file name for the script. The file type is set to **Automatic** by default.
6. Select **Save**.

Executing this automatic script causes the report to run with the inputs provided during its creation.

Creating a script to export report data

Procedure

1. Run a report and display it to screen.

CMS Supervisor displays the window for the selected report.

2. From the **Edit** menu of the report window, select one of the following actions:

- **Export Chart Data**
- **Export Table Data**
- **Export All Data**

The data export dialog box is displayed. The dialog that is displayed will vary according to which export option is selected.

Some of these options can also be selected from a pop-up menu by performing a right-click in the report window.

3. Set the appropriate options in the data export dialog, and then select the **Script** button.

 Important:

Do *not* select **OK** after the options are selected.

CMS Supervisor displays the Save as Script window.

4. Select a directory and file name for the script, and set the file type to either **Interactive** or **Automatic**.
5. Select **Save**.

Creating a script to export report data as HTML

Procedure

1. Select a report that you want to export as HTML and display it to the screen.

CMS Supervisor displays the report window.

2. From the menu bar of the report window, select **Reports > Save As**.

CMS Supervisor displays the Save as HTML window.

3. Select the appropriate option from the **Template** group.

A template can be used to provide company logos, background color, specific fonts, or surrounding text to the HTML file. If you do not select a template, the export process generates basic HTML tags to display the report.

CMS Supervisor provides you with several templates that can be found in the `\samples` directory of the main CMS Supervisor directory.

4. In the **Output** field, select a name for the HTML file you are creating.

To save the file in a directory other than the current directory, specify a full file path, such as `c:\temp\myrpt.htm`. You may also use the browse button located to the right of this field to navigate to a target directory.

5. Select the **Script** button.

CMS Supervisor displays the Save as Script window.

6. Select a directory and file name for the script, and set the file type to either **Interactive** or **Automatic**.
7. Select **Save**.

If there are charts associated with the file, they are converted into `.GIF` files. After the HTML is saved, you can move or copy it and all associated graphics files to a web server directory for viewing on the Internet or an Intranet.

Scripting operational tasks

This section provides information on the procedures used to create and save scripts for operational tasks, that is, actions not associated with reports. Operational tasks include:

- Displaying an input window for actions, not reports, requiring data entry when the script is run.
- An **Add**, **Modify**, or **Delete** action.

About scripting an input window

This procedure describes how to create a script that displays an input window for a specific, non-report operation. Executing the script displays the input window for the operation selected when this script was created.

Actions associated with the following functions can be captured in a script:

- Dictionary
- Exceptions
- Maintenance
- System Setup
- Agent Administration
- Call Center Administration

Scripting an input window

Procedure

1. Select the necessary item from the **Commands** menu on the Controller window.

CMS Supervisor displays the associated selector window for the item selected.

Important:

Do not double-click the option or press the `Enter` key when an operation is highlighted or the action will be initiated and the script recording will be aborted.

2. Highlight the operation to be made into a script from the **Operations** list on the Operations tab of the selector window and then select the **Script** button in the selector window.

CMS Supervisor displays the Save as Script window.

The file type is set to **Interactive** by default.

3. Complete the Save as Script window by entering a file name and folder location and then select **Save** when finished.

CMS Supervisor displays an acknowledgment message to indicate that the script has been saved.

4. Select the **OK** button on the acknowledgment message box.

CMS Supervisor closes the Save as Script window and the selector window remains open.

Scripting an action

About this task

Use this procedure to create a script that results in the execution of an action. Running the saved script will cause an add, modify, no action, or delete action to be performed for the selected operation.

Caution:

When using scripts to change VDNs, verify that only one script is running at a time. If multiple scripts execute in parallel that are all changing VDNs, some VDN changes may not finish.

Valid items for scripting an action include:

- Dictionary
- Exceptions
- Maintenance
- System Setup
- Agent Administration
- Call Center Administration

Procedure

1. Select the necessary item from the **Commands** menu on the Controller window.

CMS Supervisor displays the selector window associated with the selected item.

2. Highlight the operation to be made into a script from the **Operations** list on the Operations tab of the selector window.
3. Select the **OK** button.

CMS Supervisor displays the input window for the selected operation.

4. Select **Actions > Scripts** from the menu bar of the input window.

If none of the valid scriptable actions, **Add**, **Modify**, or **Delete**, are present, you cannot select **Script**.

CMS Supervisor displays the Save as Script - Action window.

5. Select the action to be performed by the script.
6. Select the **OK** button.

CMS Supervisor displays the Save as Script window.

 Note:

If the **Cancel** button is selected, Supervisor dismisses this window and displays the input window without saving an action.

CMS Supervisor displays the Save as Script window.

 Note:

If the **Cancel** button is selected, CMS Supervisor dismisses this window and displays the input window without saving an action.

7. In the Save as Script window, select a file folder location and file name.
8. Specify the script type as either **Automatic** or **Interactive**.
9. Select **Save**.

CMS Supervisor displays an acknowledgment message box stating that the script has been saved.

10. Select the **OK** button on the acknowledgment message box

CMS Supervisor displays the Save as Script - Action window.

Organizing scripts

About this task

The Organize Scripts window provides a simple file management interface which allows you to rename, delete or move script files.

Procedure

1. Select **Scripts > Organize Scripts** from the menu bar on the Controller window.

CMS Supervisor displays the Organize Scripts window.

2. Perform actions on the scripts as needed.

This can include renaming, deleting, and moving.

3. When you are finished organizing scripts, select **Close** to exit the Organize Scripts window.

Error and warning messages

This section lists possible error messages which may be encountered when running scripts and describes their associated causes and possible solutions.

Table 1:

Message	Reason	Solution
This script will not run unless a CMS login ID and password have been specified.	The CMS login ID and password have not been set on the Scripting tab of the Controller Options window.	Specify a login ID and password on the User Information window.
Automatic scripts are set to run with the permissions of another user of the PC.	The User Information window designates the other user as the owner of automatic scripts.	You can change the permissions via the login information on the Scripting tab of the Controller Options window. The change will apply to subsequent automatic scripts that are run on the PC.
(Action) Supervisor displays the Save as Script: Add or Replace window.	The file already exists.	Select one of the following actions at the bottom of the window: • Add (default) - Adds the new script to the end of the existing script • Replace - Deletes the existing script and create a new script file • Cancel - Closes the Add or Replace window and returns to the Save as Script window • Help - Displays the help topic for the current window.

Chapter 15: Using the operating system to access CMS and manage passwords

The CMS server uses the Linux operating system. To perform some administrative tasks, you must use the CMS command line interface. This chapter provides high-level information about how to log in to the CMS server and how to manage passwords from the command line interface.

CMS server login

Some administration tasks are not available through CMS Supervisor. To perform these tasks, you must use the command line interface. You can log in to the CMS server from the remote console or your virtual machine web console.

Logging in to CMS from the remote console

About this task

You can log in to the CMS server from a remote console. For example, you can use Terminal Emulator to log in to CMS.

Ensure that users do not use the same login ID because this will use up operating system processes.

Before you begin

Configure the connection settings for the CMS server you are logging in to. For example, select the **SSH** connection type and then specify the CMS network address and port number.

Procedure

1. Open the console.
2. When prompted, enter your login ID.
For example, type `cms` and then press `Enter`.
3. Enter your password when prompted.
A prompt for the terminal type is displayed.

4. Enter your terminal type when prompted or accept the default option.

If you use a login other than “cms”, the CMS Main Menu opens automatically. If you are using the “cms” login, you must run the `cms` command after entering your password to view the Main Menu.

Logging in to the CMS server from the virtual console

About this task

You can use the virtual machine web console to access CMS. For example, if CMS is deployed through Red Hat KVM, you can use the Red Hat web console to access the CMS server.

Important:

You cannot log in to the console with the `/usr/bin/cms` shell. Use a login account with a shell such as `/bin/bash` or `/bin/ksh`.

About this task

Ensure that the CMS virtual machine is deployed. For more information, see *Deploying Avaya Call Management System*.

Procedure

1. Open the web console for your virtual environment and ensure that your virtual machine is running.
2. Navigate to the Console area for the virtual machine.

For example, you can use the VNC console option.

Administering passwords

For system security, passwords are required for all CMS user login IDs. If a password is not entered on your first login, the system will prevent you from continuing until one is supplied.

CMS users can enter and change their passwords, but only a CMS administrator working on the CMS operating system or using the Web Client can reset a forgotten password.

For more information about how to change passwords using the Web Client, see [Password management in the Web Client](#) on page 179.

Considerations for password management

- Use the CMS ASCII interface to force a password change or administer password aging. You can access the ASCII interface through a Terminal Emulator connection or your virtual machine web console.
- Use a password with no less than six characters. The password must have at least one number or special character and a minimum of two alphabetic characters.

- When changing a password, the new password must have at least three characters that are different from the previous password.

Changing a user's password through the command line interface

About this task

As an administrator, you can use the command line interface to forcibly cause a user's password to expire. In this procedure, enter a new password for the user and then run the command that will force the user to change their password the next time they log in to CMS. This procedure is useful if the user forgot their password.

Procedure

1. From the CMS Main Menu, press **F3** to access the **Commands** menu.
2. Select the Unix option.

The screen clears and a `$` prompt is displayed.

3. Run the `su` command.
4. When prompted, enter the root password.
5. Run the `passwd <userid>` command.

Replace `<userid>` with the ID of the user whose password needs to be changed.

6. When prompted, enter a new password for the user.
7. When prompted, enter the password again to confirm it.
8. At the command prompt, run `chage -d 0 <userid>` to force the user to change their password the next time they log in.

Replace `<userid>` with the ID of the user whose password you just changed.

9. At the command prompt, enter `exit` and then press **Enter**.

Repeat this step to return to the main menu.

Enabling password aging

About this task

When password aging is disabled, passwords do not expire. You can turn on password aging if you want user passwords to expire after a set number of weeks. You can set the number of weeks between 1 and 52. When this period of time elapses, CMS users are forced to change their passwords.

To manage the password aging feature, you must use the CMS ASCII interface. This feature is not accessible through CMS Supervisor.

This high-level procedure describes how to enable password aging. For more information about password aging, see *Maintaining and Troubleshooting Avaya Call Management System*.

Procedure

1. From the CMS Main Menu, press **F3** to access the **Commands** menu.
2. Enter **1** to turn password aging on.
3. When prompted to enter the number of weeks before passwords expire, enter a value between 1 and 52.

If you press **Enter** without specifying a value, passwords will expire after 9 weeks by default.

Chapter 16: Using timetables and shortcuts

This chapter provides information about creating and administering timetables and shortcuts. Timetables and shortcuts are used to run multiple administrative tasks and are only available through the CMS ASCII interface.

You can access the CMS ASCII interface through:

- Terminal Emulator.
- Virtual console to the CMS server. For example, you can access CMS from the Red Hat KVM console.

Timetables

A timetable is a CMS feature that enables the scheduling of one or more administrative tasks. Each timetable can consist of up to 100 tasks and can be scheduled to run at any specific time. When you are creating a timetable, CMS records the tasks you perform and includes them in the timetable. This feature is similar to macros in many PC applications that perform multiple tasks or actions when the single macro is run.

Timetables are better suited for mission-critical tasks than Supervisor scripts. This is due to the fact that scripts reside on the PC where they were created. If network difficulties occur or if the PC where the script resides is powered down, the script cannot run. Timetables run directly on the CMS server and do not suffer from such problems.

Before using timetables

The following items should be read and understood before working with timetables.

General

- You cannot schedule real-time reports, Vector Contents, or custom report creation through a timetable.
- Timetables run in the background, not in the terminal session.
- Timetables that fail at some point during execution are logged in the Maintenance Error Log Report.
- Up to five timetables can be scheduled to run at the same time.
- You can have tasks associated with different ACDs in the same timetable.

- Do not create a timetable that attempts to write a file in the home directory of different user.
- The ACD that is currently selected when a timetable task is created will be the ACD on which the task runs. To change the ACD, you must delete the task and reset the current ACD before adding the correct task.
- When a CMS user is deleted, any timetables associated with that user ID are also deleted. For this reason, it is recommended that mission-critical timetables be created under the `cms` user ID.
- If the System Administration Terminal (SAT) terminal is still logged in to the Communication Manager system and is displaying a screen used in timetables, those timetables will not run.
- Timetables cannot run if CMS is in single-user mode.

Printing

- You cannot select the terminal as the destination for report output through a timetable.
- To print a report more than once from a timetable, you must enter a task for each copy of the report.
- Print jobs from timetables go to the default printer for the user who owns the timetable unless otherwise specified when the timetable is created. If the default printer for a user is changed, there is no need to edit the timetable as CMS automatically sends the print jobs from the timetable to the new default printer.
- If a user specifies a printer other than their default printer for a timetable task and that printer is out of service, the timetable will not execute.
- If the printer jams while attempting to print timetable tasks, you must resubmit the request that did not print.

Backups

- Timetables for incremental and full backups are created when the system is installed, but are not scheduled.
- Be sure to schedule backups to run either before archiving begins or after archiving has been completed.

Permissions for timetables

Depending on the procedure that you want to perform, you need the following permissions:

- To view timetables, the user ID used to log in to this CMS session requires “read” permission for the Timetables feature, the requested CMS actions, and any ACD entities accessed by the timetable.
- To add, delete, or modify timetables, the user ID used to log in to this CMS session requires “write” permission for the Timetables feature.
- Users who are not Administrators can view and copy timetables from other users, but they cannot add, delete, or modify the timetables or the task entries.
- Users with Administrator permissions can add, delete, and modify timetables created by other users.
- If a timetable contains tasks for which the user does not have adequate permissions, the timetable will fail.

Creating and scheduling a timetable

About this task

This topic provides the procedure for creating and scheduling a timetable through the CMS ASCII interface.

Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK), using one of the following methods, depending on the connection method:
 - For Terminal Emulator, select the F4 key.
 - From the CMS console, press the F4 key.
 - For a telnet session from a PC, press Ctrl+P+4.
2. Select **Timetable name** and press the Enter key.

CMS displays the Timetable window.

The screenshot shows the 'Timetable' window in a terminal-like interface. The window has a title bar 'Timetable' and a window name 'test1'. The main area contains the following fields and options:

- Timetable name:
- Description:
- User ID: cms
- Start time:
- Start date:
- Frequency and attributes (Select only one):
 - ☒ Once
 - ☐ Dates:
- ☐ Hourly, Stop time: 11:59 PM
- ☐ Daily,
- Hourly/Daily Days (Select any you wish):
 - ☒ Sunday ☒ Tuesday ☒ Thursday ☒ Saturday
 - ☒ Monday ☒ Wednesday ☒ Friday
- This timetable will run on this or another CMS server
 - ☐ Run only on this CMS server*
 - ☒ Run on this or another CMS server*
- *These fields not used for Find one or List all

On the right side, there is a menu with the following options: Add, Copy, Delete, Find one, Get contents, Global edit, List all, Modify, Next, Previous. The window size is indicated as 21x68 in the bottom right corner.

3. In the **Timetable name** field, enter a unique name for this timetable. The name of the timetable cannot be changed after it has been created. Every timetable must have a unique name.

The following list provides the types of characters that can be entered in this field:

- Alphanumeric (A-z, 0-9)
- Underscore ()

- Blank ()
- Comma (,)
- Period (.)
- Single Quotation Marks (')
- Plus sign (+)

4. In the **Description** field, enter a description for the timetable.

This field is optional.

5. In the **User ID** field, the user ID currently logged in is displayed. If you are an administrator and want to create this timetable for another user ID, enter that user ID in this field.
6. In the **Start Time** field, enter the time when the timetable will be executed. If you do not wish to schedule the timetable at this time, leave this field blank.

This field can accept time in the following formats:

- HH AM/PM
- HH:MM AM/PM
- 24-hour (00:00 - 23:59)

If AM/PM is not specified, CMS assumes that the time entered is in the 24-hour format.

7. In the **Start Date** field, enter the date on which the timetable will begin running.

Use one of the following formats for entering the date in this field:

- MM/DD/YY - For example, 12/12/01. Do not enter four-digits years in this field.
- Relative format - For example, entering a 1 specifies the timetable will begin one day from today (tomorrow).

 Important:

If you do not wish to schedule the time table at this point, leave the **Start Time** and **Start Date** fields blank, ensure an **x** is in the **Once** field, and skip ahead to Step [11](#) on page 427.

8. In the **Frequency and attributes** group, choose from the following options:

- **Once** - This option runs the timetable one time for the date and time specified in the **Start Date** and **Start Time** fields. This is the default value for this field group.
- **Dates** - This option runs the timetable on specific dates. Enter the dates in the fields provided for this option.
- **Hourly** - This option runs the timetable each hour. In the **Stop Time** field, enter the time when the timetable should stop running.
- **Daily** - This option runs the timetable on the selected days in the **Hourly/Daily Days** group.

9. If the **Hourly** or **Daily** option was selected in the previous step, place an **x** next to the days in the **Hourly/Daily Days** group for which the timetable should run.
10. Place an **x** in one of the following options:

- **RunonlyonthisCMSserver** - The timetable will run only on this CMS server. If this timetable is backed up and migrated to another CMS server, it will not run.
- **Run on this or another CMS server** - The timetable is capable of running on this or any other CMS server. If this timetable is backed up and migrated to another CMS server, it will function normally.

11. Press the **Enter** key, highlight the **Add** item on the action list by using the arrow keys on the keyboard, and press **Enter** again.

The window displays a **Working** message. If the timetable name is currently present, **Already exists** displays on the status line and you must enter a different timetable name in the **Timetable name** field. If all entries are valid, the **Main Menu** displays with **Keeping Entries** displayed in the border.

12. Select a task from the CMS **Main Menu** that will be recorded to this new timetable.

CMS displays an **Entries Stored** in the status line of the current window when the task is run.

13. To run an historical report for the system:

- a. Select **Reports** from the **Main Menu**.
- b. Select **Historical**.
- c. Select **System**.
- d. Select **System**.
- e. Select **Daily**.

CMS displays the report window.

14. Enter the required information in the **Split(s)/Skill(s)** and **Date** fields.

The **Date** field can accept relative dates; for example, 0 represents today and -1 represents yesterday.

15. Press the **Enter** key to access the action list, select the menu item that performs the necessary action, and then press the **Enter** key again.

CMS displays a confirmation window.

It is possible to create more than one timetable task from a window. For example, suppose you want historical split/skill summary interval reports for skills 1 through 9, and you also want the same date and times for each report.

16. To create this report, perform the following steps:

- a. Go to the report window and enter 1 for the skill number, 0 for the date, and 8:00-16:00 for the times.

- b. Select **Run** on the action list. This creates a timetable task for skill 1.
 - c. Returning to the report input window, enter 2 for the skill number and select **Run** on the action list. This creates a timetable task for skill 2. Repeat the same process for skills 3 through 9.
17. Exit the window for the task and return to the **Main Menu**.
18. To add more tasks to the timetable, return to Step [12](#) on page 427. Otherwise, open the **Keep** SLK menu and then select the **Stop** option.
CMS displays a confirmation window asking if the timetable should be saved.
19. When CMS displays the confirmation window, press the `Y` key and then the `Enter` key to save the task.

 **Note:**
To exit the timetable at any time without saving your changes, select **Stop** from the **Keep** SLK menu and then enter `n` in the confirmation window.
20. Select the **Exit** SLK to close the Timetable window.

Adding tasks to a timetable

About this task

This topic provides the procedure for adding tasks to an existing timetable. This feature enables you to add tasks to a timetable in the same way you added tasks when you first created the timetable.

Procedure

1. From the CMS main menu, press `F4` (Keep).
2. Select **Timetable** and press the `Enter` key.

CMS displays the Timetable window.

Timetable test1

Timetable name:

Description:

User ID: cms

Start time:

Start date:

Frequency and attributes (Select only one):

☒ Once

☐ Dates:

☐ Hourly, Stop time: 11:59 PM

☐ Daily,

Hourly/Daily Days (Select any you wish):

☒ Sunday ☒ Tuesday ☒ Thursday ☒ Saturday

☒ Monday ☒ Wednesday ☒ Friday

This timetable will run on this or another CMS server

☐ Run only on this CMS server*

☒ Run on this or another CMS server*

*These fields not used for Find one or List all

21x68

Add
 Copy
 Delete
 Find one
 Get contents
 Global edit
 List all
 Modify
 Next
 Previous

3. Press **Ctrl+Z**.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable to which you want to add a task.
5. Press the **Enter** key.

CMS shifts focus to the action list.

6. In the action list, use the arrow keys to select **Get contents** and press the **Enter** key.

CMS displays the Timetable: Get Contents window.

Timetable: Get Contents test1

Task(s):

Timetable: Sample timetable Number of tasks: 10

Task	Action	Window Title
1	Run	Rpts: Hist: Agent: Summary: Interval Input
2	Run	Rpts: Hist: Agent: Summary: Daily Input
3	Run	Rpts: Hist: Agent: Summary: Weekly Input
4	Run	Rpts: Hist: Agent: Summary: Monthly Input
5	Run	Rpts: Hist: Agent: Split/Skill: Interval Input
6	Run	Rpts: Hist: Agent: Split/Skill: Daily Input
7	Run	Rpts: Hist: Agent: Split/Skill: Weekly Input

Add tasks
 Copy
 Delete
 Global edit
 Modify

test1 a510
test1 a510
test1 a510
test1 a510

103x132 >

7. In the **Task(s)** field, enter the number of the task that you want to precede the task being added.

If the task being added should appear as the fifth task, enter **4** in the **Task(s)** field.

To add a task to the beginning of the timetable, leave the **Task(s)** field blank. The new task is added before the first task.

To add tasks to a timetable with no tasks, leave the **Task(s)** field blank.

8. Press the `Enter` key.

CMS shifts focus to the action list.

9. Use the arrow keys to highlight the **Add tasks** item and press the `Enter` key.

CMS displays the **Main Menu** and is waiting for you to perform an action that it can add as a task. The status line of the **Main Menu** displays `Keeping Entries`.

10. Perform the task that you wish to have added to timetable.

For more information on the steps necessary in adding a task to a timetable, see Step [12](#) on page 425 in [Creating and scheduling a timetable](#) on page 425.

When the task is performed, CMS displays `Entries Stored` in the status line.

11. Exit the task window.

CMS displays the **Main Menu**.

At this point, more tasks can be added simply by performing them. These tasks will be added to the timetable in order following the previous task.

12. If you finished adding tasks to the timetable, open the **Keep** SLK menu and then select the **Stop** option.

CMS displays a confirmation window asking if the timetable should be saved.

13. Press the `Y` key and then the `Enter` key.

CMS saves the timetable with the newly added tasks and displays the **Timetable: Get Contents** window.

Listing all timetables

About this task

This topic provides the procedure for listing all timetables that currently exist in the CMS database. Listing all timetables can assist in finding specific timetables when you cannot remember the entire name of a timetable. It is also useful in helping to determine if too many timetables are scheduled to run at the same time.

Procedure

1. From the CMS main menu, press `F4` (Keep).
2. On the **Keep** SLK menu, select **Keep Timetable**.

CMS displays the **Timetable** window.

3. Press `Ctrl+Z`.

CMS clears the default information from all fields in the **Timetable** window.

4. Press the **Enter** key.

CMS shifts focus to the action list.

5. Using the arrow keys, move the cursor to the **List all** menu item and press the **Enter** key.

CMS displays the Timetable: List All window listing all timetables.

Timetable: List All				G3V5 eas
<u>Timetable Name</u>	<u>User ID</u>	<u>Status</u>	<u>Next Run</u>	<u>Start Time</u>
skh11.20.2	cms	finished		1:30 PM
temp7	cms			
temp9	cms	finished		1:30 PM
tst	cms			
4 matches found				7x240 >

Use the right- and left-arrow keys to scroll to the other fields in this window.

The following list describes the entries that can appear in the **Status** field.

- **Finished:** This message indicates that the timetable was scheduled to run once and it completed successfully.
- **Failed:** This message indicates that the timetable failed to run successfully for the last scheduled run time.
- **Successful:** This message indicates that the timetable completed successfully.
- **Unscheduled:** This message indicates that the timetable does not have a start time or start date.
- **Running:** This message indicates that the timetable is currently running.

Copying a timetable

About this task

This topic provides the procedure for copying an existing timetable to a new timetable. Although you can copy timetables from other users, you cannot copy over an existing timetable. When you copy a timetable, the scheduling information and tasks in the timetable are copied. The name of the timetable that will be copied should be known before starting this procedure.

Procedure

1. Select **Timetable** on the **Keep** Screen-Labeled Key (SLK) menu.

CMS displays the Timetable window.

2. In the **Timetable name** field, enter the name that will be used for the new timetable.

The following list provides the types of characters that can be entered in this field:

- Alphanumeric (A-z, 0-9)
- Underscore (_)
- Blank ()
- Comma (,)
- Period (.)
- Single Quotation Marks (')
- Plus sign (+)

3. In the **User ID** field, confirm that your user ID is present.

4. Press the **Enter** key.

CMS shifts focus to the action list.

5. Use the arrow keys to highlight the **Copy** item in the action list and press the **Enter** key.

CMS displays the Timetable: Copy window.

6. In the **Copy from** field, enter the name of the timetable to copy.
7. In the **User ID** field, enter the user ID that is currently associated with the existing timetable.
8. Press the `Enter` key.

CMS shifts focus to the action list of the Timetable: Copy window.

9. Press the `Enter` key again.

CMS displays `Successful` in the status bar.

If this new timetable is not scheduled to run, CMS displays a message notifying you that this copy needs to be rescheduled.

10. Select the **Exit SLK** to close the Timetable window.

Copying timetable tasks

About this task

This topic provides the procedure for duplicating tasks within a timetable.

Before you begin

The following items should be read and understood before copying timetable tasks:

- Only the owner of the timetable or an administrator can copy timetable tasks.
- You cannot copy a task more than once using the **Copy** command in the Timetable: Get Contents window. You must reuse the **Copy** command to make additional copies of a task.
- You cannot copy more than 100 tasks into a timetable. If you exceed the limit, none of the tasks are copied. The status line will display a `Failed` message when this occurs.
- Copies of tasks can be placed after a specified task in the timetable, or each copy can be placed directly after the task from which it was copied. The default is to place the copies after the last task in the timetable.

Procedure

1. From the CMS main menu, press `F4` (**Keep**).
2. Select **Timetable** and press the `Enter` key.

CMS displays the Timetable window.

Timetable test1

Timetable name:

Description:

User ID: cms

Start time:

Start date:

Frequency and attributes (Select only one):

☒ Once

☐ Dates:

☐ Hourly, Stop time: 11:59 PM

☐ Daily,

Hourly/Daily Days (Select any you wish):

☒ Sunday ☒ Tuesday ☒ Thursday ☒ Saturday

☒ Monday ☒ Wednesday ☒ Friday

This timetable will run on this or another CMS server

☐ Run only on this CMS server*

☒ Run on this or another CMS server*

*These fields not used for Find one or List all

21x68

Add
 Copy
 Delete
 Find one
 Get contents
 Global edit
 List all
 Modify
 Next
 Previous

3. Press **Ctrl+Z**.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable containing the task to copy.
5. In the **User ID** field, enter the user ID that created the timetable.

If you are not the owner or an administrator, you will not be able to copy tasks in the timetable.

6. Press the **Enter** key.

CMS shifts focus to the action list.

7. Use the arrow keys to highlight the **Get contents** menu item and press the **Enter** key.

CMS displays the Timetable: Get Contents window.

Timetable: Get Contents test1

Task(s):

Timetable: Sample timetable Number of tasks: 10

Task	Action	Window Title
1	Run	Rpts: Hist: Agent: Summary: Interval Input
2	Run	Rpts: Hist: Agent: Summary: Daily Input
3	Run	Rpts: Hist: Agent: Summary: Weekly Input
4	Run	Rpts: Hist: Agent: Summary: Monthly Input
5	Run	Rpts: Hist: Agent: Split/Skill: Interval Input
6	Run	Rpts: Hist: Agent: Split/Skill: Daily Input
7	Run	Rpts: Hist: Agent: Split/Skill: Weekly Input

Add tasks
 Copy
 Delete
 Global edit
 Modify

test1 a510
test1 a510
test1 a510
test1 a510

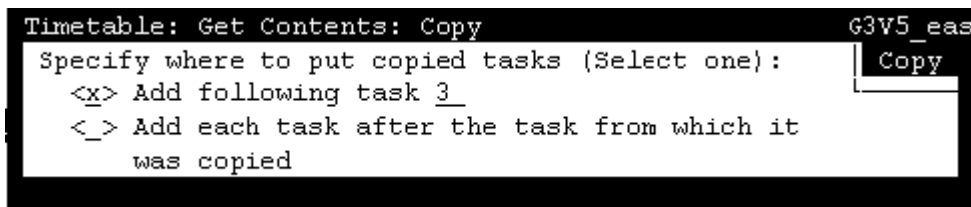
103x132 >

8. In the **Task(s)** field, enter the task number to copy and press the **Enter** key.

CMS shifts focus to the action list of the Timetable: Get Contents window.

9. Using the arrow keys, highlight the **Copy** menu item, and press the `Enter` key.

CMS displays the Timetable: Get Contents window.



10. Choose one of the following options by placing an `x` next to it:
 - **Add following task** - The copied task will be placed immediately after the task specified in this field.
 - **Add each task after the task from which it was copied** - The copied task is placed immediately after itself.

The default action is to place the copied task at the end of the list.

11. Press the `Enter` key.

CMS shifts focus to the action list.

12. Press the `Enter` key again.

CMS displays `Working` in the status line. When the operation completes, the status line displays `Successful`. CMS closes the Copy window and displays the Timetable: Get Contents window.

If the operation fails, a message window appears stating the reason for the failure.

13. To close the Timetable: Get Contents window, select the **Exit** SLK.

Modifying timetable tasks

About this task

This topic provides the procedure for modifying tasks within a timetable. The Modify feature allows you to modify the action or data associated with any task within the selected timetable.

Before you begin

The following items should be read and understood before modifying timetable tasks:

- Only the owner or an administrator can modify timetable tasks.
- The **Current** and **Main Menu** Screen-Labeled Keys (SLKs) are blocked while modifying tasks.
- If you press the **Exit** SLK without selecting a task action, a popup window is displayed stating that the task modification has been cancelled.
- To exit the timetable without saving any changes, select the **Stop** item from the **Keep** SLK menu.

Procedure

1. From the CMS main menu, press F4 (Keep).
2. Select **Timetable** and press the Enter key.

CMS displays the Timetable window.

3. Press Ctrl+Z.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable containing the task to modify.
5. In the **User ID** field, enter the user ID that created the timetable.

If you are not the owner or an administrator, you will not be able to modify tasks in the timetable.

6. Press the Enter key.

CMS shifts focus to the action list.

7. Use the arrow keys to highlight the **Get contents** menu item and press the Enter key.

CMS displays the Timetable: Get Contents window.


```

Timetable: Get Contents                                     test1
Task(s):
Timetable: Sample timetable          Number of tasks: 10
Task Action Window Title
1 Run Rpts: Hist: Agent: Summary: Interval Input
2 Run Rpts: Hist: Agent: Summary: Daily Input
3 Run Rpts: Hist: Agent: Summary: Weekly Input
4 Run Rpts: Hist: Agent: Summary: Monthly Input
5 Run Rpts: Hist: Agent: Split/Skill: Interval Input
6 Run Rpts: Hist: Agent: Split/Skill: Daily Input
7 Run Rpts: Hist: Agent: Split/Skill: Weekly Input
Add tasks
Copy
Delete
Global edit
Modify
test1 a510
test1 a510
test1 a510
test1 a510
103x132 >

```

8. In the **Task(s)** field, enter the number of the task to modify and press the `Enter` key.

CMS shifts focus to the action list of the Timetable: Get Contents window.

9. Using the arrow keys, highlight the **Modify** menu item and press the `Enter` key.

CMS displays a window for the specified task.

Example:

```

Rpts: Hist: Agent: Summary: Interval Inp          test1
Agent: 0001                                         Run
Date: 0
Times: 10:00
Report destination (Select one):
<> Printer, Printer name:
< > File,
File name:

```

10. Make any necessary changes to the task.
11. When the changes have been made, press the `Enter` key.
CMS shifts focus to the action list.
12. Using the arrow keys, highlight the appropriate action to perform in the action list and press the `Enter` key.
CMS displays a confirmation window asking if changes should be saved.
13. To save the changes made to the task, press the `Y` and then press the `Enter` key.
CMS saves the task changes to the timetable and displays the Timetable: Get Contents window.
14. To exit the Timetable: Get Contents window, select the **Exit SLK**.

Editing timetables globally

About this task

Globally editing timetables changes the server compatibility for all timetables associated with a user ID.

Server compatibility of timetables can be one of the two following states:

- **Add following task** - The timetable will run only on this CMS server. If this timetable is backed up and migrated to another CMS server, it will not run.
- **Add each task after the task from which it was copied** - The timetable is capable of running on this or any other CMS server. If this timetable is backed up and migrated to another CMS server, it will function normally.

Before you begin

The following items should be read and understood before making global edits to timetable tasks:

- Only the owner of the timetable or an administrator can globally edit a timetable.
- If an error is made during a global edit, CMS displays an error message describing the nature of the problem. All errors must be corrected before CMS allows you to complete the modifications.

Procedure

1. From the CMS main menu, press **F4** (Keep).
2. Select **Timetable** and press the **Enter** key.

CMS displays the Timetable window.

Timetable test1

Timetable name:

Description:

User ID: cms

Start time:

Start date:

Frequency and attributes (Select only one):

☒ Once

☐ Dates:

☐ Hourly, Stop time: 11:59 PM

☐ Daily,

Hourly/Daily Days (Select any you wish):

☒ Sunday ☒ Tuesday ☒ Thursday ☒ Saturday

☒ Monday ☒ Wednesday ☒ Friday

This timetable will run on this or another CMS server

☐ Run only on this CMS server*

☒ Run on this or another CMS server*

*These fields not used for Find one or List all

21x68

Add

Copy

Delete

Find one

Get contents

Global edit

List all

Modify

Next

Previous

3. Press **Ctrl+Z**.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable containing the tasks to modify globally.

5. Press the `Enter` key.

CMS shifts focus to the action list.

6. Using the arrow keys, highlight **Find one** and press the `Enter` key.

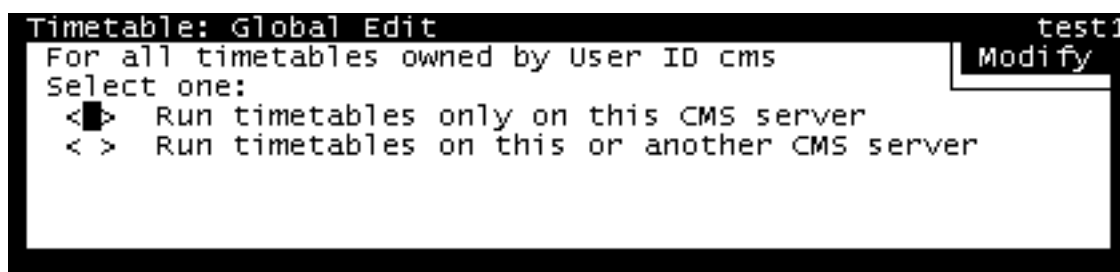
CMS locates the timetable and populates the remaining fields with the information from the timetable.

7. Press the `Enter` key.

CMS shifts focus to the action list.

8. Using the arrow keys, highlight **Global edit** and press the `Enter` key.

CMS displays the Timetable: Global Edit window.



9. Select one of the following options by placing an `x` in the associated field:

- **Add following task** - All timetables owned by the specified user ID will be modified so that they can only run on this CMS server. Timetables migrated to another server will not function.
- **Add each task after the task from which it was copied** - All timetables owned by the specified user ID will be modified so that they can run on the current CMS server or, if migrated, a different CMS server.

10. Press the `Enter` key.

CMS shifts focus to the action list and highlights the **Modify** action.

11. Press the `Enter` key again.

CMS will display a message in the status line of this window indicating how many timetables were updated.

12. Use the **Exit** SLK to close this window and return to the Timetable window.

The timetable displayed in the Timetable window does not update automatically. Use the **Find one** action to re-query for this table in order to show the current configuration.

Globally editing tasks in a timetable

About this task

This topic provides the procedure for changing multiple tasks in a timetable to use a common date, time, or printer destination. For example, you may want to run all reports within a timetable

so that instead of reporting on data for today (relative date: 0), the reports will use data from yesterday (relative date: -1). Using the global edit feature can change the dates used for these reports in a simple series of steps instead of modifying each task separately. This feature can also be used to modify tasks that have different values for times, dates, or printer destinations so that all specified tasks use consistent values.

Before you begin

The following items should be read and understood before making global edits to timetable tasks:

- Only the owner of the timetable or an administrator can globally edit a timetable.
- If an error is made during a global edit, CMS displays an error message describing the nature of the problem. All errors must be corrected before CMS allows you to complete the modifications.

Procedure

1. From the CMS main menu, press F4 (Keep).
2. Select **Timetable** and press the Enter key.

CMS displays the Timetable window.

Timetable test1

Timetable name: _____

Description: _____

User ID: cms _____

Start time: _____

Start date: _____

Frequency and attributes (Select only one):

<x> Once

<_> Dates: _____

<_> Hourly, Stop time: 11:59 PM

<_> Daily,

Hourly/Daily Days (Select any you wish):

[x] Sunday [x] Tuesday [x] Thursday [x] Saturday

[x] Monday [x] Wednesday [x] Friday

This timetable will run on this or another CMS server

<_> Run only on this CMS server*

<x> Run on this or another CMS server*

*These fields not used for Find one or List all

21x68

Menu:

- Add
- Copy
- Delete
- Find one
- Get contents
- Global edit
- List all
- Modify
- Next
- Previous

3. Press Ctrl+Z.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable containing the tasks to modify globally.

5. Press the **Enter** key.

CMS shifts focus to the action list.

6. Using the arrow keys, highlight **Find one** and press the **Enter** key.

CMS locates the timetable and populates the remaining fields with the information from the timetable.

7. Press the **Enter** key.

CMS shifts focus to the action list.

8. Using the arrow keys, highlight **Get contents** and press the **Enter** key.

CMS displays the Timetable: Get Contents window.

Timetable: Get Contents					test1	
Task(s):					Add tasks	
Timetable: Sample timetable					Copy	
Number of tasks: 10					Delete	
Task	Action	Window	Title		Global edit	
1	Run	Rpts: Hist: Agent: Summary: Interval	Input		Modify	
2	Run	Rpts: Hist: Agent: Summary: Daily	Input			
3	Run	Rpts: Hist: Agent: Summary: Weekly	Input			
4	Run	Rpts: Hist: Agent: Summary: Monthly	Input	test1	a510	
5	Run	Rpts: Hist: Agent: Split/Skill: Interval	Input	test1	a510	
6	Run	Rpts: Hist: Agent: Split/Skill: Daily	Input	test1	a510	
7	Run	Rpts: Hist: Agent: Split/Skill: Weekly	Input	test1	a510	
					103x132 >	

9. In the **Task(s)** field, enter the tasks to modify using the following methods:

- Range - For example, 1-50.
- Separate values - For example, 1;3;6;7.
- Combination - For example, 1;3-7;10.

10. After the tasks to globally edit have been specified, press the **Enter** key.

CMS shifts focus to the action list.

11. Using the arrow keys, highlight **Global edit** and press the **Enter** key.

CMS displays the Timetable: Get contents: Global edit window.

Timetable: Get Contents: Global Edit		test1
Field to change (Select one):		Confirm
<x> Date/Dates		Modify
<_> Times		
<_> Printer		

12. Place an **x** in the field that will be changed for all specified tasks.

13. In the field to the right of the selected option, enter one or more values as necessary.

To have multiple reports retrieve call center data that occurred at 2:00 PM, place an **x** in the **Times** option and enter 2:00 PM or 14:00 in the associated field to the right.

For the **Date/Dates** option, enter dates in either MM/DD/YY format or the relative format based on today (0 for today, -1 for yesterday). You can separate individual data entry items with semicolons (;) and value ranges with hyphens (-) between entries.

14. Press the `Enter` key.

CMS shifts focus to the action list.

15. Using the arrow keys, highlight **Confirm** and press the `Enter` key.

CMS displays the Timetable: Get Contents: Global Edit: Confirm window.

```

Timetable: Get Contents: Global Edit: Confirm                                test 1
The following tasks have fields of the selected type and can be modified to
use the new value(s) as shown below.

Task Title                                Values
2      Rpts: Hist: Skill: AUX: Daily Input 42 0 lpr /usr/tmp/11.21

Successful
    
```

This window is used to confirm the tasks that will be modified. No changes have been made at this point. If some specified tasks do not appear in the confirmation window, it is because those tasks do not use the data specified when they are run. For example, some reports only use a date value to retrieve information; therefore, changing the time value will not modify this task. If the tasks listed in this window are not correct, you can go back to the previous windows and make adjustments as necessary.

16. Select the **Exit** SLK.

CMS closes the Timetable: Get Contents: Global Edit: Confirm window.

17. If you are satisfied with the changes, press the `Enter` key.

CMS shifts focus to the action list.

18. Using the arrow keys, highlight **Modify** and press the `Enter` key.

CMS modifies the tasks in this timetable with the data values specified, closes the Timetable: Get contents: Global edit window, and displays `Successful` in the status line when the operation is complete.

19. Close the Timetable: Get contents: Global edit by selecting the **Exit** SLK.

Deleting tasks from a timetable

Before you begin

The following items should be read and understood before deleting tasks from a timetable:

- Only the owner of the timetable or an administrator can delete tasks from a timetable.
- To exit the timetable without saving any changes, select the **Stop** item from the **Keep SLK** menu.

Procedure

1. From the CMS main menu, press F4 (Keep).
2. Select **Timetable** and press the Enter key.

CMS displays the Timetable window.

3. Press Ctrl+Z.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable containing the tasks to modify globally.
5. Press the Enter key.

CMS shifts focus to the action list.

6. Using the arrow keys, highlight **Find one** and press the Enter key.

CMS locates the timetable and populates the remaining fields with the information from the timetable.

7. Press the **Enter** key.

CMS shifts focus to the action list.

8. Using the arrow keys, highlight **Get contents** and press the **Enter** key.

CMS displays the Timetable: Get Contents window.

Timetable: Get Contents					test1	
Task(s):					Add tasks	
Timetable: Sample timetable					Copy	
Number of tasks: 10					Delete	
Task Action Window Title					Global edit	
					Modify	
1	Run	Rpts: Hist: Agent: Summary: Interval Input			test1	a510
2	Run	Rpts: Hist: Agent: Summary: Daily Input			test1	a510
3	Run	Rpts: Hist: Agent: Summary: Weekly Input			test1	a510
4	Run	Rpts: Hist: Agent: Summary: Monthly Input			test1	a510
5	Run	Rpts: Hist: Agent: Split/Skill: Interval Input			test1	a510
6	Run	Rpts: Hist: Agent: Split/Skill: Daily Input			test1	a510
7	Run	Rpts: Hist: Agent: Split/Skill: Weekly Input			test1	a510
					103x132 >	

9. In the **Task(s)** field, enter the number of the task to delete.

10. Press the **Enter** key.

CMS shifts focus to the action list.

11. Using the arrow keys, highlight **Delete** and press the **Enter** key.

CMS displays a confirmation window.

12. Press the **Y** key and then the **Enter** key to save the changes.

CMS deletes the task from the timetable, the tasks are renumbered, the timetable is saved, and the status line displays a **Successful** message.

13. Select the **Exit** SLK to close the Timetable: Get Contents window.

Deleting a timetable

About this task

Only the owner of the timetable or an administrator can delete timetables.

Procedure

1. From the CMS main menu, press **F4** (Keep).
2. Select **Timetable** and press the **Enter** key.

CMS displays the Timetable window.

Timetable
test1

Timetable name:

Description:

User ID: cms

Start time:

Start date:

Frequency and attributes (Select only one):

☒ Once

☐ Dates:

☐ Hourly, Stop time: 11:59 PM

☐ Daily,

Hourly/Daily Days (Select any you wish):

☒ Sunday ☒ Tuesday ☒ Thursday ☒ Saturday

☒ Monday ☒ Wednesday ☒ Friday

This timetable will run on this or another CMS server

☐ Run only on this CMS server*

☒ Run on this or another CMS server*

*These fields not used for Find one or List all

Add

Copy

Delete

Find one

Get contents

Global edit

List all

Modify

Next

Previous

21x68

3. Press **Ctrl+Z**.

The fields in the window are cleared of all default information.

4. In the **Timetable name** field, enter the name of the timetable containing the tasks to modify globally.
5. Press the **Enter** key.

CMS shifts focus to the action list.

6. Using the arrow keys, highlight **Find one** and press the **Enter** key.

CMS locates the timetable and populates the remaining fields with the information from the timetable.

7. Press the **Enter** key.

CMS shifts focus to the action list.

8. Using the arrow keys, highlight **Delete** and press the **Enter** key.

CMS displays a confirmation window.

9. Press the **Y** key and then the **Enter** key.

CMS deletes the timetable and a successful message is displayed in the status line.

Shortcuts

A shortcut is similar to a timetable except that it is not run based on time but rather when it is executed by a user. A shortcut is a fast and easy way for an ASCII terminal user to select windows that are used often. For example, you can create a shortcut for two different real-time reports that you normally view throughout the day. The shortcut displays these reports, fills out the input windows, and places them on the terminal screen so that they can both be viewed at once. Although useful for other tasks, shortcuts are most commonly used to run real-time reports.

Before using shortcuts

The following items should be read and understood before working with shortcuts:

- Shortcuts are only available through the ASCII interface to CMS .
- Each user can create a maximum of ten shortcuts.
- Once a shortcut has started running, it cannot be stopped.
- Shortcuts can be copied from those created by other users.
- You cannot exceed your maximum allowable window count by using a shortcut.
- You cannot create a custom report using a shortcut.
- When using the **Keep** mode to record the tasks for a shortcut, the **Current** Screen-Labeled Key (SLK) will only shift focus between windows in the shortcut window. It will not shift focus to windows that were open before you entered **Keep** mode.
- When you create a shortcut, tasks that have errors in them are saved, but they will not execute when the shortcut is run. The task containing the error will display an error message which causes the shortcut to stop. The error must be corrected before the shortcut can run properly. To delete the error, exit the shortcut without saving changes or edit the shortcut if the error has already been saved.
- Deleting a CMS user who owns shortcuts results in those shortcuts also being deleted.

Permissions for shortcuts

Depending on the procedure that you want to perform, you need the following permissions:

- All users are allowed to create shortcuts.
- You must have “read” and “write” permissions for any CMS subsystems and ACD entities associated with the tasks included in a shortcut.
- Users without the Administrator permission can view and copy the shortcuts of other users, but they cannot add, modify, or delete those shortcuts.
- If the access permissions for a user are changed, it could cause the shortcuts of that user to not run properly. For example, removing skill permissions for a user can result in a shortcut report not running or displaying data for that skill.

Creating a shortcut

About this task

This topic provides the procedure for creating a shortcut and adding tasks for it to perform.

Procedure

1. From the CMS main menu, press F4 (Keep).
2. Select **Shortcut** and press the `Enter` key.

CMS displays the Shortcut window.

3. In the **Shortcut name** field, enter a unique name for this shortcut.

Keep the name for the shortcut simple as it becomes the name that must be entered when you wish to execute it from the CMS **Main Menu**.

4. In the **Description** field, enter a brief description for the shortcut.

This field is optional.

5. Press the `Enter` key.

CMS shifts focus to the action list.

6. Highlight the **Add** item and press the `Enter` key.

CMS displays the **Main Menu**. CMS is now in Keep mode.

7. Use the **Main Menu** to select tasks. Multiple windows can be shown on the screen at one time.
8. Use the **Move** and **Size** items from the **Wind SLK** menu to adjust the placement and dimensions of each window.
9. When satisfied with the report windows, input windows, and their placement and sizes on the screen, select the **Stop** item from the **Keep SLK** menu.

CMS displays a confirmation window asking if the shortcut should be saved.

10. Press the `Y` key and then `Enter` to save the shortcut.

CMS displays the Shortcut window again and the status line displays a `Successful` message indicated that the shortcut was saved.

11. Select the **Exit** SLK to close the Shortcut window and return to the **Main Menu**.

Adding tasks to a shortcut

About this task

This topic provides the procedure for adding tasks to an existing shortcut.

Procedure

1. From the CMS main menu, press F4 (Keep).
2. Select **Shortcut** and press the **Enter** key.

CMS displays the Shortcut window.

3. In the **Shortcut name** field, enter the name of the shortcut which will have new tasks added.
4. Press the **Enter** key.

CMS shifts focus to the action list.

5. Highlight **Get contents** and press the **Enter** key.

CMS displays the Shortcut: Get Contents window.

Task	Action	Window	Title
1	Run	Rpts: Real: Split/Skill: Skill Top Agent Report In g	C
2	Run	Rpts: Hist: Agent: AUX: Interval Input	g

6. In the **Task(s)** field, enter the number of the task that the new task will follow.
To add a task in the second position of the shortcut, enter 1 in the **Task(s)** field.

If you wish the new task to be in the first position, leave the **Task(s)** field blank.

7. Press the `Enter` key.

CMS shifts focus to the action list.

8. Highlight **Add tasks** and press the `Enter` key.

CMS displays the **Main Menu**.

9. On the **Main Menu**, use the normal menu items to perform the tasks you want to add to the shortcut.

When you have made and validated each action list selection, `Entries Stored` displays on the status line.

10. When you have finished performing tasks for the shortcut, select **Stop** from the **Keep SLK** menu.

CMS displays a confirmation asking if the changes should be saved.

11. Press the `Y` key and then the `Enter` key.

CMS saves the tasks and displays the Shortcut: Get Contents window.

12. Select the **Exit** SLK to close the Shortcut: Get Contents window.

Running a shortcut

About this task

This topic provides the procedure for executing a shortcut.

Procedure

1. At the CMS **Main Menu**, press the `;` (semicolon) key.

CMS selects the command line of the **Main Menu**.



2. Enter the name of the shortcut to run and press the `Enter` key.

The shortcut starts running and locks the keyboard until the shortcut finishes. When the shortcut finishes, the status line displays a `Successful` message.

Modifying a shortcut description

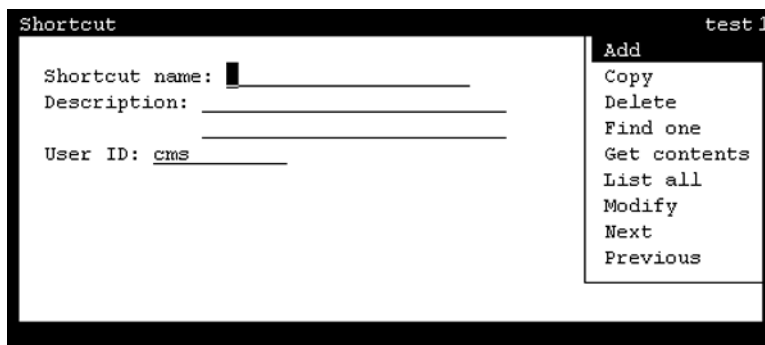
About this task

This topic provides the procedure for editing the name or description of a shortcut.

Procedure

1. From the CMS main menu, press `F4` (Keep).
2. Select **Shortcut** and press the `Enter` key.

CMS displays the Shortcut window.



The screenshot shows a terminal-style window titled "Shortcut" with a status bar on the right showing "test 1". Inside the window, there are three input fields: "Shortcut name:" with a cursor, "Description:", and "User ID: cms". To the right of these fields is an open action list with the following options: "Add", "Copy", "Delete", "Find one", "Get contents", "List all", "Modify", "Next", and "Previous".

3. In the **Shortcut name** field, enter the name of the shortcut to modify.
4. Press the `Enter` key.

CMS shifts focus to the action list.

5. Highlight **Find one** and press the `Enter` key.

CMS retrieves the shortcut and populates the **Description** and **User ID** fields with information from the shortcut.

6. Make the necessary change to the **Description** field.
7. Press the `Enter` key.

CMS shifts focus to the action list.

8. Highlight **Modify** and press the `Enter` key.

CMS saves the changes to the shortcut displays a `Successful` message in the status line.

9. Select the **Exit** SLK to close the Shortcut window.

Copying a shortcut

About this task

This topic provides the procedure for copying an existing shortcut into a new shortcut. All users can copy shortcuts owned by other users. However, no shortcuts owned by your user ID, even as an Administrator, can be copied by you to another user. It is not possible to copy a shortcut over an existing shortcut.

Procedure

1. From the CMS main menu, press **F4** (Keep).
2. Select **Shortcut** and press the **Enter** key.

CMS displays the Shortcut window.

3. In the **Shortcut name** field, enter the name of the new shortcut that will be created.
4. In the **Description** field, enter a brief phrase identifying the new shortcut.

This field is optional.

5. In the **User ID** field, ensure your user ID is present.
6. Press the **Enter** key.

CMS shifts focus to the action list.

7. Highlight **Copy** and press the **Enter** key.

CMS displays the Shortcut: Copy window.

8. In the **Copy from** field, enter the name of the shortcut to copy as the new shortcut.
9. In the **User ID** field, enter the ID of the user that owns the shortcut to copy.
10. Press the **Enter** key.

CMS shifts focus to the action list.

11. Press the `Enter` key again.

CMS creates the new shortcut, closes the Shortcut: Copy window, and displays a `Successful` message in the status line.

12. Select the **Exit** SLK to close the Shortcut window.

Copying shortcut tasks

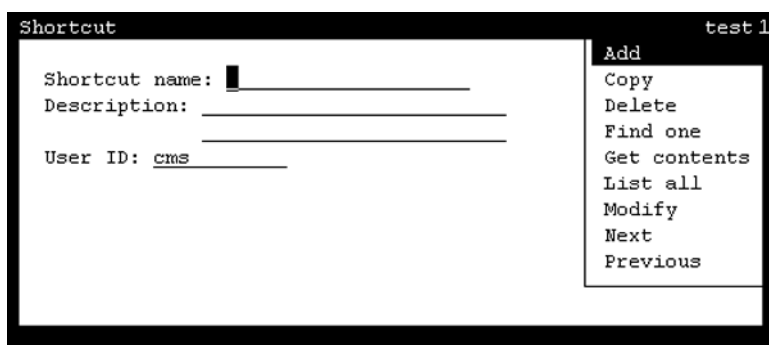
About this task

This topic provides the procedure for copying tasks within a shortcut.

Procedure

1. From the CMS main menu, press `F4` (Keep).
2. Select **Shortcut** and press the `Enter` key.

CMS displays the Shortcut window.



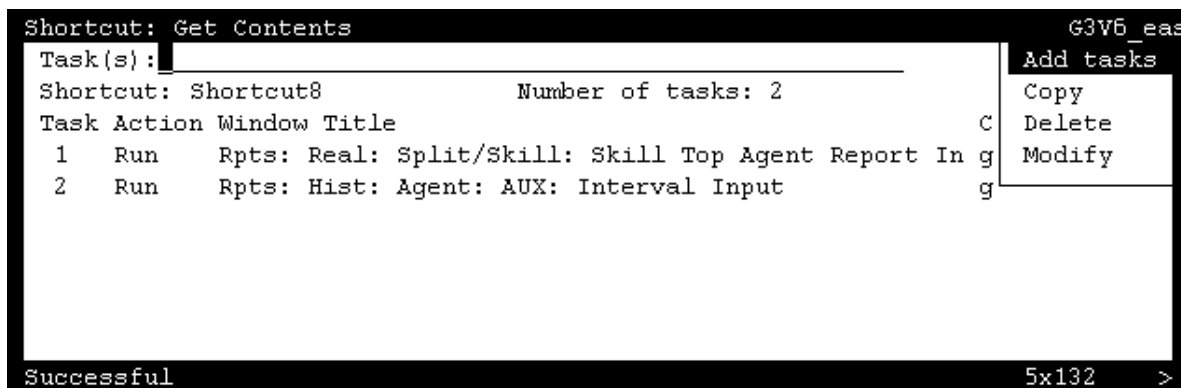
The screenshot shows a terminal-style window titled "Shortcut" with a sub-tab "test 1". On the left, there are three input fields: "Shortcut name:" with a cursor, "Description:", and "User ID: cms". On the right, there is a vertical list of actions: "Add", "Copy", "Delete", "Find one", "Get contents", "List all", "Modify", "Next", and "Previous".

3. In the **Shortcut name** field, enter the name of the shortcut in which a task will be copied.
4. Press the `Enter` key.

CMS shifts focus to the action list.

5. Highlight **Get contents** and press the `Enter` key.

CMS displays the Shortcut: Get Contents window.

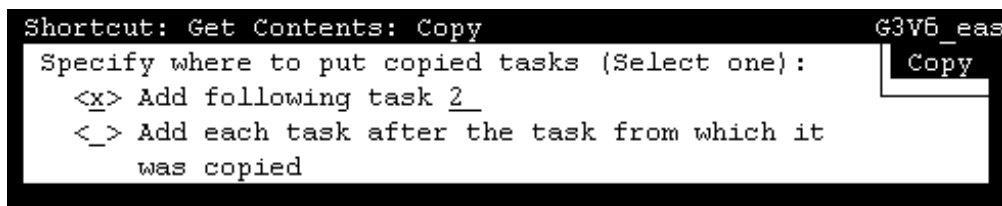


6. In the **Task(s)** field, enter the number of the task to copy and press the **Enter** key.

CMS shifts focus to the action list.

7. Highlight **Copy** and press the **Enter** key.

CMS displays the Shortcut: Get Contents: Copy window.



8. Place an **x** in one of the following options:

- **Add following task** - This option will create the task after the task number specified in the field to the right.
- **Add each task after the task from which it was copied** - This option will create the task and place it immediately following the original task. If you specified to make a copy of task #1, the copy will be created as task #2. Any other tasks are shifted to a higher number to accommodate this action.

9. Press the **Enter** key.

CMS shifts focus to the action list.

10. Press the **Enter** key again.

CMS copies the original task, creates the new task, closes the Shortcut: Get Contents: Copy window, and displays a **Successful** message in the status line.

If any sort of error occurs, the status line will display **Failed** and CMS displays an error message describing the nature of the error.

11. Select the **Exit** SLK to close the Shortcut: Get Contents window.

Modifying shortcut tasks

About this task

This topic provides the procedure for editing tasks within a shortcut.

Procedure

1. From the CMS main menu, press F4 (Keep).
2. Select **Shortcut** and press the Enter key.

CMS displays the Shortcut window.

3. In the **Shortcut name** field, enter the name of the shortcut where tasks will be modified.
4. Press the Enter key.

CMS shifts focus to the action list.

5. Highlight **Get contents** and press the Enter key.

CMS displays the Shortcut: Get Contents window.

Task	Action	Window Title
1	Run	Rpts: Real: Split/Skill: Skill Top Agent Report In g
2	Run	Rpts: Hist: Agent: AUX: Interval Input g

6. In the **Task(s)** field, enter the number of the task to modify and press the Enter key.
7. Highlight **Modify** and press the Enter key.

CMS displays the input window of the specified task.

8. Change the input parameters of the window as necessary.

For example, this might include changing the split, agent, or another entity on which a report is based. This can also include making changes to the size and position of the task window.

9. When the appropriate information has been entered, press the `Enter` key.

CMS shifts focus to the action list.

10. Highlight **Modify** and press the `Enter` key.

CMS displays a confirmation asking if the changes should be saved.

11. Press the `Y` key and then the `Enter` key.

CMS saves the changes to the task, closes the task window, and displays a `Successful` message in the status line.

12. Select the **Exit** SLK to close the Shortcut: Get Contents window.

Deleting shortcut tasks

About this task

This topic provides the procedure for deleting a task from a shortcut.

Procedure

1. From the CMS main menu, press `F4` (Keep).
2. Select **Shortcut** and press the `Enter` key.

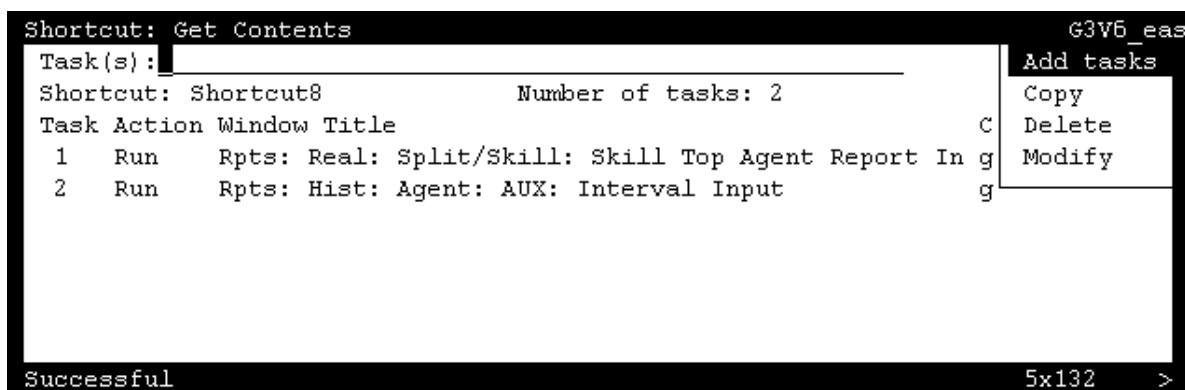
CMS displays the Shortcut window.

3. In the **Shortcut name** field, enter the name of the shortcut containing the task to delete.
4. Press the `Enter` key.

CMS shifts focus to the action list.

5. Highlight **Get contents** and press the `Enter` key.

CMS displays the Shortcut: Get Contents window.



6. In the **Task(s)** field, enter the number of the task to delete.

7. Press the `Enter` key.

CMS shifts focus to the action list.

8. Highlight **Delete** and press the `Enter` key.

CMS displays a confirmation window asking if the changes to the shortcut should be saved.

9. Press the `Y` key and then the `Enter` key.

CMS deletes the specified tasks and displays the Shortcut: Get Contents window.

10. Select the **Exit** SLK to close the Shortcut: Get Contents window.

Deleting a shortcut

About this task

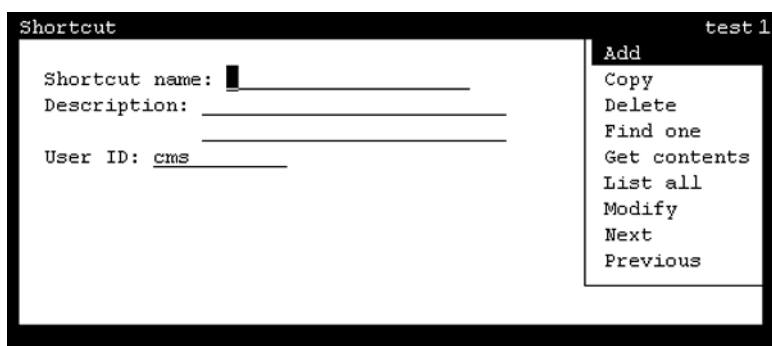
This topic provides the procedure for deleting a shortcut from the CMS server.

Procedure

1. From the CMS main menu, press `F4` (Keep).

2. Select **Shortcut** and press the `Enter` key.

CMS displays the Shortcut window.



3. In the **Shortcut name** field, enter the name of the shortcut to delete.

Shortcuts owned by other users cannot be deleted.

4. Press the `Enter` key.

CMS shifts focus to the action list.

5. Highlight **Find one** and press the `Enter` key.

CMS retrieves the information for the specified shortcut. If the shortcut with the name specified cannot be found, this will be indicated on the status line.

6. Verify that this is the shortcut to be deleted and press the `Enter` key.

CMS shifts focus to the action list.

7. Highlight **Delete** and press the `Enter` key.

CMS displays a confirmation window.

8. Press the `Y` key and then the `Enter` key.

CMS deletes the specified shortcut and displays a `Successful` message in the status line.

Chapter 17: Resources

Documentation

CMS and CMS Supervisor documents

Title	Description	Audience
Overview		
<i>Avaya Call Management System Overview and Specification</i>	Describes tested product characteristics and product capabilities including feature descriptions, interoperability, performance specifications, security, and licensing requirements.	All users
Installation and maintenance		
<i>Deploying Avaya Call Management System</i>	Describes how to install and configure CMS in a virtualized VMware or KVM environment.	Implementation engineers, administrators
<i>Deploying Avaya Call Management System in an Infrastructure as a Service Environment</i>	Describes how to deploy CMS in an Amazon Web Services or Google Cloud Platform environment.	Implementation engineers, administrators
<i>Maintaining and Troubleshooting Avaya Call Management System</i>	Describes how to configure, maintain, and troubleshoot CMS.	Administrators, support personnel
<i>Avaya Call Management System and Communication Manager Connections, Administration, and Troubleshooting</i>	Describes how to connect and administer the Automatic Call Distribution (ACD) systems used by CMS.	Administrators, installation personnel, support personnel
<i>Avaya Call Management System High Availability Connectivity, Upgrade and Administration</i>	Describes how to connect to HA servers and upgrade to HA.	Administrators, installation personnel, software specialists involved with HA
<i>Using Avaya Call Management System High Availability and Admin-Sync</i>	Describes how to install and maintain your CMS High Availability (HA) system.	Administrators, support personnel
Upgrading		

Table continues...

Title	Description	Audience
<i>Upgrading Avaya Call Management System</i>	Describes the procedures required to upgrade to a new CMS release. This document is focused on full software or platform upgrades.	System administrators, implementation engineers
<i>Avaya Call Management System Base Load Upgrade</i>	Describes how to perform a simplified base load upgrade. You can perform a base load upgrade within a CMS release or for other approved scenarios. Not all releases support base load upgrades.	System administrators, implementation engineers
Administration		
<i>Administering Avaya Call Management System</i>	Provides instructions on administering a call center using CMS Supervisor.	Avaya support personnel, Administrators
<i>Avaya Call Management System Call History Interface</i>	Describes the format of the Call History data files and how to transfer these files to another computer.	Administrators, supervisors
<i>Using ODBC and JDBC with Avaya Call Management System</i>	Describes how to use Open Database Connectivity (ODBC) and Java Database Connectivity (JDBC) with CMS.	Administrators, support personnel
<i>Avaya Call Management System Database Items and Calculations</i>	Describes each database item and calculation that CMS tracks and how CMS calculates the values displayed on CMS reports and CMS Supervisor reports.	Administrators, support personnel
<i>Avaya Call Management System Custom Reports</i>	Describes how to design and create custom reports in CMS.	Administrators, report designers
<i>Avaya Call Management System Security</i>	Describes how to implement security features in CMS.	Administrators, support personnel
CMS Supervisor		
<i>Avaya CMS Supervisor Clients Installation and Getting Started</i>	Describes how to install and configure CMS Supervisor.	Implementation engineers, system administrators
<i>Avaya CMS Supervisor Reports</i>	Describes how to use CMS Supervisor reports.	Supervisors, administrators
<i>Avaya CMS Supervisor Report Designer</i>	Describes how to create new reports and to edit existing reports through Report Designer and Report Wizard.	Supervisors, administrators

Avaya Solutions Platform Documents

Title	Description	Audience
<i>Avaya Solutions Platform Overview and Specification</i>	Describes the key features of Avaya Solutions Platform server	All users

Table continues...

Title	Description	Audience
<i>Installing the Avaya Solutions Platform 130 Series</i>	Describes how to install Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel
<i>Maintaining and Troubleshooting Avaya Solutions Platform 130 Series</i>	Describes procedures to maintain and troubleshoot Avaya Solutions Platform 130 Series servers.	Implementation engineers, solution architects, support personnel

Finding documents on the Avaya Support website

Procedure

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Documents**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. In **Select Release**, select the appropriate release number.
This field is not available if there is only one release for the product.
6. **(Optional)** In **Enter Keyword**, type keywords for your search.
7. From the **Select Content Type** list, select one or more content types.
For example, if you only want to see user guides, click **User Guides** in the **Select Content Type** list.
8. Click  to display the search results.

Avaya Documentation Center navigation

For many programs, the latest customer documentation is available on the Avaya Documentation Center website at <https://documentation.avaya.com>. Some functionality is only available when you log in to the Avaya Documentation Center. The available functionality depends on your role.

Important:

If the documentation you are looking for is not available on the Avaya Documentation Center, you can find it on the [Avaya Support website](https://support.avaya.com).

While navigating through the Documentation Center, you can click the **Avaya Documentation Center** logo at the top of the screen to return to the home page anytime. On the Avaya Documentation Center, you can do the following:

- Click **Avaya Links** in the top menu bar to access other Avaya websites, including the Avaya Support website.

- Click **Languages** (🌐) in the top menu bar to change the display language and view localized documents.
- In the **Search Documentation** field, search for keywords and click **Filter** to filter by solution category, product, or user role.
You can select multiple items in each filter category. For example, you can select a product and multiple user roles.
- Click **Library** in the top menu bar to access the complete library of documents. Use the filtering options to refine your results.
- After performing a search or accessing the library, you can sort content on the search results page. When you find the item you want to view, click it to open it.
- Use the table of contents in a document for navigation. You can also click < or > next to the document title to navigate to the previous topic or the next topic.
- Click **Share** (➦) to share a topic by email or copy the URL.
- Download a PDF of the current topic in a document, the topic and its subtopics, or the entire document.
- Print the section you are viewing.
- Add content to a collection by clicking **Add to My Topics** (📁). You can add the topic and its subtopics or add the entire publication.
- View the topics in your collections. To access your collections, click your name in the top menu bar and then click **My Topics**.

You can do the following:

- Create, rename, and delete a collection.
- Set a collection as the default or favorite collection.
- Save a PDF of the selected content in a collection and download it to your computer.
- Share content in a collection with others through email.
- Receive collections that others have shared with you.
- Click **Watch** (👁) to add a topic to your watchlist so you are notified when the content is updated or removed.
- View and manage your watchlist by clicking **Watchlist** from the top menu with your name.

You can do the following:

- Enable **Email notifications** to receive email alerts.
- Unwatch the selected content or all topics.
- Send feedback for a topic.

Viewing Avaya Mentor videos

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

About this task

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

- To find videos on the Avaya Support website, go to <https://support.avaya.com/> and do one of the following:
 - In **Search**, type `Avaya Mentor Videos`, click **Clear All** and select **Video** in the **Select Content Type**.
 - In **Search**, type the product name. On the Search Results page, click **Clear All** and select **Video** in the **Select Content Type**.

The **Video** content type is displayed only when videos are available for that product.

In the right pane, the page displays a list of available videos.

- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and do one of the following:
 - Enter a keyword or keywords in the **Search Channel** to search for a specific product or topic.
 - Scroll down Playlists, and click a topic name to see the list of videos available. For example, Contact Centers.

Note:

Videos are not available for all products.

Support

Go to the Avaya Support website at <https://support.avaya.com> for the most up-to-date documentation, product notices, and knowledge articles. You can also search for release notes, downloads, and resolutions to issues. Use the online service request system to create a service request. Chat with live agents to get answers to questions, or request an agent to connect you to a support team if an issue requires additional expertise.

Using the Avaya InSite Knowledge Base

The Avaya InSite Knowledge Base is a web-based search engine that provides:

- Up-to-date troubleshooting procedures and technical tips.
- Information about service packs.

- Access to customer and technical documentation.
- Information about training and certification programs.
- Links to other pertinent information.

If you are an authorized Avaya Partner or a current Avaya customer with a support contract, you can access the Knowledge Base without extra cost. You must have a login account and a valid Sold-To number.

Use the Avaya InSite Knowledge Base for any potential solutions to problems.

1. Go to <https://support.avaya.com>.
2. To log in, click **Sign In** at the top of the screen and then enter your login credentials when prompted.
3. Click **Product Support > Products**.
4. In **Search Product**, start typing the product name and then select the appropriate product from the list displayed.
5. Select the release number, if applicable.
6. Click the **Technical Solutions** tab to view articles for resolving technical issues.

Appendix A: Updating time zones

Updating time zones displayed to users

About this task

A time zone list stored on the CMS server is used by the CMS Supervisor PC client and Web client for display of available time zones in any report input screens as well as on the System Setup Data Summarization Time Zone administration screen.

Note:

For daily, weekly, and monthly archived data reports, you must administer time zones specific to each ACD and tenant (If the Multi-Tenancy feature is installed) using System Setup Data Summarization Time Zone. Your available choices for this administration screen is based on the `TimeZoneList.dat` file.

If a CMS Supervisor client on the current release is connecting to a CMS server on an older release, follow the setting time zones for interval reports instructions in *Avaya CMS Supervisor Clients Installation and Getting Started*.

Procedure

1. Enter the following commands to display the time zone DAT files. The `TimeZoneList.dat` file is a subset of full time zone list file, `TimeZoneFullList.dat`.

```
cd /cms/db/config
```

```
ls
```

The system displays the list of DAT files:

```
TimeZoneFullList.dat TimeZoneList.dat TimeZoneShortList.dat
```

2. Save the time zone list file copying it to a temporary file.

```
cp TimeZoneList.dat TimeZoneListSaved.dat
```

3. If you only want to add new time zones to the `TimeZoneList.dat` file, skip this step. Otherwise, edit the file to remove any time zones you do not wish to use. Each time zone is on a separate line. Remove only those lines that you do not need.

```
vi TimeZoneList.dat
```

4. When finished editing, save and close the file.

```
:wq!
```

5. To add new time zones, make a temporary copy of the TimeZoneFullList.dat file for editing. Edit your temporary file to contain only the new time zones you wish to add to your TimeZoneList.dat file. Each time zone is on a separate line. Remove only those time zones you do not need.

```
cp TimeZoneFullList.dat TimeZoneEditList.dat
```

```
vi TimeZoneEditList.dat
```

6. When finished editing, save and close the file.

```
:wq!
```

7. Create one new TimeZoneList.dat file with your changes and delete your temporary files.

```
cat TimeZoneList.dat TimeZoneEditList.dat > MyTimeZoneList.dat
```

```
mv MyTimeZoneList.dat TimeZoneList.dat
```

```
rm MyTimeZoneList.dat TimeZoneEditList.dat TimeZoneListSaved.dat
```

The CMS server will automatically update the CMS Supervisor PC and Web clients with the new time zone choices.

Glossary

abandoned call	A call on which a caller hangs up before an agent answers.
abandoned call search	An ACD capability that enables the system to verify that the caller is still on the line before passing the call to an agent.
acceptable service level	1) A target value for the acceptable amount of time before an agent answers a call. 2) A percentage of calls answered within a set amount of time (for example, 80% of calls answered within 20 seconds).
access permissions	Permissions assigned to a CMS user so that the user can access different CMS capabilities or administer specific elements such as splits/skills, trunks, or vectors. Access permissions can be read, write, or exceptions. See also read permission on page 475, write permission on page 478.
ACD	See Automatic Call Distribution (ACD) on page 468
ACD call	1) A call that queues to a split/skill and is answered by an agent in that split/skill. 2) A call that queues as a direct agent call and is answered by the agent for whom it was queued.
Action List	A menu in the upper right-hand corner of most CMS ASCII screens. The menu lists the actions available for that particular window.
active VDN calls	A Call Vectoring feature on Communication Manager systems that provides conditional branching to a different step in the same vector or to a different vector, based on the number of incoming trunk calls a VDN is processing in a vector or at an agent position. Also called counted calls to VDN.
Adjunct/Switch Applications Interface (ASAI)	A recommendation for interfacing adjuncts and communications systems that is based on the CCITT Q.932 specification for layer 3. ASAI supports activities such as event notification and call control.
after call work (ACW)	An agent state consisting of work related to the preceding ACD call. If an agent hangs up after an ACD call, the agent is in ACW. ACW is also

accessible by a button on the agent's set and does not have to be related to an ACD call.

agent	A person or VRU port that answers calls to an ACD split/skill. The agent is represented to CMS by a login identification keyed into a voice terminal.
agent login ID	A 1- to 9-digit number keyed by an ACD agent from a voice terminal to activate the agent position. Agent logins are needed for all CMS-measured ACD agents.
agent occupancy	The percentage of time that you expect or target for each split/skill agent to spend on ACD calls and in ACD while logged in.
agent position (EAS)	The combination of the agent login ID and the skills the agent is assigned. Data is collected for the agent by skill so that the total work for the agent is the sum of all skills in which the agent worked.
agent position (non-EAS)	The combination of the agent login ID and the split the agent logged into. Agents logged into multiple splits are associated with multiple positions. Call data is collected separately for each agent/split combination.
agent role	A description of the kind of service an agent in multiple skills give for one of these skills. Agent role is a combination of call-handling preference and skill/reserve levels.
agent skill	An attribute that is associated with an ACD agent and that qualifies the agent to handle calls requiring the attribute. An agent can be assigned up to 60 skills; for example, the ability to speak a particular language or the expertise to handle a certain product. See also primary skill on page 475 , secondary skill on page 476 , and skill level on page 476
agent state	A feature of agent call handling that allows agents to change their availability to the switch; for example, ACW, AVAIL, AUX.
agent terminal	The voice terminal used by a call center agent.
agent trace	A CMS capability that allows you to trace agent activities such as state changes which can then be shown in a report.
AI	See Auto-in (AI) on page 468.
ANI	See Automatic Number Identification (ANI) on page 468.
announcement	A recorded voice message that typically identifies the call's destination, asks the caller to stay on the line, and describes the product or service offered. With the Call Vectoring feature, announcements can be part of a vector's call processing.

ASA	See Average Speed of Answer (ASA) on page 469.
ASAI	See Adjunct/Switch Applications Interface (ASAI) on page 466.
auto-available split	An ACD capability that enables VRUs such as the CONVERSANT® Voice Information System to be brought online again immediately after a power failure or system restart without time-consuming reprogramming.
Auto-in (AI)	An ACD work mode that makes the agent available to receive calls and allows the agent to receive a new ACD call immediately after disconnecting from the previous call.
Automatic Call Distribution (ACD)	1) A switch feature that channels high-volume incoming and outgoing call traffic to agent groups (splits/skills). 2) An agent state in which the extension is engaged on an ACD call.
Automatic Number Identification (ANI)	An industry term for notification of the calling party number (CPN). When the calling party is connected through a switch, the CPN can be either a billing number for the switch or the station identification (SID) number.
AUX	See auxiliary work (AUX) on page 468.
AUX reason codes	Codes that enable a call center to track an agent's time more precisely when the agent is in the AUX state. Agents can specify why they are in the AUX state - for example, on break or in a meeting.
auxiliary work (AUX)	An agent state in which the agent is doing non-ACD work, is on break, or is in a meeting. Agent enter AUX work by pressing the AUX WORK button or dialing the access code from their voice terminal. Agents can also enter AUX work by going off-hook to make or answer an extension call while in AVAIL mode or with a call on hold.
AVAIL	See available (AVAIL) on page 468.
available (AVAIL)	An agent work mode in which the extension can accept an ACD call. The agent enters this state by selecting the AI (auto-in) or MI (manual-in) work mode.
Avaya Business Advocate	A set of features designed to enhance call and agent selection in a contact center.
Avaya Interactive Response	A powerful voice-response system that may include automated call routing, announcement storage, message retrieval, and callback. Used to be called CONVERSANT.
average agent service time	The average time you are expecting or targeting each agent to spend on an ACD call including talk time and ACW time.

Average Speed of Answer (ASA)	The average time a caller waits in queue before connecting to an agent. The ASA for a split/skill includes the time spent in queue and the time ringing an agent. The ASA for a VDN includes the time spent in vector processing including the time spent in queue and the time ringing for the VDN that the call was answered in.
backup	The process of protecting data by writing the contents of the disk to an archive, such as tape, that can be removed from the computer environment and stored safely.
calculation	A formula for representing call center entities in the Dictionary. Calculations generate the date for fields in a report.
Call Prompting	A switch feature that routes incoming calls based on information supplied by the caller such as an account number. The caller hears an announcement and is prompted to select an option from those listed in the announcement.
Call Vectoring	A switch feature that provides a highly flexible method for processing ACD calls using VDNs and vectors as processing points between trunk groups and splits. Call Vectoring permits a treatment of calls that is independent of splits.
Call Work Code (CWC)	An ACD capability that allows the agent to enter a string of digits during or after the call and send them to CMS for management reporting.
call-based items	The category of database items in CMS that are entered in the database after a call completes. If a call starts and ends in different intrahour intervals, the call-based data is recorded for the interval in which the call completed. Most database items are call-based.
call-handling performance	A parameter of agent administration in an EAS environment that specifies how calls are selected for the agent.
call-handling profile	A set of objectives describing how a split/skill handles calls. Call-handling profiles are part of the Avaya CMS Forecast product.
calls carried	The number of inbound/outbound calls carried by a trunk.
change agent skills	A CMS capability that allows you to change a single agent's skill assignment or apply an agent template to multiple agents.
connected (CONN)	A trunk state in which a caller and an agent are connected on an ACD call.
connected call	A non-ACD call connected to an agent through a VDN and for which CMS receives an indication that the call rang or was answered.
CONVERSANT	See Avaya Interactive Response on page 468.

current	A CMS operation that displays data from the current interval.
current interval	The current intrahour period of time (15, 30, or 60 minutes) which is archived to the historical database when the period expires. The current interval is part of the real-time database.
current wait time	The time a call has waited for service in a call queue adjusted for queue priority.
custom report	A real-time or historical report that has been customized from standard reports or created by the user through the Custom Reports subsystem of CMS.
daily data	Interval data that has been converted to a 1-day summary.
data collection	This CMS feature can be used to determine if call activity and the associated ACD data is recorded. In many maintenance operations, it is necessary to disable data collection. If data collection is turned off, CMS does not void data on current call activity.
database	The CMS databases are used to store ACD data according to a specific time period. This can be current and previous intrahour real-time data or intrahour, daily, weekly, and monthly historical data.
database item	A name for a specific type of data stored in one of the CMS databases. A database item can store ACD identifiers such as split numbers or names, login IDs, and VDNs or statistical data on ACD performance such as number of ACD calls, wait time for calls in queue, current states of individual agents, and so forth.
database tables	Each CMS database can consist of several database tables which are used to logically separate data based on different criteria. For example, historical reports can be used to display data on a daily, weekly, or monthly basis; each of these different time measurements are stored in separate database tables.
DDC	See direct department calling (DDC) on page 471.
dequeued and abandoned (DABN)	A trunk state in which the trunk quickly goes idle after the caller abandons the call.
designer reports	Customized reports that you create and run through Avaya CMS Supervisor Report Designer. See the Avaya CMS Supervisor Report Designer User Guide for more information.
Dictionary	A CMS capability used to assign easily-interpreted names to call center entities such as login IDs, splits/skills, trunk groups, VDNs, and vectors.
DID	See direct inward dialing (DID) on page 471.

Digital Subscriber Line (DSL)	A public switched telephone network (PSTN) line that provides high bandwidth for short distances using copper cable. This type of line operates at the Basic Rate Interface (BRI) with two 64-kilobit per second circuit-switched channels and one 16-kilobit packet-switched channel. DSL can carry both data and voice signals at the same time.
direct agent ACD (DACD)	An agent state in which the agent is on a direct agent ACD call.
direct agent ACW (DACW)	An agent state in which the agent is in the after call work (ACW) state for a direct agent ACD call.
direct agent calling	An EAS capability that allows a caller to reach the same agent every time and allows the call center to include the call as an ACD call in management tracking. This is ideal for claims processing in which a client needs to speak with the agent handling the claim. It also ensures a high level of customer service without reducing management control.
direct department calling (DDC)	A non-EAS option to select an agent when more than one agent is available. The call goes to the agent closest to the top of an ordered list.
direct inward dialing (DID)	The use of an incoming trunk used for dialing directly from the public network into a communications system without help from the attendant.
DSL	See Digital Subscriber Line (DSL) on page 471.
EAS	See Expert Agent Selection (EAS) on page 472.
entity	A generic term for an agent, split/skill, trunk, trunk group, VDN, or vector.
EWT	See expected wait time (EWT) on page 471.
exception	Activity in an ACD which falls outside the limits you have defined and usually indicates abnormal or unacceptable performance of the ACD, agents, splits/skills, VDNs, vectors, trunks, or trunk groups. The parameters used to determine the occurrence of an exception are defined in the Exceptions subsystem of CMS.
exception permissions	The rights that a user has in being notified or viewing the instances where calls, call center entities, or subsystems operated above or below specified thresholds.
expected wait time (EWT)	An estimate of how long a caller will have to wait to be served by a contact center while in queue. EWT is based on current and past traffic, handling time, and staffing conditions. Time spent in vector processing before being queued and time spent ringing an agent with manual answering is not included in the EWT. This is switch-based calculation.

Expert Agent Selection (EAS)	An optional Communication Manager feature that routes incoming calls to an agent who is a member of the specific skill required to handle the problems of the caller.
extension call	A call originated by an agent or a non-ACD call received by an agent. Extension calls include calls an agent makes to set up a conference or transfer.
flex agents	Agents who have the role of roving, backup, or allocated. Top and reserve agents are not flex agents. See the Avaya Business Advocate User Guide for more information.
flexible routing	An ACD capability that allows you to choose how incoming calls should be routed to agents in a split. Calls can be routed to the first available agent or to the most-idle agent.
forced busy (FBUSY)	A trunk state in which the caller receives a forced busy signal.
forced disconnect (FDISC)	A trunk state in which the caller receives a forced disconnect.
Forced Multiple Call Handling (FMCH)	A feature available for Communication Manager system which, when activated for a split/skill, allows calls to be automatically delivered to an idle line appearance if the agent is in the AI (auto-in) or MI (manual-in) work mode and if an unrestricted line appearance is available on the voice terminal.
historical database	A CMS database consisting of intrahour records for up to 370 days, daily records for up to 5 years, and weekly/monthly records for up to 10 years for each CMS-measured agent, split/skill, trunk, trunk group, VDN, and vector.
historical reports	Reports of past ACD data for various agent, split/skill, trunk, trunk group, VDN, or vector activities. Historical reports summarize call data into daily, weekly, or monthly totals.
Inbound Call Management (ICM)	A set of switch and adjunct features using ASAI to enable the adjunct to provide automatic screen delivery and call routing.
Information Indicator (II)	A 2-digit code that identifies the type of originating line for incoming ISDN PRI calls, such as hotel or pay phone.
Informix	A relational database management system used to store and retrieve CMS data.
Integrated Services Digital Network (ISDN)	A digital standard for telephony that enables analog and digital signals on the same line.

interflow	A call center process where calls are redirected out of the current ACD. Interflow can occur if a call has been in the queue for too long and it cannot be handed within the ACD. For example, the call can be redirected to another answering point, such as a voicemail system or trunk group outside of the current ACD.
interval ASA	The average time a call waits in queue before connecting to an agent, calculated on reporting interval boundaries. Interval ASA is cleared to zero at the start of each reporting interval. See also Average Speed of Answer (ASA) on page 469 and rolling ASA on page 475.
interval-based items	A category of database items that represent the amount of time during a collection interval spent on a particular activity. Interval-based items are updated throughout the collection interval and timing is restarted at the end of the interval.
intraflow	A call center process for redirecting calls within the ACD environment. For example, calls that have been in the queue for a long time might flow into and out of a split/skill group.
intrahour interval	A 15-, 30-, or 60-minute segment of time starting on the hour. An intrahour interval is the basic unit of CMS report time.
Logical Agent	An EAS feature that associates an agent's login ID with a physical extension when the agent logs in. Properties such as the assigned skills, class of restriction, and coverage path are associated with the login ID rather than the physical extension. This allows agents to log in at any available set.
logout reason codes	Codes that enable an agent to specify the reason for logging out such as the end of a shift or for training.
Look Ahead Interflow (LAI)	A switch feature that can be used to balance the call load among multiple call centers. LAI works with Call Vectoring and ISDN PRI trunks to intelligently route calls between call centers. This allows multiple call centers to share workloads, expand hours of coverage, and allows calls to be transparently handled by call centers in different time zones.
maintenance	A CMS subsystem that is used for routine maintenance of CMS, such as backing up data, checking on the status of the connection to the switch, and scanning the error log.
maintenance busy (MBUSY)	A trunk state in which the trunk is out of service for maintenance purposes.
Manual-In (MI)	An ACD work mode in which an agent is available to receive an ACD call and is automatically placed into the ACW state upon release from the call.

measured	A term meaning that an ACD element such as agent, split/skill, trunk, trunk group, VDN, or vector that is identified to CMS for data collection. If the ACD element is not measured, no data is collected.
MI	See Manual-In (MI) on page 473.
MIA	See Most Idle Agent (MIA) on page 474.
monthly data	Daily data that has been converted to a monthly summary.
Most Idle Agent (MIA)	An ACD distribution method that maintains a queue of idle agents. An agent is put at the end of the list for a particular split when the agent completes an ACD call for that split. The agent continues to advance on the list as long as he or she remains staffed and in ACW, AVAIL, or on AUXIN/OUT extension calls from the AVAIL mode.
multi-user mode	A CMS state in which any administered user can log into CMS and data continues to be collected if the data collection feature is enabled.
Multiple Call Handling (MCH)	A process in which an agent receives an ACD call while other calls are active on the agent's station. The agent must put the current call on hold and press Auto-In/Manual-In to receive another ACD call.
multiple split queuing	A Call Vectoring capability that directs a call to up to three splits at the same time, with the first agent who is free receiving the call.
name (synonym) fields	A field in which you can input a name (synonym) that you have entered in the Dictionary. For example, you can input names of agents, splits/skills, agent groups, trunk groups, VDNs, or vectors.
night service	A switch capability that enables calls that arrive after business hours or on weekends to be automatically re-routed to a split, an announcement, or an alternate destination set up for after-hours coverage.
nonprimary split/skill	The second and third splits/skills to which a call queued to multiple splits/skills queues in a VDN. Also called secondary and tertiary split/skill, respectively.
Outbound Call Management (OCM)	A set of switch and adjunct features using ASAI that distributes outbound calls initiated by an adjunct to internal extensions (usually ACD agents).
percent within service level	The percentage of calls that you are expecting or targeting to be answered by an agent within a specific number of seconds.
phantom abandon call timer	A CMS capability that tracks information about abandoned calls. When the phantom abandon call timer is enabled, calls with a duration shorter than the administered value (0 to 10 seconds) are counted as phantom abandon calls. Setting the timer to 0 disables this capability.

previous interval	An intrahour interval that is part of the real-time database. At the end of each intrahour interval, the contents of the current intrahour interval are copied to the previous intrahour interval portion of the real-time database.
primary skill	A skill assigned to an agent as that agent's strongest skill. Primary skills are the areas in which the agent has the most expertise.
pseudo-ACD	An area created on CMS to place previously backed-up ACD data. A pseudo-ACD is not a live (real) ACD and does not communicate with any switch.
queue	A holding area for calls waiting to be answered in the order in which they were received. Calls in a queue may have different priority levels, in which case, calls with a higher priority are answered first.
QUEUED	A trunk state in which an ACD call has seized the trunk and is queued to a split/skill, waiting for an agent to answer.
read permission	A permission with which a CMS user can access and view data; for example, running reports or viewing the Dictionary subsystem.
real-time database	A CMS database consisting of the current intrahour data on each CMS-measured agent, split, trunk, trunk group, VDN, and vector.
real-time reports	A report that shows ACD call activity on agents, split/skills, trunks, trunk groups, VDNs, and vectors for the current or previous intrahour interval.
Redirect On No Answer	An ACD capability that assist the user if a call is not answered in a specified number of rings. The terminal extension, including ports with VRUs, is busied out and the call goes back into the queue at top priority.
refresh rate	The number of seconds that CMS should wait for each update of real-time report data.
reserve agent	An agent whose skills are set so that they do not have a top skill, but are used to handle calls when all other agents of that skill are unavailable. Reserve agents are used for high-priority skills where customers must not wait for long periods of time.
RINGING	1) An agent state consisting of the time a call rings at an agent's voice terminal after leaving the queue and before the agent answers the call. 2) A trunk state in which a call is ringing at the agent's voice terminal.
rolling ASA	A running, weighted, average calculation made without using interval boundaries. Rolling ASA is used for vector routing; it is calculated on the Communication Manager system and set to CMS.

screen-labeled key (SLK)	The first eight function keys at the top of the keyboard that correspond to the screen labels at the bottom of the CMS ASCII terminal screen. The screen labels indicate each key's function.
scripting	A CMS Supervisor capability that allows you to automate operations such as changing an agent's skills, running a report, and exporting report data.
secondary skill	A skill assigned to an agent in a subject that is not that agent's strongest area of expertise. Secondary skills are used in Communication Manager systems with Expert Agent Selection (EAS).
SEIZED	A trunk state in which an incoming or outgoing call is using the trunk.
service level	A time, in seconds, within which all calls should be answered. Also called acceptable service level.
Service Observing - Remote	A feature that allows a user to dial into the switch and monitor a call.
Service Observing - VDNs	A feature available with Communication Manager systems that give a user the ability to monitor the treatment that a call receives as it is processed by a VDN.
shortcut	A series of tasks which, when run, are performed on the CMS server. Shortcuts are a fast, easy way to view windows every day for the same ACD entities.
single-user mode	A CMS mode in which only one administrator can log in to the CMS server. Data continues to be collected if the data collection feature is enabled.
skill	See agent skill on page 467.
skill level	A rating from 1 (highest) to 16 (lowest) that indicates an agent's level of expertise in handling calls for which that expertise is needed.
split	A group of extensions that receive calls.
staffed agent	An agent who is currently logged in to the switch.
standard reports	The set of reports that are supplied with CMS or CMS Supervisor.
station	1) An unmeasured extension 2) An extension that is not currently staffed by an agent or that is a member of an unmeasured split/skill.
switch	A system providing voice or voice/data communication services for a group of terminals.

timetable	A CMS feature that allows you to schedule one or more activities to run unattended. Timetables can be set to run once or at multiple times.
trunk	A telephone circuit that carries calls between two switches, between a central office and a switch, or between a central office and a telephone.
trunk group	A group of trunks that are assigned the same dialing digits: either a phone number or a direct inward dialed (DID) prefix.
uniform call distribution (UCD)	A method of call distribution in which the most idle agent for a skill receives the call (if the agent is available).
universal call identifier (UCID)	A number that uniquely identifies a call in a network of nodes that support UCID.
UNSTAF	An agent state in which the agent is not logged in and, therefore, is not tracked by CMS.
VDN of Origin Announcement (VOA)	A short announcement that is assigned to a VDN through switch administration. The VOA identifies the origin or purpose of a call for the call center agent who answers the call.
VDN skill preference	A prioritized list of agent skills administered for a VDN that are needed or preferred for the answering agent. VDN skill preferences require a call to be routed to an ACD agent with a particular attribute or set of attributes.
vector	A list of steps that process calls according to a user definition. The steps in a vector can send calls to splits, play announcements and music, disconnect calls, give calls a busy signal, or route calls to other destinations based on specific criteria.
Vector Directory Number (VDN)	An extension number that enables calls to connect to a vector for processing. A VDN can connect calls to a vector when the calls arrive over an assigned automatic-in trunk group or when the calls arrive over a DID trunk group and the final digits match the VDN. The VDN by itself may be dialed to access the vector from any extension connected to the switch.
vector step	A single task within a vector that performs an action regarding a call. A vector step consists of a command with the possibility of one or more conditions or parameters, if necessary.
vector step condition	A condition accompanying a vector command that defines the circumstances in which the command is applied to a call.
voice terminal	A telephone set, usually with buttons.
weekly data	Daily data that has been converted to a weekly summary.

write permission

A permission with which a CMS user can add, modify, or delete data and execute processes.

Index

A

accessing script options	411	adding	100 , 102
accessing scripts	410	ACD access permissions	197
ACD		ACD groups	120 , 122
access permissions	196	ACD to an ACD group	120 , 123
settings	268	ACD user permissions	199
settings, viewing	268	agent exceptions	220
setup	267	agent group	46 , 175
ACD access considerations	196	agents to agent group	46 , 50
ACD access permissions		agents to tenant agent groups	250
adding	197	AUX reason code name	59 , 61
deleting	198 , 200	backup/restore devices	327 , 329
modifying	197 , 200	call work code names	68 , 70
ACD Administration Log field descriptions	376	call work codes	127 , 129
ACD Administration Log report	374 , 375	constants	72 , 74
ACD data		custom database items	75 , 77
tracking	27	custom menu	292
ACD features	267	custom menu access permissions	184
ACD from an ACD group		location ID	80 , 82
deleting	120 , 125	login ID name	84 , 86
ACD group benefits	119	logout reason code name	87 , 90
ACD group considerations	118	printer	332 , 333
ACD group contents		pseudo-ACD	271
viewing	121	split or skill name	92
ACD group name		split/skill call profiles	133 , 135
modifying	124	split/skill exceptions	227
renaming	124	split/skill name	94
ACD groups	44 , 118	split/skill permissions	187
adding	120 , 122	split/skill user permissions	189
Call Center Administration	118	tenant agent assignments	248
deleting	121 , 126	tenant agent groups	249
listing	121	tenant call work codes	252
ACD groups in the Dictionary		tenant data user permissions	211
before using	44	tenant split/skill	254
ACD Groups in the Dictionary		tenant trunk groups	255
List all	45	tenant VDNs	257
view contents	44 , 45	tenant vectors	258
ACD name		trunk group name	104 , 106
deleting	42 , 43	trunk group permissions	192 , 194
ACD names	41	users	175
ACD permissions		VDN call profile	143 , 145
viewing	198	VDN name	110 , 112
ACD status	32 , 340	VDN permissions	206 , 209
field descriptions	341	vector data user permissions	201
viewing	340 , 341	vector name	114 , 116
ACD to an ACD group		vector permissions	204
adding	120 , 123	adding a user	175
ACD user permissions		adding an ACD name	41 , 42
adding	199	adding an agent group	49
listing all	199	adding exceptions	
ACD-for-migration description	269	vector	241
activate trace	164	adding VDN access	206
		adding vector access	204
		administering	

administering (<i>continued</i>)		
call center features	118	
custom menu items and access	183	
split/skill exceptions	226	
splits	167	
trunk group exceptions	231	
user permissions	172	
users	172, 173	
VDN assignments	141	
VDN exceptions	235	
VDN skill preferences	130	
vector exceptions	240	
administering exceptions	215	
administering printers	331	
administration		
reports	349	
administration jobs		
scheduling	403	
administration overview	23	
administration scheduling	403	
agent		
changing skills	155	
exceptions, definitions	223	
exceptions, report	352, 359	
templates, changing skills for	155	
tenant	260	
agent exceptions	219	
adding	220	
configuring	219	
deleting	222	
modifying	221	
agent group	48, 49	
adding	46, 175	
deleting	48, 49	
listing agents	50	
Agent group	46	
agent group members		
running a report	352	
agent groups	45	
tenant	261	
agent skill change	151	
agent skills		
adding	152	
changing	153	
deleting	154	
agent string value field descriptions	52	
agent string values	51	
agent trace	163–165	
listing records	166	
agent trace activation	164	
agent tracing	163	
agents		
adding to an agent group	46, 50	
administering	151	
deleting from an agent group	47, 51	
agents from agent group		
deleting	251	
agents to tenant agent groups		
adding	250	
allocated space	282	
allocating		
disk space	279	
allocation per ACD	283	
Already exists status message	32	
ANI/SID		
see automatic number identification/station number		
identification	354, 362	
announcement name		
adding	54, 57	
deleting	56, 58	
listing	56	
modifying	55, 57	
viewing	56	
announcement names	54	
archiving data	297	
data summarizing	298	
archiving status	342	
field descriptions	343	
viewing	342, 343	
assigning		
custom menu access permissions	185	
assigning trunk group access	194	
assigning vectors	204	
automatic number identification/station number		
identification	354, 362	
AUX reason code name		
deleting	60, 62	
AUX reason code names	58	
adding	59, 61	
considerations	58	
listing	60	
modifying	59, 61	
viewing	60	
Avaya InSite Knowledge Base	462	
Avaya support website	462	
B		
backing up data	310	
pseudo-ACD	274	
backing up real ACD data to load on a pseudo-ACD	274	
backup		
adding a full maintenance backup timetable for an		
ACD	320	
cmsadm	310	
maintenance	312	
maintenance backup	313, 314	
performing a CMSADM backup	312	
backup and restore		
considerations	317	
reducing times	318	
backup and restore times		
factors	318	
backup data check	275	

Backup Data window	315
backup error messages	316
backup files used	319
backup storage device	
maintenance best practices	319
backup/restore device	
viewing	329
backup/restore devices	
adding	327 , 329
deleting	328 , 330
listing all	329
modifying	327 , 330
backups	
cmsadm	310
maintenance	310
before administering a printer	331
before administering access to trunk group data	191
before administering passwords	420
before administering report properties	336
before backing up data for a pseudo-ACD	274
before changing agent skills	152
before changing extension split assignments	167
before loading pseudo-ACD data	275
before migrating data	304
before modifying data storage allocation	280
before moving extensions between splits	169
before restoring data	322
before using	
ACD groups in the dictionary	44
before using ACD Administration Log report	374
before using calculations	63
before using call work codes	68
before using exceptions	217
before using External Application Status	301
before using Maintenance Error Log	376
before using shortcuts	446
before using split or skill names	92
before using split or skill string values	96
before using split/skill exceptions	226
before using Switch Setup	267
before using trunk group members report	369
before using VDN assignments	141
before using VDN call profiles	143
before using VDN exceptions	235
before using VDN names	110
before using VDN skill preferences	130
before using vector configuration report	371
before using vector exceptions	240
before using vector names	114
before viewing ACD status	340
before viewing trunk group assignments	138
before you begin scripting CMS operations	409
binary backup	
to a network device	320
bulk removal	
tenant agent assignments	249

C

calculating data space	
CMSADM backup	311
full maintenance backup	313
calculation names	
adding	63
calculations	62
adding	66
deleting	67
listing all	65
modifying	64 , 66
viewing	65
Call Center Administration	
ACD groups	118
call center features	
administering	118
call handling preference	
changing	156
call profiles	
split or skill	132
Call Vectoring	151
Call Work Code	
tenant	262
call work code 0	126
call work code names	
adding	68 , 70
deleting	69 , 71
listing all	70
modifying	69 , 71
viewing	69
call work codes	68 , 126
adding	127 , 129
configuring	126
deleting	127 , 129
listing all	128
unassigned	126
viewing	128
Cancelled status message	32
change password	29 , 179
change skills	
multi-agent	160
changing	
agent skills	155
CMS state	294
exception notification	218
master ACD	294
passwords	180
VDN skill preferences	130 , 131
changing agent skills	151
changing agent string value descriptions	52
changing password	179
changing skills for multiple agents	
PC Client	162
changing user password	
command line	421
changing your password	179

chunks	26	content (<i>continued</i>)	
CMS database items		sort by last updated	460
standard	98	watching for updates	460
CMS overview	23	copying	
CMS remote console	419	agent group	48 , 49
CMS server		tenant agent groups	251
local login	420	creating	
CMS state	293	new report color scheme	35
changing	293 , 294	custom calculations	63
CMS Supervisor		deleting	64
web login	29	custom database items	75
CMS tenancy feature	246	adding	75 , 77
cmsadm backup	310	deleting	76 , 78
collection		listing all	77
delete	460	modifying	76 , 78
edit	460	viewing	76
generating PDF	460	custom menu	
sharing content	460	adding	292
colors threshold	36	deleting	292
colors, reports	34	modifying	292
Communications Tab	34 , 37	custom menu access permissions	
configuring LDAP	347	adding	184
connection status	337	assigning	185
descriptions	338	listing all	185
viewing	337 , 338	modifying	184 , 185
considerations	46	viewing	184 , 185
ACD access	196	custom menu items	291
agent exceptions	219	custom menu items and access	184
AUX reason codes	58	administering	183
backing up and restoring	317		
call vectors	201	D	
data storage allocation	278	data	
deleting users	178	historical, migrating	305 , 306
free space allocation	282	migrating	305 , 306
login ID names	83	storage, allocating	279
maintenance backup	313	data archiving	297
migrate data	317	data backup	310
multi-agent skill changes	160	data chunks	26
restore data	317	data collection	
tenant access permissions	211	disabling	296
trunk group names	104	enabling	296
VDN access	206	report	354 , 361
vector access	201	turning on and off	295 , 296
considerations for ACD groups	118	data restore	376
considerations for CMS state	293	data storage allocation	278
considerations for pseudo-ACDs	269	modifying	280
considerations for user permissions	172	Data Storage Allocation	279
constants	72	field definitions	280
adding	72 , 74	data summarization time zone	149 , 299 , 300
deleting	73 , 75	Data summarization time zone fields	150
listing	73	data summarizing	24 , 285 , 297 , 298
modifying	72 , 74	data summarizing time settings	
viewing	73	modifying	289
content		data tracking	27
publishing PDF output	460	Database constants	72
searching	460	database items	
sharing	460		

database items (<i>continued</i>)		
custom	75	
date and time on status indicator	32	
dbspace	26	
dbspaces		
contents, viewing	285	
Default ACD	33	
defining entity formats	37	
definitions		
split/skill exceptions	229	
deleting		
ACD access permissions	198 , 200	
ACD from an ACD group	120 , 125	
ACD groups	121 , 126	
agent exceptions	222	
agent group	48 , 49	
agents from an agent group	47 , 51	
announcement name	56 , 58	
AUX reason code name	60 , 62	
backup/restore devices	328 , 330	
calculations	67	
call work code names	69 , 71	
call work codes	129	
constant	73 , 75	
custom calculations	64	
custom database items	76 , 78	
custom menu	292	
location ID	81 , 83	
login ID name	85 , 87	
logout reason code name	88 , 91	
printer	333 , 335	
pseudo-ACDs	273	
skill name	93	
split/skill call profile	137	
split/skill exceptions	229	
split/skill name	95	
tenant agent group	252	
tenant call work codes	253	
tenant name	101 , 103	
tenant permissions	212	
tenant split/skill	255	
tenant trunk groups	256	
tenant VDNs	258	
tenant vectors	259	
trunk group data user permissions	193	
trunk group name	105 , 107	
users	179	
VDN call profile	148	
VDN data user permissions	207	
VDN exceptions configuration	238	
VDN name	111 , 113	
VDN permissions	210	
vector name	115 , 117	
vector permissions	202 , 205	
deleting a user	178	
deleting access		
split/skill	188	
deleting agents		
from agent group	251	
deleting permissions		
split/skill	188	
devices		
backup/restore	327	
dictionary		
global search results	40	
searching	40	
Dictionary		
ACD groups	44	
ACD Groups in the Dictionary	44 , 45	
ACD name, deleting	43	
adding announcement	54	
agent group members report, running	352	
announcement name, adding	57	
announcement name, viewing	56	
calculation names	63	
calculations	65 , 66	
call work code names, listing all	70	
call work codes	68	
constants	72	
custom database items	75	
location ID, listing all	81	
location IDs	80	
login ID names	83	
logout reason code names	87	
removing ACD name	42	
reports, printing	351	
searching	40	
split/skill names	91	
split/skill string values	95	
standard CMS database items	98	
trunk group names	103	
trunk string values	107 , 108	
VDN names	110	
vector names	113	
Dictionary ACDs Report	350	
Dictionary Login Identifications Report	350	
Dictionary permissions	39	
Dictionary rules	39	
Dictionary Standard CMS Items Report	350	
Dictionary tenant report	350	
Dictionary Trunk Groups Report	351	
Dictionary VDNs Report	351	
Dictionary Vectors Report	351	
direct agent calls		
changing skills	157	
disabling		
data collection	296	
disk space	283	
allocating	279	
document changes	21	
documentation	458	
documentation center	460	
finding content	460	
navigation	460	

documentation portal	460
Does not exist status message	32

E

EAS (See Expert Agent Selection), Expert Agent Selection	151
enabling	
data collection	296
entity formats, defining	37
error and warning messages	418
error log messages	
maintenance	378
Error status message	32
events that start or stop data collection	27
exception capacities	216
exception counter	32
exception notification	
changing	218
exception reports	352
exceptions	215
agent	219
agent, definitions	223
agent, report	352 , 359
data collection	354 , 361
deleting exceptions	
trunk group	233
malicious call trace report	354 , 362
notification	218
real-time exceptions log	244
split skill	226
split/skill, report	355 , 363
trunk group	230 , 233
trunk group, adding	232
trunk group, modifying	233
trunk group, report	356 , 365
VDN	237
VDN, adding	236
VDN, report	357 , 366
vector	240
vector, deleting	243
vector, modifying	242
vector, report	358 , 368
export	
report output	413
Export All Data window	413
Export Chart Data window	413
extensions	
split assignments, changing	167
splits, moving between	168
External Application Status feature	301
disabling	302
enabling	302
external applications	
starting or stopping	303
states, viewing	302

F

Failed status message	32
feature access	
changes	183
list all	182
modifications	183
feature access permissions	180 , 181
modifying	181 , 183
viewing	181
field definitions	
Data Storage Allocation	280
user	175
field descriptions	
split/skill string value	97
finding content on documentation center	460
firewall status	
viewing	344
First Day of Week	33
free space	282 , 283
free space allocation	282
viewing	283
Free Space Allocation	
contents, viewing	285
viewing	284
free space allocation considerations	282

G

generic string value synonyms	79
generic string values	
modifying	79
viewing	79
getting started	29
global search results	40

H

historical data	
archiving	298
historical databases	23
how calls are tracked	27
how CMS logically stores ACD data	23
how CMS tracks ACD data	27

I

input window	
scripting	415
interactive and automatic scripts	410
interactive report script	
creating	412
interrupt type associated with the skill	
changing	157
interval	
intrahour	285

intervals		location ID (<i>continued</i>)	
storage	285	viewing	81
intrahour interval	285	location IDs	80
modifying	288	adding	82
J		logging in	
job details	405	CMS Supervisor Web	29
jobs area	405	logging in to CMS	419
K		logical data storage	23
KB		logical database	26
Support site	462	logical storage	
L		ACD data	23
LDAP		login ID name	
cmsadm command	347	adding	84 , 86
LDAP integration	346	deleting	85 , 87
license status		listing	85
viewing	345	modifying	84 , 86
Linux		viewing	85
remote login	419	login ID names	83
list all permissions	182	considerations	83
listing		login status	32
ACD groups	121	logout reason code name	
announcement name	56	adding	87 , 90
AUX reason code names	60	deleting	88 , 91
constants	73	listing all	89
custom database items	77	modifying	88 , 90
custom menu access permissions	185	viewing	89
login ID name	85	logout reason code names	87
logout reason code name	89	M	
split/skill name	93	Main Menu Addition	291
trunk group names	105	main menu addition access	183
VDN name	112	maintenance	309
vector name	115	reports	349
listing agents in an agent group	50	maintenance backup	312
listing agents traced	166	maintenance backup timetable	
listing all		for an ACD	320
ACD user permissions	199	maintenance error log	
backup/restore devices	329	report	377
call work codes	128	Maintenance Error Log	
printers	333	running	376
split/skill permissions	189	Maintenance Error Log messages	378
trunk group permissions	194	maintenance reports	374
VDN permissions	208	making changes	
VDN skill preferences	131	finishing	159
vector data user permissions	203	malicious call trace	
loading data		report	354 , 362
pseudo-ACD	276 , 277	master ACD	
location ID		changing	294
adding	80	time synchronization	293
deleting	81 , 83	maximum retention settings	407
modifying	80 , 82	migrate data	317
		Migrate Data field descriptions	307
		migrating data	304 – 306
		migration	304
		modifying	
		ACD access permissions	197 , 200

modifying (<i>continued</i>)		
ACD group name	124	
agent exceptions	221	
agent string value descriptions	51	
announcement name	55, 57	
AUX reason code name	59, 61	
backup/restore devices	327, 330	
call work code	69	
call work code names, modifying	71	
constants	72, 74	
custom calculation	64, 66	
custom database items	76, 78	
custom menu	292	
custom menu access permissions	184, 185	
data storage allocation	280	
data summarizing time settings	289	
feature access permissions	181	
generic string values	79	
intrahour interval	288	
location ID	80, 82	
login ID name	84, 86	
logout reason code name	88, 90	
printer options	332, 334	
report properties	336	
skill name, modifying	92	
skill string values	96	
split or skill call profile	133	
split/skill call profile	136	
split/skill exceptions	228	
split/skill string values	96	
split/skill user permissions	190	
ssplit/skill name, modifying	94	
switch time zone	289	
tenant data user permissions	212	
tenant name	101, 102	
trunk group data permissions	193, 195	
trunk group name	104, 106	
trunk string value	107, 108	
users	178	
VDN access	207	
VDN call profile	144, 147	
VDN name	110, 112	
VDN permissions	207, 209	
vector data user permissions	202	
vector name	114, 116	
vector permissions	204	
modifying a user	177	
modifying access	184	
split/skill	188	
modifying an ACD name	41, 43	
modifying custom menu item access	184	
modifying exceptions		
VDN	237	
modifying permissions		
split/skill	188	
trunk group access	193	
modifying trunk group access	195	
mounted volume contains CMS data	317	
Mounted volume is bad	317	
multi-agent skill change	160	
multi-user mode	293	
setting	294	
multiple agents		
applying changes	158	
multiple split/skill profiles in the Web client	134	
N		
N matches found	32	
Name Format Tab	37	
network mount point		
maintaining	319	
new percent allocation		
specifying	158	
new report color scheme, creating	35	
No CMS access to specified device	317	
No matches found status message	32	
No permission status message	32	
O		
operating system, Linux	419	
Options		
Communications Tab	37	
Default ACD	33	
First Day of Week	33	
general	33	
Name Format Tab	37	
report colors	34	
threshold colors	36	
time synchronization	33	
Options window, before using	31	
Options...		
Communications Tab	34	
P		
password aging		
cmsadm	421	
password change	179	
password management		
Web Client	179	
passwords		
changing	179, 180	
choosing	420	
PC Client tenant administration sub-menus	260	
period reboots		
preventative maintenance	309	
permissions	172	
ACD	196	
agent administration	151	
agent exceptions	219	
custom menu access	185	

permissions (<i>continued</i>)		
Dictionary reports	350	
for ACD Administration Log report	374	
for changing extension split assignments	167	
for External Application Status	302	
for moving extensions between splits	169	
for running a split members report	170	
for shortcuts	446	
for timetables	424	
for trunk group members report	370	
for vector configuration report	371	
Free Space Allocation	283	
list all split/skill	189	
split/skill exceptions	226	
split/skill, deleting user	191	
split/skill, modifying user	190	
trunk group exceptions	231	
VDN exceptions	235	
vector exceptions	240	
permitted ones displayed	32	
phantom abandon call timer	267	
preferences	30	
settings	30	
prerequisite tasks		
tenant administration	247	
printer		
adding	332 , 333	
deleting	333 , 335	
printer options		
modifying	332 , 334	
printers		
listing all	333	
pseudo-ACD		
adding	270 , 271	
deleting	270	
loading data	276 , 277	
pseudo-ACD data		
loading	275	
pseudo-ACDs		
deleting	273	
viewing	270	
Pseudo-ACDs	269	
R		
real-time exceptions log	245	
reason code		
logout	87	
reason code name		
logout	88	
reboot CMS server	309	
reduce system failure risks		
reboot	309	
reducing backup and restore times	318	
related documentation	458	
remove		
call work codes	127	
remove agent		
from tenant agent group	250	
remove one agent		
from tenant agent group	250	
removinf		
VDN call profile	144	
removing		
individual agent	248	
individual tenant trunk group	256	
single agent from tenant	248	
tenant agent assignments	249	
Removing	134	
split or skill call profile	134	
removing a call work code	253	
Removing a multiple call work codes in the Web Client	127	
removing agent from agent group		
Dictionary	47	
removing agents		
from a skill	161	
removing agents in bulk		
from tenant	249	
removing an agent	248	
removing an individual agent	248	
removing individual agent		
from agent group	47	
removing multiple VDN call profiles	144	
removing tenant split/skill	254	
removing tenant trunk group	256	
removing trunk group		
for tenant	256	
removing VDN		
from tenant	257	
removing vector		
from tenant	259	
report		
ACD Administration Log	375	
trunk group members	370	
vector configuration	371 , 372	
report colors	34	
report properties	335	
modifying	336	
reports		
ACD Administration Log	374	
administration	349	
colors	36	
data collection	354 , 361	
Dictionary	349	
Dictionary, printing	351	
exceptions	352	
exceptions, agent	352 , 359	
exceptions, trunk group	356 , 365	
maintenance	349	
maintenance error log	377	
malicious call trace	354 , 362	
members, trunk group	369	
split members, running	170	
split/skill, exceptions	355 , 363	

reports (<i>continued</i>)	
tenant agent group members	373
tenant agent groups	373
VDN, exceptions	357 , 366
vector, exceptions	358 , 368
reports saved as HTML	414
restore	
automatic	323 , 324
manual	323 , 325
restore data	317
restore database from a binary backup	326
restore error messages	316
restore list file	319
restoring data	322 , 376
retention period	
customizing	407
running	
ACD Administration Log report	375
running a split members report	170
S	
Save As HTML window	414
Save as Script - Action window	416
scheduled jobs	403
Scheduler page	405
scheduling administration jobs	403
script	
creating automatic	413
creating to run reports	410
exporting report output	413
to export report data as HTML	414
Script descriptions	411
scripting	
tasks	415
scripting an action	416
scripting an input window	415
Scripting tab	34
scripts	
accessing	410
organizing	417
searching for content	460
searching the dictionary	40
See status window message	32
service level	
increment	133 , 135
increments	142
setting	
preferences	30
setting user ID and password	412
setting users	412
settings	
ACD	268
ACD, viewing	268
switch	268
setup	
ACD switch	267
severity of errors	378
sharing content	460
shortcuts	423
copying	451
copying tasks in	452
creating	447
deleting	456
description, modifying	450
overview	446
running	449
tasks, adding	448
tasks, deleting	455
tasks, modifying	454
single tenant call work code	
deleting	253
removing	253
single-user mode	293
setting	294
skill assigned to the agent or template	
removing	157
skill assignment for other agents	
changing	159
skill name	
deleting	93
modifying	92
skill string values	
modifying	96
skills for multiple agents	
adding	160
deleting	161
moving	161
sort documents	460
split	
extension assignments, changing	167
extensions, moving	168
members report, running	170
split or skill	
call profiles	132
string values	95
split or skill access	186
split or skill call profile	
deleting	134
modifying	133
split or skill name	
adding	92
split skill	
exceptions	226
split/skill	
exceptions, report	355 , 363
listing all	189
user permissions	189
user permissions, deleting	191
split/skill access	187
split/skill access considerations	186
split/skill call profile	
deleting	137
modifying	136

split/skill call profile (<i>continued</i>)		tasks (<i>continued</i>)	
viewing	135	timetable, adding	423 , 428
split/skill call profiles		timetable, modifying	435
adding	133 , 135	tasks scripts can automate	409
split/skill exceptions		tenancy examples	246
adding	227	tenancy feature package	100
administering	226	tenancy prerequisites	247
definitions	229	tenant	
deleting	229	agent	260
modifying	228	agent groups	261
split/skill for tenant		Call Work Code	262
removing one	254	trunk group	264
split/skill name		VDN	264
adding	94	vector	265
deleting	95	tenant access	210 , 213
modifying	94	operations	213
viewing	93	tenant access considerations	211
split/skill names	91	tenant administration	100
listing all	93	tenant administration reports	372
split/skill permissions		tenant agent assignments	
deleting	188	adding	248
modifying	188	removing	249
removing	188	tenant agent group	
split/skill string value		deleting	252
field descriptions	97	remove one agent	250
split/skill string values		tenant agent group members	
modifying	96	report	373
viewing	96	tenant agent groups	
split/skill user permissions		adding	249
adding	189	copying	251
viewing	188	report	373
standard CMS database item		tenant call work code	
viewing	99	deleting	253
standard CMS database items	98	removing	253
standard database items		tenant call work codes	
viewing alphabetically	99	adding	252
status indicators on controller window	32	deleting	253
status messages on Controller window	32	tenant data user permissions	
storage interval considerations	286	adding	211
storage intervals	285	modifying	212
viewing	286 , 288	tenant features	246
Successful status message	32	tenant name	100 , 102
support	462	adding	100 , 102
switch		deleting	101 , 103
settings	268	modifying	101 , 102
settings, viewing	268	viewing	101
switch setup information		tenant names	100
viewing	267	Tenant names	
switch time zone		Listing all	102
modifying	289	tenant permissions	
system settings		deleting	212
configuring	267	tenant prerequisites	100
T		tenant split/skill	
table cannot be backed up	317	adding	254
tasks		deleting	255
		Tenant split/skill assignment	263
		tenant trunk groups	

tenant trunk groups (<i>continued</i>)		trunk group assignment	
adding	255	viewing a single	139
deleting	256	viewing by VDN or split	140
tenant user access restrictions	247	trunk group assignments	
tenant VDNs		viewing	139
adding	257	viewing all	139
deleting	258	trunk group data access	191
tenant vectors		trunk group data permissions	192
adding	258	modifying	193 , 195
deleting	259	trunk group data user permissions	
tenants	100	deleting	193
the agent or template		Trunk group exception definitions	234
adding skill	158	trunk group exceptions	
threshold colors	36	administering	231
time synchronization	33	trunk group members	
master ACD	294	report	370
time zones		trunk group name	
updating	464	adding	104 , 106
timetable		deleting	105 , 107
deleting	444	listing all	105
maintenance backup	320	modifying	104 , 106
tasks, adding	423	trunk group names	103
timetables	423	listing	105
backups	423	trunk group naming considerations	104
changing	423	trunk group permissions	
copying	431	adding	194
creating	423 , 425	deleting	196
global edits	437	listing all	194
listing all	430	viewing	194
overview	423	trunk string value descriptions	108
prerequisites	423	trunk string values	107
scheduling	425	modifying	107 , 108
tasks, adding	428	viewing	107 , 108
tasks, copying	433	turning data collection on and off	295
tasks, modifying	435	type associated with the skill	
timezone		changing	157
adjustment, ACD	285	types of exceptions	215
top skill for the agent			
assigning	158	U	
trace agents	163	Unix	
track calls	27	password change	421
tracking CMS calls	27	user	
tracking data	27	field definitions	175
trunk group		user administration	172
assignments	138	user data	173
deleting exceptions	233	user permissions	
exceptions	230	administering	172
exceptions, adding	232	considerations	172
exceptions, modifying	233	list all	182
exceptions, report	356 , 365	modifying	183
members report	369	viewing	182
tenant	264	user permissions example	172
trunk group access		users	
adding	192	ACD permissions	196
trunk group access entry		adding	175
deleting	196	administering	172 , 173
removing	196		

users (<i>continued</i>)			
custom menu access permissions	185		
deleting	178 , 179		
feature access permissions	182		
modifying	177 , 178		
permissions	182		
permissions, deleting split/skill	191		
viewing	173 , 174		
using split or skill call profiles	132		
V			
VDN			
call profiles	142		
exceptions, adding	236		
exceptions, report	357 , 366		
tenant	264		
VDN access	205		
VDN access considerations	206		
VDN assignments	140		
administering	141		
modifying	142		
viewing	141		
viewing by vector	142		
VDN call profile			
adding	143 , 145		
deleting	144 , 148		
modifying	144 , 147		
viewing	145		
VDN data user permissions			
deleting	207		
VDN exceptions	235		
administering	235		
deleting	238		
modifying	237		
VDN name			
adding	110 , 112		
deleting	111 , 113		
listing	112		
modifying	110 , 112		
viewing	111		
VDN names	110		
VDN permissions			
adding	206 , 209		
deleting	210		
listing all	208		
modifying	207 , 209		
viewing	208		
VDN skill preferences			
administering	130		
changing	130 , 131		
listing all	131		
viewing	131		
vector			
configuration report	371		
exceptions, deleting	243		
exceptions, modifying	242		
vector (<i>continued</i>)			
exceptions, report	358 , 368		
tenant	265		
vector access	201		
deleting	205		
removing	205		
vector access considerations	201		
vector configuration			
report	371 , 372		
vector data permissions			
deleting	202 , 205		
modifying	204		
vector data user permissions			
adding	201		
listing all	203		
modifying	202		
viewing	203		
vector exception definitions	244		
vector exceptions	240		
adding	241		
administering	240		
vector name			
adding	114 , 116		
deleting	115 , 117		
listing	115		
modifying	114 , 116		
viewing	115		
vector names	113		
vector permissions			
adding	204		
videos	462		
viewing			
ACD group contents	121		
ACD permissions	198		
ACD status	340 , 341		
announcement name	56		
archiving status	342 , 343		
AUX reason code name	60		
backup/restore device	329		
call work code names	69		
call work codes	128		
connection status	337 , 338		
constants	73		
custom database item	76		
custom menu access permissions	184 , 185		
feature access permissions	181		
firewall status	344		
Free Space Allocation	284		
generic string values	79		
license status	345		
location ID	81		
login ID name	85		
logout reason code name	89		
pseudo-ACDs	270		
real-time exceptions log	245		
split/skill call profile	135		
split/skill name, viewing	93		

viewing (<i>continued</i>)	
split/skill string values	96
split/skill user permissions	188
standard CMS database item	99
standard database items	99
storage intervals	286 , 288
tenant name	101
trunk group assignments	139
trunk group name	105
trunk group permissions	194
trunk string value	107 , 108
user permissions	182
users	173 , 174
VDN assignments	141
VDN call profile	145
VDN name	111
VDN permissions	208
VDN skill preferences	131
vector data user permissions	203
vector name	115
viewing a single	
trunk group assignment	139
viewing ACD groups	
Dictionary	44
viewing all	
trunk group assignments	139
viewing by VDN or split	
trunk group assignment	140
virtual login	420
volume mounted has errors	317
volume mounted is the last backup volume	317

W

watchlist	460
web client	
agent exceptions	219
Web Client scheduling	403
working status message, successful status message, error status message, failed status message	32