# Avaya Call Management System Administration

Release 18
October 2015

© 2015, Avaya Inc.
All Rights Reserved.

**Notice**

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

**Documentation disclaimer**

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

**Link disclaimer**

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

**Warranty**

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

**Licenses**

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

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

**License type(s)**

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A “Unit” means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

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

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as “shrinkwrap” or “clickthrough” license accompanying or applicable to the Software (“Shrinkwrap License”).

**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, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

**Third Party Components**

“Third Party Components” mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements (“Third Party Components”), which contain terms regarding the rights to use certain portions of the Software (“Third Party Terms”). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available

in the products, Documentation or on Avaya's website at: http://support.avaya.com/Copyright or such successor site as designated by Avaya. You agree to the Third Party Terms for any such Third Party Components.

**Preventing Toll Fraud**

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

**Avaya Toll Fraud intervention**

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: http://support.avaya.com or such successor site as designated by Avaya. Suspected security vulnerabilities with Avaya products should be reported to Avaya by sending mail to: securityalerts@avaya.com.

**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, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

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: http://support.avaya.com, or such successor site as designated by Avaya.

**Contact Avaya Support**

See the Avaya Support website: http://support.avaya.com for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: http://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** ..... 18
Purpose ..... 18
Intended audience ..... 18
Document changes since last issue ..... 18
Related resources ..... 19
Documentation ..... 19
Viewing Avaya Mentor videos ..... 19
Documentation websites ..... 20
Support ..... 20
**Chapter 2: About CMS Administration** ..... 21
About CMS Administration ..... 21
What is Avaya CMS? ..... 21
How Avaya CMS stores ACD data ..... 22
How Avaya CMS logically stores ACD data ..... 22
How Avaya CMS physically stores ACD data ..... 25
ACD Administration ..... 27
How CMS tracks ACD data ..... 27
About CMS tenancy ..... 29
Administering tenancy at a high level ..... 30
**Chapter 3: Configuring Avaya CMS Supervisor** ..... 32
Configuring Avaya CMS Supervisor ..... 32
Before using the Options window ..... 32
Controller features ..... 33
Overview of the Controller ..... 33
Toolbar ..... 33
Status indicators ..... 33
Status messages ..... 33
Menu bar ..... 34
General tab ..... 34
Scripting tab ..... 35
Report Colors tab ..... 36
Creating a new report color scheme ..... 36
Threshold Colors tab ..... 37
Creating a new threshold color scheme ..... 37
Name Format tab ..... 38
Defining entity formats ..... 39
**Chapter 4: Using The Dictionary To Name Contact Center Entities** ..... 40
Using the Dictionary to name contact center entities ..... 40
About the Dictionary ..... 40

Before using the Dictionary window ... 41
Dictionary rules ... 41
About searching the Dictionary ... 42
Dictionary global search results ... 43
ACD Groups in the Dictionary ... 43
Before using ACD groups ... 44
Permissions for ACD groups ... 44
Listing all ACD Groups ... 44
Viewing the contents of an ACD Group ... 45
ACDs ... 45
Permissions for ACDs ... 46
Adding an ACD name ... 46
Modifying an ACD name ... 46
Deleting an ACD Name ... 47
Agent groups ... 47
Permissions for agent groups ... 48
Considerations when sizing and reporting on agent groups ... 48
Adding an agent group ... 48
Listing agents in an agent group ... 49
Copying an existing agent group to a new name ... 49
Adding agents to an existing agent group ... 50
Deleting agents in an existing agent group ... 50
Deleting an agent group ... 51
Agent string values ... 51
Permissions for agent string values ... 51
Changing agent string value descriptions ... 51
Agent string value field descriptions ... 52
Announcements ... 54
Permissions for announcement names ... 54
Before using announcement names ... 54
Adding an announcement name ... 54
Viewing an announcement name ... 55
Listing all announcement names for an ACD ... 55
Modifying an announcement name ... 56
Deleting an announcement name ... 56
AUX reason code names ... 57
Permissions for AUX reason code names ... 57
Before using AUX reason code names ... 57
Adding an AUX reason code name ... 58
Viewing an AUX reason code name ... 58
Listing all AUX reason code names ... 59
Modifying an AUX reason code name ... 59
Deleting an AUX reason code ... 60

Calculations ... 60
Permissions for calculations ... 60
Before using calculations ... 61
Viewing a calculation ... 61
Listing all calculations ... 62
Adding a calculation ... 62
Modifying a custom calculation ... 63
Deleting a custom calculation ... 63
Call work codes ... 64
Permissions for call work codes ... 64
Before using call work codes ... 64
Adding a name to a call work code ... 65
Viewing a call work code name ... 65
Listing all call work code names ... 66
Modifying a call work code name ... 66
Deleting a call work code name ... 67
Constants ... 67
Permissions for constants ... 67
Adding a constant ... 68
Viewing a constant ... 68
Listing all constants ... 68
Modifying a constant ... 69
Deleting a constant ... 69
Custom database items ... 70
Permissions for custom database items ... 70
Before using custom database items ... 70
Adding a custom database item ... 70
Viewing a custom database item ... 71
Listing all custom database items ... 71
Modifying a custom database item ... 72
Deleting a custom database item ... 72
Generic string values synonyms ... 73
Permissions for Generic string values synonyms ... 73
Viewing generic string values ... 73
Modifying generic string values ... 73
Location IDs ... 74
Permissions for location ids ... 74
Adding a location ID ... 74
Viewing a location ID ... 74
Listing all location IDs ... 75
Modifying a location ID ... 75
Deleting a location ID ... 76
Login ID names ... 76

Permissions for login IDs ... 77
Before using login ID names ... 77
Adding a name to a login ID ... 77
Viewing a login ID name ... 78
Listing all login ID names ... 78
Modifying a login ID name ... 79
Deleting a login ID name ... 79
Logout reason code names ... 80
Permissions for logout reason code names ... 80
Before using logout reason code names ... 80
Adding a logout reason code name ... 80
Viewing a logout reason code name ... 81
Listing all logout reason code names ... 81
Modifying a logout reason code name ... 82
Deleting a logout reason code name ... 82
Split/skill string values ... 83
Permissions for split/skill string values ... 83
Before using split/skill string values ... 83
Viewing split/skill string values ... 83
Modifying split/skill string values ... 84
Split/skill string value field descriptions ... 84
Split/Skill names ... 85
Permissions for split/skill names ... 86
Before using split/skill names ... 86
Adding a split/skill name ... 86
Viewing a split/skill name ... 87
Listing all the split/skill names ... 87
Modifying a split/skill name ... 87
Deleting a split/skill name ... 88
Standard database items ... 89
Permissions for standard database items ... 89
Viewing a standard database item ... 89
Viewing all standard database items alphabetically ... 90
Tenant names ... 90
Permissions for tenant names ... 90
Before using tenant names ... 91
Adding a tenant name ... 91
Viewing a tenant name ... 91
Listing all tenant names ... 92
Modifying a tenant name ... 92
Deleting a tenant name ... 92
Trunk group names ... 93
Permissions for trunk group names ... 93

Before using trunk group names ..... 93
Adding a trunk group name ..... 94
Viewing a trunk group name ..... 94
Listing all trunk group names ..... 95
Modifying a trunk group name ..... 95
Deleting a trunk group name ..... 95
Trunk string values ..... 96
Permissions for trunk string values ..... 96
Viewing and modifying trunk string values ..... 96
Trunk string values field descriptions ..... 97
VDN names ..... 98
Permissions for VDN names ..... 99
Before using VDN names ..... 99
Adding a VDN name ..... 99
Viewing a VDN name ..... 100
Listing all VDN names ..... 100
Modifying a VDN name ..... 101
Deleting a VDN name ..... 101
Vector names ..... 102
Permissions for vector names ..... 102
Before using vector names ..... 102
Adding a vector name ..... 103
Viewing a vector name ..... 103
Listing all vector names ..... 104
Modifying a vector name ..... 104
Deleting a vector name ..... 104
Dictionary reports ..... 105
Permissions for dictionary reports ..... 105
Types of Dictionary reports ..... 105
Printing dictionary reports ..... 107
Running an agent group members report ..... 108
**Chapter 5: Using Reports** ..... 109
Background ..... 109
About reports ..... 110
Interfaces for reports ..... 110
Types of reports ..... 110
What reports summarize ..... 111
The Reports subsystem ..... 111
Choosing a report ..... 112
Generating a report ..... 112
Printing a report ..... 113
Printing a Historical report ..... 113
Changing the print setup ..... 114

Restarting a report ..... 114
Restarting a report in CMS Supervisor Web ..... 114
**Chapter 6: Scripting CMS Operations** ..... 115
Scripting CMS operations ..... 115
Before you begin scripting CMS operations ..... 115
Tasks scripts can automate ..... 115
Interactive and automatic scripts ..... 116
Script creation ..... 116
Scripting options description ..... 117
Setting user ID and password ..... 118
Creating an interactive report script ..... 118
Creating an automatic report script ..... 119
Creating a script to export report data ..... 119
Creating a script to export report data as HTML ..... 120
Scripting other Supervisor operations ..... 121
Actions not associated with reports ..... 121
About scripting an input window ..... 121
Scripting an action ..... 122
Organizing scripts ..... 123
Error and warning messages ..... 123
**Chapter 7: Administering Contact Center Agents** ..... 125
Administering contact center agents ..... 125
About starting or stopping an agent trace ..... 125
Viewing current agent trace states ..... 127
About listing agents traced ..... 127
About changing agent skills ..... 129
Before changing agent skills ..... 129
Permissions for changing agent skills ..... 130
Changing agent skills ..... 130
Change agent skills in CMS Supervisor Web ..... 133
Changing agent skills ..... 134
Adding agent skills ..... 134
Deleting agent skills ..... 135
About changing skills for multiple agents ..... 136
Before changing skills for multiple agents ..... 136
Permissions for changing skills for multiple agents ..... 137
Changing skills for multiple agents ..... 137
Multi-Agent skill change in CMS Supervisor Web ..... 138
Adding skills for multiple agents ..... 139
Moving skills for multiple agents ..... 139
Deleting skills for multiple agents ..... 140
About changing extension split assignments ..... 140
Before changing extension split assignments ..... 141

Permissions for changing extension split assignments..... 141
Changing extension split assignments..... 141
About moving extensions between splits..... 142
Before moving extensions between splits..... 142
Permissions for moving extensions between splits..... 143
Moving extensions between splits..... 143
About running a split members report..... 144
Permissions for running a split members report..... 144
Running a split members report..... 144
**Chapter 8: Administering The Contact Center**..... 146
Administering the contact center..... 146
Before administering the contact center..... 146
ACD Groups..... 146
Call work codes..... 153
Before using call work codes..... 153
Permissions for call work codes..... 154
Adding call work codes..... 154
Viewing call work codes..... 155
Listing all call work codes..... 155
Deleting call work codes..... 156
VDN skill preferences..... 156
Before using VDN skill preferences..... 157
Permissions for VDN skill preferences..... 157
Changing VDN skill preferences..... 157
Viewing VDN skill preferences..... 158
Listing all VDN skill preferences..... 158
Split/skill call profiles..... 159
Before using split/skill call profiles..... 159
Permissions for split/skill call profiles..... 159
Adding split/skill call profiles..... 160
Viewing an existing split/skill call profile..... 161
Modifying a split/skill call profile..... 162
Deleting a split/skill call profile..... 162
Trunk group assignments..... 163
Before using trunk group assignments..... 163
Permissions for trunk group assignments..... 163
Viewing all trunk group assignments..... 164
Viewing a single trunk group assignment..... 164
Viewing a trunk group assignment by VDN or split..... 165
Trunk group members report..... 165
Before using trunk group members report..... 166
Permissions for trunk group members report..... 166
Running a trunk group members report..... 166

VDN-to-vector assignments ... 167
Before using VDN-to-vector assignments ... 167
Permissions for VDN-to-vector assignments ... 167
Viewing all VDN-to-vector assignments ... 167
Listing VDNs associated with a vector ... 168
VDN call profiles ... 168
Before using VDN call profiles ... 169
Permissions for VDN call profiles ... 169
Adding a VDN call profile ... 169
Viewing an existing VDN call profile ... 170
Modifying a VDN call profile ... 171
Deleting a VDN call profile ... 172
Vector configuration report ... 172
Before using vector configuration report ... 173
Permissions for vector configuration report ... 173
Running vector configuration reports ... 173
Data summarization time zone ... 174
Data summarization time zone fields ... 174
**Chapter 9: Administering Exceptions** ... 176
Administering exceptions ... 176
About exceptions ... 176
Before using exceptions ... 178
Permissions for exceptions ... 179
Exception notification ... 179
Changing exception notification ... 180
Agent exceptions ... 180
Before using agent exceptions ... 180
Permissions for agent exceptions ... 181
Adding agent exceptions ... 181
Modifying agent exceptions ... 182
Deleting agent exceptions ... 183
Agent exception definitions ... 184
Split/skill exceptions ... 187
Before using split/skill exceptions ... 187
Permissions for split/skill exceptions ... 187
Adding split/skill exceptions ... 187
Modifying split/skill exceptions ... 188
Deleting split/skill exceptions ... 189
Split/skill exception definitions ... 190
Trunk group exceptions ... 191
Before using trunk group exceptions ... 191
Permissions for trunk group exceptions ... 192
Adding trunk group exceptions ... 192

Modifying trunk group exceptions..... 193
Deleting trunk group exceptions..... 194
Trunk group exception definitions..... 194
VDN exceptions..... 195
Before using VDN exceptions..... 195
Permissions for VDN exceptions..... 196
Adding VDN exceptions..... 196
Modifying VDN exceptions..... 197
Deleting VDN exceptions..... 198
VDN exception definitions..... 199
Vector exceptions..... 200
Before using vector exceptions..... 200
Permissions for vector exceptions..... 201
Adding vector exceptions..... 201
Modifying vector exceptions..... 202
Deleting vector exceptions..... 203
Vector exception definitions..... 203
Real-time exceptions log..... 204
Before using real-time exceptions log..... 204
Running the real-time exceptions log..... 205
Exception reports..... 205
Running the agent exceptions by location report..... 206
Running the data collection exceptions report..... 207
Running the malicious call trace report..... 208
Running the split/skill exceptions report..... 209
Running the trunk group exceptions report..... 211
Running the VDN exceptions report..... 212
Running the vector exceptions report..... 214
**Chapter 10: Administering User Permissions**..... 216
Administering user permissions..... 216
Before using the User Permissions subsystem..... 216
Example of user permissions..... 216
User data..... 217
About adding a CMS user..... 217
Before adding a CMS user..... 217
Permissions for adding a CMS user..... 217
Adding a CMS user..... 218
About viewing CMS users..... 220
Before viewing CMS users..... 220
Permissions for viewing CMS users..... 220
Viewing CMS users..... 220
About modifying CMS users..... 221
Before modifying CMS users..... 221

Permissions for modifying CMS users ..... 222
Modifying CMS users ..... 222
About deleting CMS users ..... 223
Before deleting CMS users ..... 223
Permissions for deleting CMS users ..... 223
Deleting CMS users ..... 223
ACD access ..... 224
Before using the ACD Access window ..... 224
Permissions for the ACD Access window ..... 225
Adding ACD access ..... 225
Viewing ACD access ..... 226
Listing all ACD access ..... 227
Modifying ACD access ..... 227
Deleting ACD access ..... 228
Feature access ..... 229
Before using the Feature Access window ..... 230
Permissions for the Feature Access window ..... 230
Viewing Feature Access user permissions ..... 231
Listing all Feature Access user permissions ..... 231
Modifying Feature Access user permissions ..... 232
Main Menu Addition Access ..... 232
Before using Main Menu Addition Access ..... 233
Permissions for Main Menu Addition Access ..... 233
Viewing Main Menu Addition Access ..... 233
Listing all Main Menu Addition Access ..... 234
Assigning or modifying Main Menu Addition Access ..... 234
About Tenant Access ..... 235
Tenant Access window ..... 236
Split/Skill access ..... 237
Before using split/skill access ..... 237
Permissions for split/skill access ..... 238
About adding split/skill user permissions ..... 238
About viewing split/skill user permissions ..... 239
About listing all split/skill user permissions ..... 240
About modifying split/skill user permissions ..... 241
Deleting split/skill user permissions ..... 242
Trunk group access ..... 243
Before using the Trunk Group Access window ..... 243
Permissions for the Trunk Group Access window ..... 244
About adding trunk group user permissions ..... 244
About viewing trunk group user permissions ..... 245
About listing all trunk group user permissions ..... 246
About modifying trunk group user permissions ..... 247

Deleting trunk group user permissions..... 248
Vector access..... 249
Before using vector access..... 249
Permissions for vector access..... 250
About adding vector user permissions..... 250
About viewing vector user permissions..... 251
About listing all vector user permissions..... 252
About modifying vector user permissions..... 253
Deleting vector user permissions..... 254
VDN access..... 255
Before using VDN access..... 255
Permissions for VDN access..... 256
About adding VDN user permissions..... 256
About viewing VDN user permissions..... 257
About listing all VDN user permissions..... 258
About modifying VDN user permissions..... 258
Deleting VDN user permissions..... 260
Tenant user restricted access..... 261
Administering tenants..... 262
Supervisor Tenant Administration sub menu..... 262
Tenant agent assignment..... 263
Tenant split/skill assignment..... 263
Tenant trunk group assignment..... 264
Tenant VDN assignment..... 265
Tenant vector assignment..... 266
Tenant Call Work Code assignment..... 267
Tenant agent groups assignment..... 267
Tenant administration reports..... 268
**Chapter 11: Configuring CMS System Settings**..... 270
Configuring CMS system settings..... 270
Before configuring CMS system settings..... 270
CMS state..... 270
Data collection..... 272
Before using Data collection..... 272
Permissions for Data collection..... 273
Changing the data collection state..... 273
Data Storage Allocation..... 274
Before using Data Storage Allocation..... 274
Permissions for Data Storage Allocation..... 275
Viewing Data Storage Allocation..... 275
About modifying Data Storage Allocation..... 275
Data summarizing..... 279
Before using Data summarizing..... 279

Permissions for Data summarizing ..... 280
Archiving data ..... 280
External Application Status ..... 281
Before using External Application Status ..... 281
Permissions for External Application Status ..... 281
Enabling or disabling the External Application Status feature ..... 282
Viewing the states of external applications ..... 282
Starting or stopping external applications ..... 283
Free Space Allocation ..... 284
Before using Free Space Allocation ..... 284
Permissions for Free Space Allocation ..... 284
Viewing Free Space Allocation ..... 284
Viewing Free Space Allocation contents ..... 285
Migrating CMS data ..... 285
Before migrating CMS data ..... 286
Permissions for migrating CMS data ..... 286
Migrating R3 data ..... 286
R3 Migrate Data field descriptions ..... 287
Pseudo-ACDs ..... 289
Before using pseudo-ACDs ..... 289
Permissions for pseudo-ACDs ..... 290
Creating a pseudo-ACD ..... 290
Viewing pseudo-ACDs ..... 293
Deleting a pseudo-ACD ..... 293
About backing up data for a pseudo-ACD ..... 294
About loading pseudo-ACD data ..... 297
Storage intervals ..... 300
Before using Storage intervals ..... 300
Permissions for Storage intervals ..... 300
Viewing storage interval settings ..... 300
About changing the intrahour interval ..... 301
About changing switch time zone ..... 302
About modifying data summarizing settings ..... 303
Switch setup ..... 305
Before using Switch Setup ..... 306
Permissions for Switch Setup ..... 306
Viewing switch setup data ..... 306
Listing all switch setup data ..... 307
**Chapter 12: Maintaining CMS** ..... 308
Maintaining CMS ..... 308
Before using the Maintenance window ..... 308
ACD status ..... 308
Archiving status ..... 311

Before using Archiving Status ..... 311
Permissions for Archiving Status ..... 311
Viewing the archiving status of a single ACD ..... 312
Viewing the archiving status of all ACDs ..... 312
Description of the Archiving Status - List All window ..... 313
Backup/restore devices ..... 313
Permissions for Backup/Restore Devices ..... 313
Viewing a backup/restore device ..... 314
Listing all backup/restore devices ..... 314
Adding a backup/restore device ..... 314
Modifying a backup/restore device ..... 315
Deleting a backup/restore device ..... 316
Data Backup ..... 316
CMSADM backup ..... 316
Maintenance backup ..... 317
Tape drives and cartridges ..... 317
USB/network backup/restore devices ..... 317
Things to consider when backing up or restoring data ..... 318
About adding a Full Maintenance Backup Timetable for an ACD ..... 322
About performing a CMSADM backup ..... 324
About performing a maintenance backup ..... 327
Description of the Backup Data window ..... 328
Restoring data ..... 334
Before restoring data ..... 334
Permissions for restoring data ..... 335
Performing an automatic restore ..... 335
Performing a manual restore ..... 335
Restore database from a binary backup ..... 337
Recommendation to restart your CMS server ..... 337
Connection status ..... 338
Permissions for Connection Status ..... 338
Viewing the connection status of an ACD ..... 338
Listing the connection status of all ACDs ..... 338
Description of the Connection Status window ..... 339
Administering a printer ..... 340
Before administering a printer ..... 340
Permissions for administering a printer ..... 341
Adding a new printer ..... 341
Listing all printers ..... 342
Modifying printer options ..... 342
Deleting a printer ..... 343
Maintenance reports ..... 343
Maintenance Error Log ..... 344

ACD Administration Log ..... 367
Administering Report Properties ..... 369
Before administering report properties ..... 370
Permissions for administering report properties ..... 370
Modifying the Report Properties ..... 370
Advanced Debugging window ..... 371
**Chapter 13: Using the Operating System** ..... 372
Using the operating system ..... 372
Before using the operating system ..... 372
Logging in to CMS ..... 372
Administering passwords ..... 373
Before administering passwords ..... 374
Changing a user's password ..... 374
Administering password aging ..... 375
**Chapter 14: Using Timetables And Shortcuts** ..... 377
Using timetables and shortcuts ..... 377
Timetables ..... 377
Shortcuts ..... 400
**Appendix A: Updating time zones** ..... 411
Updating time zones displayed to users ..... 411
**Glossary** ..... 413

# Chapter 1: Introduction

## Purpose

The document describes how to administer a contact center through Avaya Call Management System (CMS) Supervisor.

## Intended audience

This document is intended for:

- CMS administrators who can gain access to all parts of CMS.
- Split or Skill supervisors with limited access to CMS.

## Document changes since last issue

The following changes have been made to this document since the last issue:

- Changes for the tenancy feature: Summary, Dictionary use, and Tenant administration.
- Changes for administering additional time zones.
- Changes for the new administrative procedures in CMS Supervisor Web.

# Related resources

## Documentation

**Table 1: Related documents**

| Title | Use this document to: | Audience |
|---|---|---|
| Using | | |
| *Avaya CMS Supervisor Reports* | Learn how to use CMS Supervisor Reports. | Call center supervisors and administrators |

## 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.

### Procedure

- To find videos on the Avaya Support website, go to http://support.avaya.com and perform one of the following actions:
  - In **Search**, type `Avaya Mentor Videos` to see a list of the available videos.
  - In **Search**, type the product name. On the Search Results page, select **Video** in the **Content Type** column on the left.
- To find the Avaya Mentor videos on YouTube, go to www.youtube.com/AvayaMentor and perform one of the following actions:
  - Enter a key word or key words in the **Search Channel** to search for a specific product or topic.
  - Scroll down Playlists, and click the name of a topic to see the available list of videos posted on the website.

**Note:**

Videos are not available for all products.

# Documentation websites

All CMS documentation can be found at support.avaya.com. New issues of CMS documentation will be placed on this website when available.

Use the following websites to view related support documentation:

- Information about Avaya products and service

  www.avaya.com

- Sun hardware documentation

  docs.sun.com

- Dell hardware documentation

  www.dell.com

# Support

Go to the Avaya Support website at http://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.

# Chapter 2: About CMS Administration

## About CMS Administration

This section provides introductory information on Avaya CMS Supervisor and complementary products. Basic information about the interfaces and usage of Avaya CMS Supervisor is found in the *Avaya CMS Supervisor Installation and Getting Started* document.

This section contains the following topics:


- What is Avaya CMS? on page 21
- How Avaya CMS stores ACD data on page 22
- ACD Administration on page 27


## What is Avaya CMS?

CMS is a software product for businesses and organizations that have an Avaya Communication Manager system and receive a large volume of telephone calls that the Automatic Call Distribution (ACD) feature processes.CMS collects call-traffic data, formats management reports, and provides an administrative interface to the ACD feature on the Communication Manager system.

A CMS administrator accesses the CMS database, generates reports, administers ACD parameters, and monitors call activities to determine the most efficient service for the calling customers.

**Note:**

In CMS R18, use the tenancy feature to restrict user access to CMS reporting data and functionality within the contact center.

### Operating system

The following platforms support Avaya CMS:

- Specific Sun Microsystems, Inc. platforms running specific versions of Solaris.
- Specific Dell platforms running specific versions of Linux®.
- Specific HP platforms running specific versions of Linux®.

Avaya CMS uses the operating system to communicate with terminals and printers, log errors, and execute processes. CMS utilizes the Informix Software, Inc. INFORMIX database management system, which provides an interface to the CMS historical database.

# How Avaya CMS stores ACD data

Avaya Call Management System (CMS) stores ACD data in two ways:

- Logically: How the CMS system organizes data for processing.
- Physically: How the CMS system mechanically stores the data on the disk drive.

This section includes the following topics:


- How Avaya CMS logically stores ACD data on page 22
- How Avaya CMS physically stores ACD data on page 25


# How Avaya CMS logically stores ACD data

The logical storage of the ACD data has more impact on the CMS user than does the physical storage. The logical data storage controls how a CMS user can gain access to 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 | 62 days |
| Daily historical data | 5 years (1825 days) |
| Weekly historical data | 10 years (520 weeks) |
| Monthly historical data | 10 years (120 months) |

**Note:**

You can use historical data to predict future call traffic and future agent and trunk requirements. For more information see *Avaya CMS Forecast User Guide*.

## 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 current interval database table is archived to the previous interval database table.

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

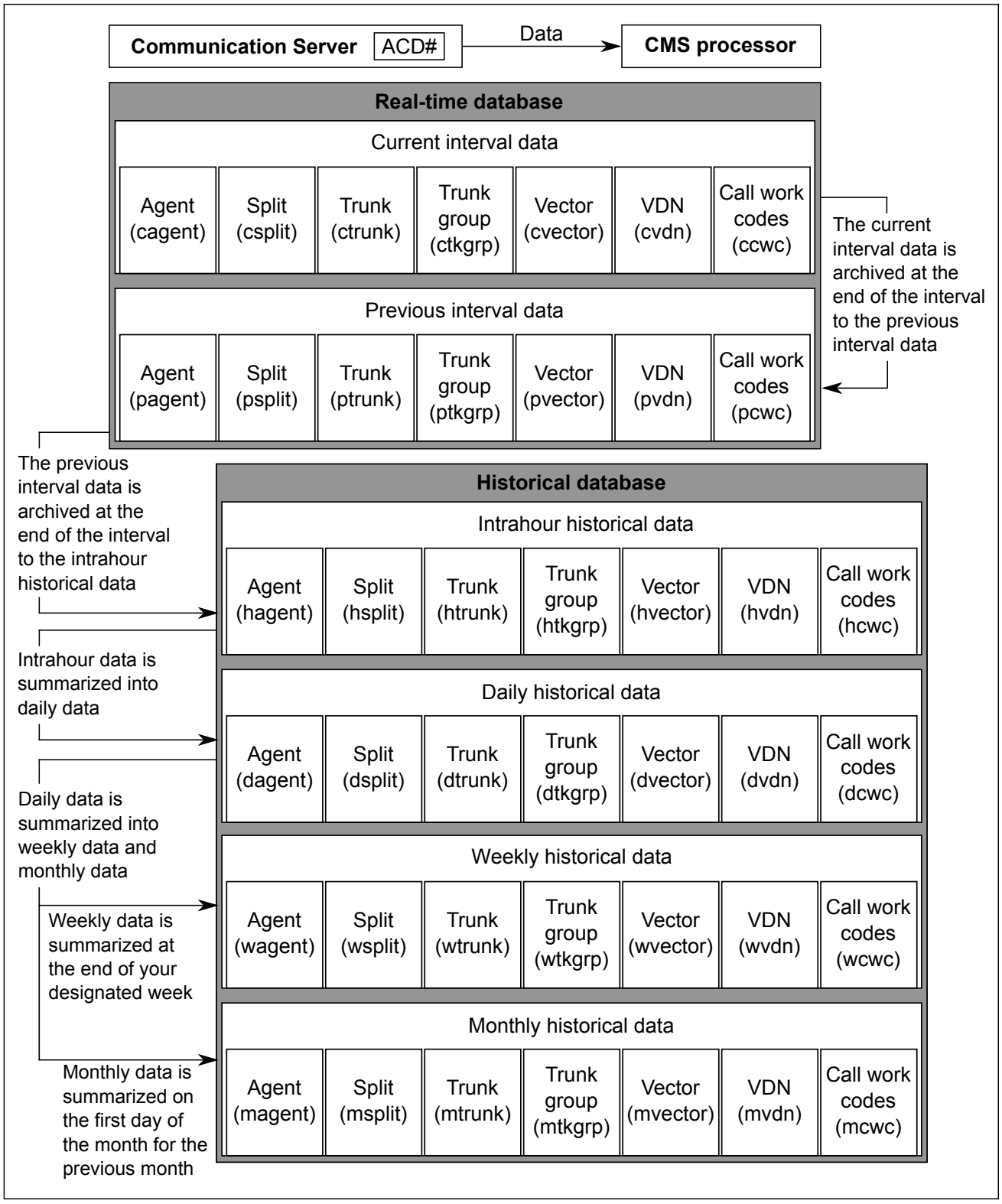
The data remains in the historical database as intrahour historical data for a maximum of 62 days. At your designated data summarizing time, the intrahour historical data is summarized into daily historical data.

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.

For more information, see CMS data storage on page 23.

## CMS data storage

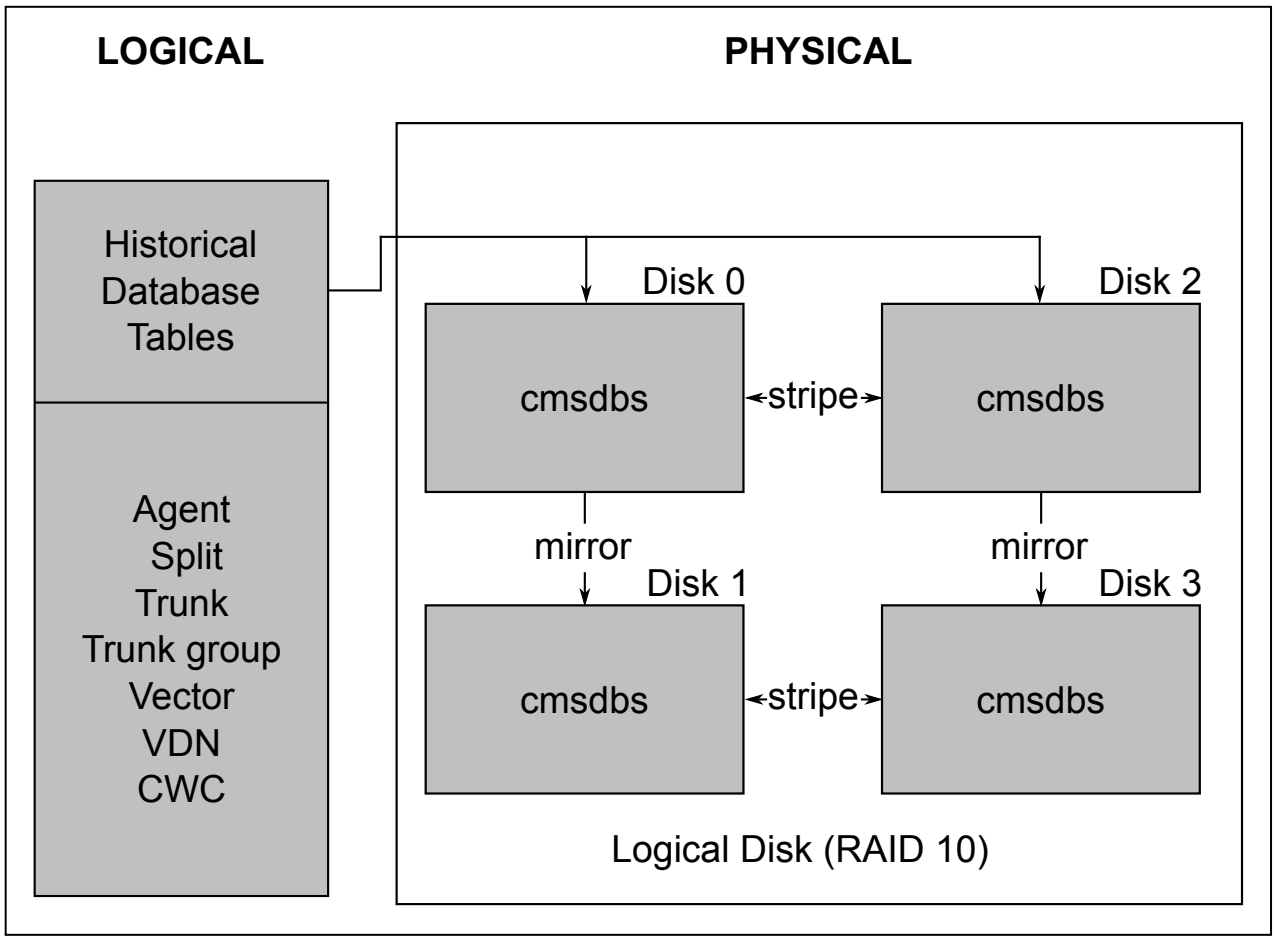
The following figure shows how CMS stores data.


Communication Server
ACD#
Data
CMS processor
Real-time database
Current interval data
Agent (cagent)
Split (csplit)
Trunk (ctrunk)
Trunk group (ctkgrp)
Vector (cvector)
VDN (cvdn)
Call work codes (ccwc)
The current interval data is archived at the end of the interval to the previous interval data
Previous interval data
Agent (pagent)
Split (psplit)
Trunk (ptrunk)
Trunk group (ptkgrp)
Vector (pvector)
VDN (pvdn)
Call work codes (pcwc)
The previous interval data is archived at the end of the interval to the intrahour historical data
Historical database
Intrahour historical data
Agent (hagent)
Split (hsplit)
Trunk (htrunk)
Trunk group (htkgrp)
Vector (hvector)
VDN (hvdn)
Call work codes (hcwc)
Intrahour data is summarized into daily data
Daily historical data
Agent (dagent)
Split (dsplit)
Trunk (dtrunk)
Trunk group (dtkgrp)
Vector (dvector)
VDN (dvdn)
Call work codes (dcwc)
Daily data is summarized into weekly data and monthly data
Weekly historical data
Agent (wagent)
Split (wsplit)
Trunk (wtrunk)
Trunk group (wtkgrp)
Vector (wvector)
VDN (wvdn)
Call work codes (wcwc)
Weekly data is summarized at the end of your designated week
Monthly historical data
Agent (magent)
Split (msplit)
Trunk (mtrunk)
Trunk group (mtkgrp)
Vector (mvector)
VDN (mvdn)
Call work codes (mcwc)
Monthly data is summarized on the first day of the month for the previous month

# How Avaya CMS physically stores ACD data

CMS uses Informix Dynamic Server (IDS) as the relational database. IDS manages the CMS data in specific dbspaces. The historical database can span multiple disks. Hardware RAID spans multiple disks of the CMS system. CMS systems use RAID 10 which stripes the data across multiple disks and also mirrors pairs of the striped disks.

The *cmsdbs* dbspace contains the CMS historical data.




**Note:**

This figure is an example based on a physical disk system consisting of four disks. The CMS system that you actually use can have a different number of total disks. CMS also supports a small Dell R620 system that only has one disk. The small Dell R620 system does not have any striping or mirroring of data on the system.

## Dbspace

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

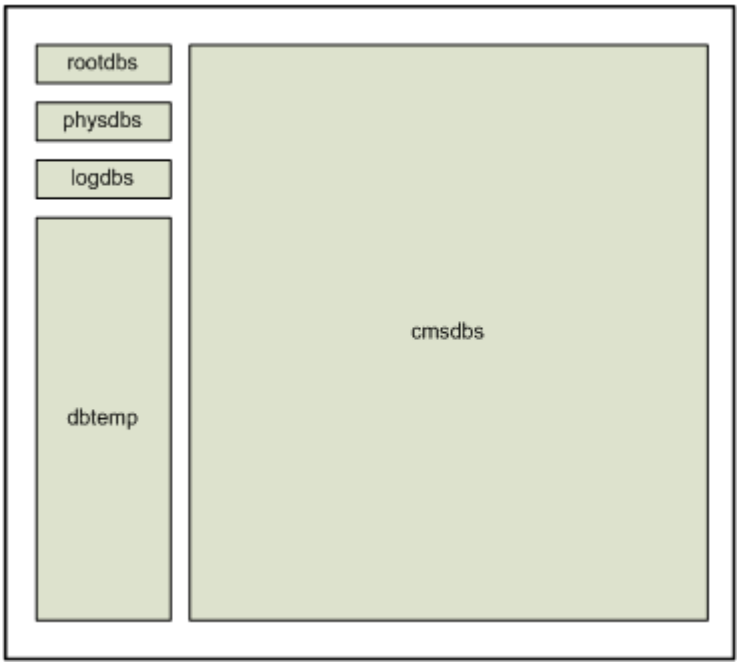
- rootdbs
- physdbs
- logdbs
- dbtemp
- cmsdbs

**Important:**

Do not try to alter rootdbs, physdbs, logdbs, dbtemp, or cmsdbs. Contact CMS services if you think that you have a problem with any of these dbspaces.

## Chunks

A chunk is a unit of physical disk space used to store database data that IDS manages. For CMS, each dbspace 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. Dbspace dbtemp is larger and is used for temporary data space. Dbspace cmsdbs is the location that stores all CMS data and contains the largest chunk of data.



# ACD Administration

CMSprovides an administrative interface to the communication server. From the ACD interface, you can view or change parameters on the communication server related to ACDs, Call Vectoring, and Expert Agent Selection (EAS). An administrator can also run reports that describe your contact center configuration.

For example, an administrator can:

- Add or remove agents from splits or skills
- Move extensions between splits
- Change skill assignments
- Change trunk group-to-split
- Change trunk group-to-VDN
- Change VDN-to-vector assignments
- Start an agent trace
- List the agents that are traced
- Create, copy, and edit call vectors

## How CMS tracks ACD data

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

This section includes the following topics:


- How CMS tracks a call on page 27
- Events that start or stop data collection on page 28

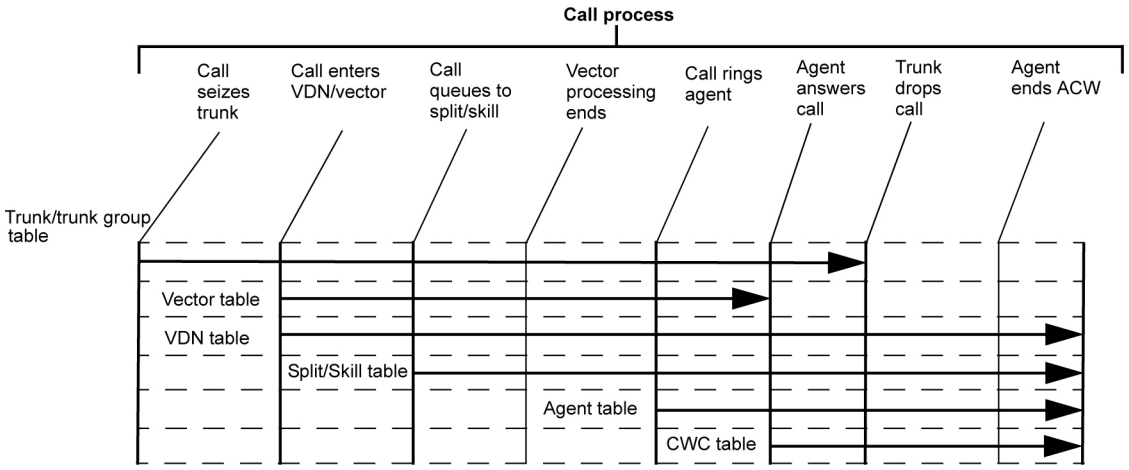

### How CMS tracks a call

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) activity.

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 diagram, the positions of the CMS database tables 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

# About CMS tenancy

## Summary

In CMS R18, the tenancy feature provides an extension to the current CMS user data access management feature to enable customers to restrict user access to CMS reporting data and functionality within their contact center. The new tenant level access for users introduces restricted data access permissions for the following contact center resources: agents, call work codes, split/skills, trunk groups, VDNs, and vectors.

Each tenant partition is assigned contact center resources which will be isolated from resources in the other tenant partitions. A tenant partition can be assigned a subset of contact center resources. All contact center resources do not have to be assigned to a tenant partition.

A user with tenant level access has permissions to access only those CMS resources which are assigned to the tenant partition. A user can be assigned permission to access more than one tenant.

Customers must install the tenancy feature package to use the CMS tenancy feature. Using this feature, customers can partition a subset of the ACD resources and assign the resources to tenants. A tenant or tenant partition enforces restricted access for Supervisor users. Within a tenant, each tenant user can have access to a restricted set of contact center resources and data based on their tenant assignments with that tenant.

The CMS tenancy feature and the Communication Manager tenancy feature are unrelated. All the administrative and tenant user actions for CMS tenancy are carried out independent of Communication Manager tenancy. However, you must perform careful Communication Manager administration to achieve effective CMS tenant partitioning and tenant reporting.

Communication Manager tenant partitioning is administered on the Communication Manager system and CMS tenant partitioning administration does not modify or impact Communication Manager tenant partitioning administration. Tenancy administration on CMS assigns resources such as agents, VDNs, and skills to a CMS tenant and defines how CMS tenant users can access call data that is stored in the CMS database.

CMS does not control the actual call operation or call delivery to agents and skills. Only Communication Manager administration controls how calls are handled and delivered to agents. Therefore, Communication Manager administration impacts data in CMS tenant reports, despite the restrictions imposed by CMS tenant administration.

For example, let the tenant administrator create CMS tenant 1 and assign agent 1 and skill 1 to CMS tenant 1, and create CMS tenant 2 and assign agent 2 and skill 2 to CMS tenant 2. If agent 1 logs into 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.

Thus, while the tenant user is restricted to running reports only for agents assigned to tenant 1, CMS will display all the call data for agent 1. This implies 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 plan tenant administration on both Communication Manager and CMS very carefully prior to any implementation of tenancy.

The resources shared between tenants must be mutually exclusive. Thus, customers cannot assign the same contact center resource to different tenants. This means that different tenants on an ACD cannot share an agent, call work code, split/skill, trunk group, VDN, and vector.

In CMS R18, there are three types of users:

- Administrator: An administrator is a user who has access to all the functions of CMS, all CMS reports, and all CMS data. Administrators can provide admin level access, normal user access, or tenant level access to other users. Administrators have the added capability to create and administer tenant users.
- Normal user: A normal user has functionality similar to the earlier releases of CMS. A normal user is given read, write, and exception permissions by the administrator for ACDs, splits/skills, trunk groups, VDNs, and vectors.
- Tenant user: This user has tenant level access which can span multiple tenant partitions. This user has permissions for viewing or working with CMS resources within the tenant partitions to which the user is assigned.

  **Note:**

  A tenant user is also assigned permission to access the split/skills, trunk groups, VDNs, and vectors within the tenant partition. Thus, additional restrictions within a tenant can be assigned to each individual tenant user.

  **Note:**

  A tenant user can create custom reports or can design reports which are accessible only to the tenant user.

### Examples of Tenancy usage

- Service Providers can use tenancy to partition their ACDs so that CMS can be used by multiple tenants or customers within the same ACD, but without access to each other's data.
- A contact center with multiple departments or business units that have separate independent functions can create tenants to allocate each business unit a different set of tenant partitions.
- Customers that have a hierarchical reporting structure can use tenancy to enable supervisors and report users to manage only a subset of the contact center resources.

**Related links**

Administering tenancy at a high level on page 30

# Administering tenancy at a high level

### About this task

A high level step-by-step description of administering tenancy includes the use of **cmssvc** , **cmsadm**, and the administrative interface.

### Procedure

1. Authorize the tenancy feature using **cmssvc** and install the tenancy feature on the CMS server using the **cmsadm** administrative tool.

   **Note:**

   The customer can perform this step.

2. Log in to the CMS server using CMS Supervisor as a user with administrative permissions and no tenant access restrictions.
3. Add a Tenant to an ACD by going to **Commands** > **Dictionary** and selecting the desired ACD from the list box.
4. Open the Tenants screen to add the tenant number.
5. From Tenant Administration, add associated entities like Agent, Split/Skill, VDN, Trunk, or CWC to a tenant.

   For example, to assign an Agent “agent1” to the tenant “Tenant 1” in ACD “acd1”, use **Tenant Administration** > **Assignments** > **Agent** .
6. Add a tenant user by going to **User Permissions** > **User Data** and selecting **Tenant user**.

   **Note:**

   Upon the creation of a userid, the userid will automatically have read/write permissions for the specified Login ACD on the CMS server. You do not need to use **User Permissions** > **ACD Access** unless the access permissions of the tenant user need to change.
7. Provide the tenant user access to Tenants by using **User Permissions** > **Tenant Access**.
8. Give the tenant user access to the entities assigned to the tenant.

   For example, to assign a Split/Skill belonging to the tenant to a tenant user, use **User Permissions** > **Split/Skill Access** .

   **Note:**

   Permissions for agents and call work codes are inferred from the tenant assignments and cannot be assigned using **User Permissions**.

   **Note:**

   The tenant user can be restricted further for accessing data within a tenant. These restrictions are imposed by the second level of permissions assigned by the administrator for agents, skills, VDNs, vectors, and trunk groups as in earlier CMS releases.

**Related links**

About CMS tenancy on page 29

# Chapter 3: Configuring Avaya CMS Supervisor

## Configuring Avaya CMS Supervisor

This section contains information about configuration of CMS Supervisor 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

This section contains the following topics:


- Before using the Options window on page 32
- Overview of the Controller on page 33
- General tab on page 34
- Scripting tab on page 35
- Report Colors tab on page 36
- Creating a new report color scheme on page 36
- Threshold Colors tab on page 37
- Creating a new threshold color scheme on page 37
- Name Format tab on page 38
- Defining entity formats on page 39


## 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 CMSIf 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. |
| 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:

- **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 Supervisor interface. For example, when you are working in the 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.
- **Use Taskbar Icon**: Select this check box to have 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:

- **User ID**: The login ID for a CMS user.
- **Set User** button: 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:

- **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 36 for instructions on creating report color schemes.
- **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 36 through Step 7 on page 37 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:

- **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 37 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 38 through 6 on page 38 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: Using The Dictionary To Name Contact Center Entities

## Using the Dictionary to name contact center entities

This section provides information on procedures for using the Dictionary to administer names that are associated with contact center entities.

### About the Dictionary

Use the Dictionary subsystem to assign synonyms or names to contact center entities. The following list gives a short sample of the items used in the Dictionary:

- Login IDs
- Splits/skills
- Call work codes
- ACDs
- AUX reason codes
- Logout reason codes
- Trunk groups
- VDNs
- Vectors
- Tenants

The Dictionary also allows users to work with items in the database such as:

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

The names assigned through the Dictionary appear on reports to help users understand them better. The Dictionary also makes it possible for users to create agent groups, change agent splits/

skills, and change trunk string values for reporting purposes. The Dictionary also provides a global search function to find any item within it.

## Before using the Dictionary window

If you select an ACD Group as the current ACD in the Dictionary window, only those operations that are valid for the ACD Group displays in the **Operations** list.

**Note:**

Changes to the dictionary must occur during off hours when there are least database updates. Otherwise, the CMS Supervisor users 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 users are denied access to CMS Supervisor.

## Dictionary rules

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

- Dictionary names can have from 1 to 20 characters.
- Names or synonyms must begin with an alphabetic character.
- Dictionary names can include the following characters:
  - Any alphanumeric character
  - Underscore (_)
  - Blank ( )
  - Comma (,)
  - Period (.)
  - Apostrophe (')
  - Plus sign (+)
- Blanks ( ) are allowed in all Dictionary names *except*:
  - Calculation names
  - 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 split/skill 1 as “sales”, but you cannot name split/skill 1 as “sales” and split/skill 2 as “sales” on the same ACD. Similarly, no two agents can have the same synonyms within the same ACD.
- Fields and entries made in the Dictionary are case-sensitive.

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

- Descriptions in the Dictionary can have from 1 to 50 characters.
- Descriptions can include all printable characters *except*:
  - Semicolon (;)
  - Backward slash (\)
  - Grave accent (`)
  - Tilde (~)
  - Double quotes (")
  - Pipe symbol (|)
  - Asterisk (*)
  - Question mark (?)

# About searching the Dictionary

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

**Note:**

Remember the following before entering the search criteria:

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

## Permissions for searching 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. |
| **In submenu** | The Dictionary submenu that contains your search pattern. |
| **Name** | The name that corresponds to the value matched. |

# ACD Groups in the Dictionary

This section provides information for viewing ACD Groups in the Dictionary. ACD Groups and the corresponding members can only be viewed through the Dictionary Operations window. Administration of ACD Groups is done through the Call Center Administration subsystem. The capability of viewing ACD Groups through the Dictionary subsystem allows those individuals who only run reports in the contact center to view which ACDs are defined within each ACD Group. This capability can assist these individuals in determining which ACD Groups should be used when running reports.

**Note:**

You cannot select ACD Groups to display information through standard CMS reports. To run reports for ACD Groups, you must create custom reports through the CMS ASCII interface. You can also have the reports created for you by contacting the Avaya Professional Services Organization.

## Before using ACD groups

You must read and understand the following before working with ACD Groups in the Dictionary:

- If you add an ACD Group, you must log out of CMS Supervisor. Then, you must log back in to see this group as a choice in the appropriate dialog boxes.
- An ACD Group cannot serve as the CMS master ACD.
- Overlapping ACD Groups, which are groups having common member ACDs, might result in synonym conflict within the members of an ACD Group if poorly administered. Because of this capability, entity IDs in overlapping ACD Groups must be 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 the group's 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.

## Permissions for ACD groups

Depending on the procedure that you want to perform, you need the following permissions:

- To view ACD Group names, you need "read" permissions for the Dictionary subsystem and the ACD Group.

## Listing all ACD Groups

### 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

### 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.

# ACDs

This section provides information on administering ACD names in the Dictionary. You can use the Dictionary Operations window to assign names to real and pseudo ACDs. Generated reports contain the ACDs names, instead of the assigned ACD numbers.

**Note:**

For tenant users, the Dictionary Operations window provides the user with the **Find one** and **List all** options. The tenant user can determine matching entries in the database for the ACD numbers and ACD names entered in the fields of the Dictionary ACDs window.

You can add, delete, or change an ACD name regardless of the ACD that you are logged in to. For example, you can be logged in to ACD 1 and change the name for ACD 3. This change does not appear on the changed window border of the ACD until you open a new window.

**Important:**

The Dictionary naming rules apply to these procedures. See Dictionary rules on page 41 for more information.

## Permissions for ACDs

Depending on the procedure that you want to perform, you need the following permissions:

- To add, delete, or change the name of an ACD, you need “write” permissions for the Dictionary subsystem and for the ACD.
- To view ACD names, you need “read” permissions for the Dictionary subsystem and for the ACD.

## Adding an ACD name

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **ACDs**.
3. Select **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 38 to correspond with the new ACD name where 1 through 8 is reserved for real ACDs, 9 through 26 is reserved for pseudo-ACDs, and 27 through 38 is reserved for ACD Groups.

   You can enter any more information about the ACD in the **Description** field. Only 50 or fewer characters can be entered in this field.

6. To add your changes to the Dictionary, select **Actions** > **Add**.

## Modifying an ACD name

### About this task

To modify the name of an ACD in the Dictionary:

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **ACDs**.

3. Select **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

### 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 name. This procedure should not be performed unless you are certain that you want to delete the ACD name.

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **ACDs**.
3. Select **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.

# Agent groups

This section provides procedures for creating and naming, copying, and deleting agent groups in the Dictionary using the Agent Groups window.

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.

## Permissions for agent groups

Depending on the procedure that you want to perform, you need the following permissions:

- To add, delete, or change agent groups, you need “write” permissions for the Dictionary subsystem.
- To view agent groups, you need “read” permissions for the Dictionary subsystem.
- For more information about considerations on creating agent groups, see Considerations when sizing and reporting on agent groups on page 48.

## Considerations when sizing and reporting on agent groups

When creating agent groups, think about the following sizing and reporting recommendations:

- Limit the size of agent groups to approximately 99 agents. Avoid any agent groups larger than 99 agents because the system performance is adversely affected.

  **Note:**

  The new CMS systems have a customer administrable flag for limiting the historical and real time reporting on agent groups to groups of 99 or less. See Administering Report Properties on page 369 for more information about this topic.

- 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

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD Group on which the agent group exists.
4. Select **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**.

## Listing agents in an agent group

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD Group on which the agent group exists.
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.
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.

## Copying an existing agent group to a new name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD Group on which the agent group exists.
4. Select **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.

## Adding agents to an existing agent group

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD Group on which the agent group exists.
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 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.
8. From the **Actions** menu, select **Add**.

## Deleting agents in an existing agent group

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD Group on which the agent group exists.
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 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.
8. From the **Actions** menu, select **Delete**.

## Deleting an agent group

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Agent Groups**.
3. In the **ACD** field, enter the ACD or ACD Group on which the agent group exists.
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 to delete.
6. From the **Actions** menu, select **Delete**.

   The selected agent group name is removed from the Dictionary.

# Agent string values

Agent string values are the descriptive words in reports that correspond with agent states. These words, such as ACD, ACW, or AUX, describe the value of the data. Strings are changed to the values you administer when these strings are displayed as data in a report. The report heading is not affected.

## Permissions for agent string values

Depending on the procedure that you want to perform, you need the following permissions:

- To change agent string values, you need “write” permissions for the Dictionary subsystem.
- To view agent string values, you need “read” permissions for the Dictionary subsystem.

## Changing agent string value descriptions

### 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.

   CMS Supervisor displays the Dictionary Agent String Values window.
4. Enter a new descriptive word in the field that you want to change.

   See Agent string value field descriptions on page 52 for field descriptions.

# Agent string value field descriptions

| Name | Description |
|---|---|
| **Work Mode** | To change any of the work-mode default names, enter the new descriptive word in the appropriate work mode field. Agents can be in any one of the following work modes:<br>• **ACD**: The agent is on an ACD call.<br>• **ACW**: The agent is in the after-call work mode.<br>• **AUX**: The agent is in the auxiliary work mode.<br>• **AVAIL**: The agent is available to take an ACD call.<br>• **DACD**: The agent is on a direct agent ACD call.<br>• **DACW**: The agent is in the after-call work mode for a direct agent ACD call.<br>• **OTHER**: The agent has just logged in and CMS has not yet been notified of the agent's state, or the agent is dialing for an extension call while in auto-in/manual-in (AI/MI), or the agent is in AI/MI and has an extension call ringing, or the agent has put a call on hold and has taken no further call-related action.<br>• **RINGING**: An ACD call is ringing at the agent's voice terminal and the agent is not doing anything else.<br>• **UNKNOWN**: CMS does not recognize the current state.<br>• **UNSTAFF**: The agent is not logged in, or is not staffed yet. |
| **Agent Trace Work Mode** | To change the agent trace, work-mode default names, enter the new descriptive word next to LOGON or LOGOFF.<br>• **LOGON**: An agent is logged in.<br>• **LOGOFF**: An agent is logged out and is not available to take ACD calls. |
| **Call Handling Preference** | To change the call-handling preference default names, enter the new descriptive word next to LEVEL, NEED, or PERCENT.<br>• **Level**: The agent's call-handling preference is by skill level.<br>• **NEED**: The agent's call-handling preference is by greatest need. |

*Table continues…*

| Name | Description |
|---|---|
| | • **PERCENT**: The agent's call-handling preference is based on an assigned percentage of time allocated to each skill. |
| **Reserve Level** | To change the reserve-level default names, enter the new descriptive word next to Rsv1 or Rsv2.<br>• **Rsv1**: The agent begins answering calls when the skill's first threshold is crossed.<br>• **Rsv2**: The agent begins answering calls when the skill's second threshold is crossed. |
| **Call Direction** | To change the call-direction default names, enter the new descriptive word next to IN or OUT.<br>• **IN**: The agent is on an incoming call.<br>• **OUT**: The agent is on an outbound call. |
| **Call Origination** | To change the call-origination default names, enter the new descriptive word next to PHONE or KEYBOARD. Agents can be on either type of the following outbound calls:<br>• **PHONE**: The agent dialed an outbound call using the voice terminal dial pad.<br>• **KEYBOARD**: The agent dialed an outbound call using the computer keyboard. |
| **Call Destination** | To change the call-destination default names, enter the new descriptive word next to PBX or OFF.<br>• **PBX**: Internal to the switch.<br>• **OFF**: External to the switch. |
| **Agent Role** | To change the agent role default names, enter the new descriptive word next to **TOP**, **ALLOCATED**, **BACKUP**, **ROVING**, or **RESERVE**.<br>• **TOP**: The agent can be counted on to answer the skill's calls, unless an agent's other skills go into overload.<br>• **ALLOCATED**: The agent has time allocated to answering the skill's calls.<br>• **BACKUP**: The agent helps answer the skill's calls when his/her top skill is not busy.<br>• **ROVING**: The agent answers a skill's calls when this skill has the greatest need.<br>• **RESERVE**: The agent helps answer the skill's calls when the skill is over threshold. These roles vary according to call-handling preference. |
| **Interrupt Type** | To change the interrupt type default names, enter the new descriptive word next to **NA**, **AUTO-IN**, **MANUAL-IN**, **NOTIFY**.<br>• **NA**: Not interruptible when the agent is in AUX.<br>• **AUTO-IN**: Auto in interrupt.<br>• **MANUAL-IN**: Manual in interrupt. |

*Table continues…*

| Name | Description |
|---|---|
| | • **NOTIFY**: Agent is notified of the interrupt and can choose whether to accept of reject the interrupt. |
| **Interrupt Status** | To change the interrupt status default names, enter the new descriptive word next to **NA**, **NOTIFYING**, **INTRRPTED**, **INTRRPTBLE**.<br>• **NA**: The agent is not in the interruptible AUX state.<br>• **NOTIFYING**: The agent is being notified of an interrupt while in the interruptible AUX state.<br>• **INTRRPTED**: The agent is interrupted in the interruptible AUX state and is handling a call.<br>• **INTRRPTBLE**: The agent is in the interruptible AUX state. |

# Announcements

This section provides information on working with announcement names in the Dictionary. Announcements are recorded messages that are played for callers. Announcement names are synonyms assigned to these recorded messages in the Dictionary.

## Permissions for announcement names

Depending on the procedure that you want to perform, you need the following permissions:

- To view announcement names, you need “read” permissions for the Dictionary subsystem.
- To add, delete, or change announcement names, you need “write” permissions for the Dictionary subsystem.

## Before using announcement names

Read and understand the following items before working with announcement names in the Dictionary:

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

## Adding an announcement name

### Procedure

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

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Select **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**.

## Viewing an announcement name

### Procedure

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

   Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.

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

   Supervisor displays the Dictionary Announcements window.
5. From the **Actions** menu, select **List all**.

## Modifying an announcement name

### Procedure

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

   Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Select **OK**.

   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

### Procedure

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

   Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Announcements**.
3. In the **ACD** field, enter the ACD on which the announcement resides.
4. Select **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**.

# AUX reason code names

This section provides information on working with AUX reason code names in the Dictionary. AUX reason codes help a contact center to track an agent's time more precisely when the agent is in the AUX work mode. The agent can specify exactly why the AUX state is used, such as for lunch or meetings. You can view, add, delete, or change AUX reason code names by selecting **AUX Reason Codes** from the **Dictionary** menu.

Complete the AUX Reason Codes window if you want the names that are associated with your AUX reason codes to appear in the AUX Reasons Code standard real-time and historical reports.

## Permissions for AUX reason code names

Depending on the procedure that you want to perform, you need the following permissions:

- To view AUX reason codes, you need “read” permissions for the Dictionary subsystem.
- To add, delete, or change AUX reason codes, you need “write” permissions for the Dictionary subsystem.

## Before using AUX reason code names

Read and understand the following items before working with AUX reason code names in the Dictionary:

- To use AUX reason codes, your switch must have EAS.
- AUX reason codes are digits 0 through 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 this 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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations**list, highlight **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which the AUX Reason Codes reside.
4. Select **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 the one-digit AUX reason code number from 0 to 9.

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

## Viewing an AUX reason code name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations**list, highlight **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which the AUX Reason Codes reside.
4. Select **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 the one-digit AUX reason code number from 0 to 9.
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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations**list, highlight **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which the AUX Reason Codes reside.
4. Select **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.

## Modifying an AUX reason code name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations**list, highlight **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which the AUX Reason Codes reside.
4. Select **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 the one-digit AUX reason code number from 0 to 9.
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

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **AUX Reason Codes**.
3. In the **ACD** field, enter the ACD or ACD Group on which the AUX Reason Codes reside.
4. Select **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 the one-digit AUX reason code number from 0 to 9.
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.

# Calculations

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

## Permissions for calculations

Depending on the procedure that you want to perform, you need the following permissions:

- To view calculations, you need “read” permissions for the Dictionary subsystem.
- To create, delete or change a custom calculation, you need “write” permissions for the Dictionary subsystem.

# Before using calculations

Read and understand the following items before changing calculations in the Dictionary:

- Calculations must be one word with no blanks.
- Reports do not run if you embed calculations more than three levels deep.
- You cannot delete standard calculations.

  The standard CMS calculations are listed in the following documents:

  - *Avaya Call Management System Database Items and Calculations*
  - *Avaya CMS Supervisor Report Designer User Guide*
  - *Avaya CMS Supervisor Reports*
  - *Avaya Call Management System Custom Reports*
- Avaya recommends that you identify your own calculations in all lowercase letters to distinguish those calculations from the standard CMS Supervisor calculations. The standard calculations are in all uppercase letters.
- If you delete a custom calculation from the Dictionary, any reports that the calculation appeared in does not run.
- You can adversely affect standard reports if you change a standard CMS Supervisor calculation. Reports might probably run, but the results might be different from your expectation.
- 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 in processing, this creates a circular pattern where the processing cannot be completed.

# Viewing a calculation

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Calculations**.
3. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Calculations**.
3. Select **OK**.

   CMS Supervisor displays the Dictionary Calculations window.
4. From the **Actions** menu, select **List all**.

## Adding a calculation

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Calculations**.
3. Select **OK**.

   CMS Supervisor displays the Dictionary Calculations window.
4. Enter the name of the calculation in the **Calculation name** field.

   **Important:**

   Use lowercase letters in the name to distinguish this custom calculations from a standard CMS calculation.
5. In the **Calculations** field, enter the formula for the calculation.

   Formulas can include:

   - Database items
   - Constants
   - Calculations. The maximum nesting level is 3.
   - The following arithmetic operators:
     - + (add)
     - (subtract)

- * (multiply)
- / (divide)
- ( ) (do first, as in standard mathematical operations)

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

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

   The custom calculation is added to the Dictionary.

# Modifying a custom calculation

## About this task

**Important:**

Avaya does not recommend modifying a standard CMS calculation. . If you change a standard CMS calculation, the meaning of that calculation changes in every report in which the calculation displays.

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Calculations**.
3. Select **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.

   Enter any changes to the descriptive information in the **Description** field.
7. From the **Actions** menu, select **Modify**.

# Deleting a custom calculation

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Calculations**.
3. Select **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**.

   CMS Supervisor retrieves and displays the information for the specified calculation, if valid.
6. From the **Actions** menu, select **Delete**.

   The specified calculation is removed from the Dictionary.

# Call work codes

Call work codes are numeric sequences that agents enter to categorize the call that the agents have received or are handling. By entering call work codes, agents can assign one of many defined categories to the calls which can be later viewed in detail through reports. The call work codes are defined in the Dictionary and can represent any type of call that are tracked. These calls include complaints, special sales, and promotional events, . You can assign up to five call work codes to each call. You can view, add, delete, or change call work codes and the names from the Call Work Codes window. These names then appear in the standard Call Work Code historical report.

## Permissions for call work codes

Depending on the procedure that you want to perform, you need the following permissions:

- To view call work code names, you need “read” permissions for the Dictionary subsystem.
- To add, delete or change call work code names, you need “write” permissions for the Dictionary subsystem.

## Before using call work codes

Read and understand the following items before changing call work codes in the Dictionary:

- Call work codes must be activated on the ACD before the administration and naming of the codes can be performed.
- Call work codes require storage space on the CMS file system. You must configure the number of call work codes available on a system through the Data Storage Allocation window. See Chapter 11: Configuring CMS system settings on page 270 for more information.
- **Call Work Code 0** is reserved for unadministered work codes so that summary data can be collected. The default name for **Call Work Code 0** is **Unadministered codes**, but this name can be changed.
- Even if 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 wish to add/delete/modify.

## Adding a name to a call work code

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Select **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.

## Viewing a call work code name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Select **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

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. In the **ACD** field, enter the ACD on which the call work codes reside.
4. Select **OK**.

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

# Modifying a call work code name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Select **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 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 for the 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

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Call Work Codes**.
3. In the **ACD** field, enter the ACD on which the call work code resides.
4. Select **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.

# Constants

Constants are items with fixed numeric values that you can enter into the Dictionary for use only in custom and designer reports. Constants do not exist in CMS whenCMS is installed.

## Permissions for constants

Depending on the procedure that you want to perform, you need the following permissions:

- To view a constant, you need “read” permissions for the Dictionary subsystem.
- To add, delete or change a constant, you need “write” permissions for the Dictionary subsystem.

# Adding a constant

## Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Constants**.
3. Select **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**.

# Viewing a constant

## Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations**list, highlight **Constants**.
3. Select **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

## Procedure

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

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Constants**.
3. Select **OK**.

   CMS Supervisor displays the Dictionary Constants window.
4. From the **Actions** menu, select **List all**.

## Modifying a constant

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Constants**.
3. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Constants**.
3. Select **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.

# Custom database items

You can define your own custom database items, which are stored in the CMS database. You can enter the custom database items from the Dictionary Custom Items window. These items allow you to combine your own data with the CMS data on custom or designer reports. You can also change or delete custom database items.

## Permissions for custom database items

Depending on the procedure that you want to perform, you need the following permissions:

- To view a custom database item, you need “read” permissions for the Dictionary subsystem.
- To add, delete, or change a custom database item, you need “write” permissions for the Dictionary subsystem.

## Before using custom database items

Read and understand the following items before working with custom database items in the Dictionary:

- You must first create the table in the database before you create a custom database item.

## Adding a custom database item

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Custom Items**.

3. Select **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**.

# Viewing a custom database item

## About this task

To view a custom database item in the Dictionary:

## Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Custom Items**.
3. Select **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

## Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Custom Items**.
3. Select **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**.

# Modifying a custom database item

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** ist, highlight **Custom Items**.
3. Select **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

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Custom Items**.
3. Select **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 values synonyms

Changing 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 appear in custom or designer reports that use the YES or NO synonyms.

## Permissions for Generic string values synonyms

Depending on the procedure that you want to perform, you need the following permissions:

- To view generic string values, you need “read” permissions for the Dictionary subsystem.
- To change generic string values, you need “write” permissions for the Dictionary subsystem.

## Viewing generic string values

### Procedure

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

   CMS Supervisor displays the Dictionary window.
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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
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 displays in reports that use YES and NO fields.

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

# Location IDs

Location IDs represent the location or site where an agent sits 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 the synonyms are used for both agents and trunks.

## Permissions for location ids

Depending on the procedure that you want to perform, you need the following permissions:

- To view the name of a location ID, you need “read” permissions for the Dictionary subsystem.
- To add, delete, or change the name of a location ID, you need “write” permissions for the Dictionary subsystem.

## Adding a location ID

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Location ID**.
3. In the**ACD** field, enter the ACD on which you want to add the location ID.
4. Select **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 to 44 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**.

## Viewing a location ID

### Procedure

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

CMS Supervisor displays the Dictionary window.

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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Location IDs**.
3. In the **ACD** field, enter the ACD on which the location IDs reside.
4. Select **OK**.

   CMS Supervisor displays the Dictionary Location IDs window.
5. From the **Actions** menu, select **List all**.

## Modifying a location ID

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Location IDs**.
3. In the **ACD** field, enter the ACD on which the location ID resides.
4. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Location IDs**.
3. In the **ACD** field, enter the ACD on which the location ID resides.
4. Select **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.

# Login ID names

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

You do not have to include agent names in the Dictionary, but CMS administration windows and reports are easier to understand with agent names instead of login IDs. Depending on the amount of space in the report, agent names can be truncated.

## Permissions for login IDs

Depending on the procedure that you want to perform, you need the following permissions:

- To view login IDs, you need “read” permissions for the Dictionary subsystem.
- To add, delete, or change login IDs, you need “write” permissions for the Dictionary subsystem.

## Before using login ID names

The following items should be read and understood before working with login ID names in the Dictionary:

- Login ID names are sorted alphabetically in the Dictionary based on the first character that you input in the **Agent Name** field. For example, if the agent is listed as “Jane Brown”, CMS sorts on the “J” for Jane. If the agent is listed as “Brown, Jane” sorts on the “B” in Brown. CMS Supervisor reports do not automatically sort by agent name, but the user can request the report to do so.
- You can assign no more than one agent name to the same login ID.
- You cannot assign the same agent name to multiple login IDs.
- You can use only numbers in login IDs.
- If you are viewing a real-time report when a change is made to a login ID that appears on that report, you must exit the report and rerun it to see the change.
- Tenant users must have permissions for the agent LOGID which they want to add/delete/modify.

## Adding a name to a login ID

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **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. Select **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**.

## Viewing a login ID name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations**list, highlight **Login Identification**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to view a login ID name.
4. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Login Identification**.
3. In the **ACD** field, enter the ACD or ACD Group in which you want to list all login ID names.
4. Select **OK**.

   CMS Supervisor displays the Dictionary Login Identifications window.
5. From the **Actions** menu, select **List all**.

# Modifying a login ID name

## Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Login Identification**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to modify a login ID name.
4. Select **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

## Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Login Identification**.
3. In the **ACD** field, enter the ACD or ACD Group in which the login ID name to delete resides.
4. Select **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**.

# Logout reason code names

An agent can use Logout reason codes to give the reason for logging out, such as attending training or the end of a shift. You can add, delete, change, and view logout reason codes from the Logout Reason Codes window. The names that you assign to the logout reason codes are displayed in the standard agent login/logout and agent trace historical reports.

## Permissions for logout reason code names

Depending on the procedure that you want to perform, you need the following permissions:

- To view logout reason codes, you need “read” permissions for the Dictionary subsystem.
- To add, delete, or change logout reason code, you need “write” permissions for the Dictionary subsystem.

## Before using logout reason code names

- Logout reason codes are single digits from 0 to 9. A zero is used when the system logs an agent out or if the agent does not specify a code.
- Logout reason code names can be up to 20 characters long.
- To use logout reason codes, your switch must have the Expert Agent Selection (EAS) feature.

## Adding a logout reason code name

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **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. Select **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**.

## Viewing a logout reason code name

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **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. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **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. Select **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.

## Modifying a logout reason code name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **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. Select **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

### Procedure

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

   Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **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. Select **OK**.

   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.

# Split/skill string values

Split/skill string values are the descriptive words used in the split/skill call profile reports instead of the split/skill numeric values. From the Split/Skill String Values window, you can change the default string values to correspond to your own requirements.

## Permissions for split/skill string values

Depending on the procedure that you want to perform, you need the following permissions:

- To view split/skill string values, you need “read” permissions for the Dictionary subsystem.
- To change split/skill string values, you need “write” permissions for the Dictionary subsystem.

## Before using split/skill string values

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

## Viewing split/skill string values

### 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

### 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 modify the split/skill string values.
4. Select **OK**.

   CMS Supervisor displays the Dictionary Split/Skill String Values window.
5. Enter a new split/skill string value in each field that you want to modify.

   See Split/skill string value field descriptions on page 84 for more information.
6. From the **Actions** menu, select **Modify**.

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

## Split/skill string value field descriptions

The following table describes the fields in the Dictionary Split/Skill String Values window.

| Name | Description |
|---|---|
| **Service Level Changed** | The service level is the time limit in seconds for calls to wait in queue before being answered. The Split/Skill Call Profile reports can be used to see how many calls were either answered or abandoned within each service level increment.<br><br>The string values in the following fields are displayed on the Split/Skill Call Profile Report:<br><br>• **YES**: The string value in this field displays on the Split/Skill Call Profile Report if the service level in the split/skill call profile has changed.<br><br>• **NO**: The string value in this field displays on the Split/Skill Call Profile Report if the service level in the split/skill call profile has not changed. |

*Table continues…*

| Name | Description |
|---|---|
| **Period Changed** | There are ten time increments of administrable length in the real-time and historical Split/Skill Call Profile Reports.<br><br>The string values in the following fields are displayed on the Split/Skill Call Profile Report:<br><br>• **YES**: The string value in this field displays on the Split/Skill Call Profile if the time in the split/skill call profile has changed.<br><br>• **NO**: The string value in this field displays on the Split/Skill Call Profile if the time in the split/skill call profile has not changed. |
| **Skill State** | Skill states are used to specify states for the different skills.<br><br>The string values in the following fields represent the following skill states:<br><br>• **UNKNOWN**: Leave the default value. The default value is UNKN.<br><br>• **Normal**: Enter the 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.<br><br>• **Overload1**: Enter the 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.<br><br>• **Overload2**: Enter the 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.<br><br>• **BEHIND**: This string indicates that a split or skill is either close to or failing to meet the administered target service level, and agents are not being autoreserved to compensate for this situation. The default value for this string is BEHIND.<br><br>• **AUTORSV**: This string indicates that a split or skill is either close to or failing to meet the administered target service level, and agents are being autoreserved to achieve the necessary level. The default value for this string is AUTORSV. |

# Split/Skill names

You can assign names to your ACD splits or skills. These split/skill names appear on the split/skill reports, making your reports easier to identify and read.

Split/skill names should reflect the configuration of your splits/skills and ACDs.

For example, if you want splits in your system to be divided according to Sales, Customer Service, and Wholesale, assign those names to the splits that handle those areas of the business. If you want skills in your system to be divided by language such as French, Spanish, and German, assign those names to the skills that handle calls in those languages.

## Permissions for split/skill names

Depending on the procedure that you want to perform, you need the following permissions:

- To view the name assigned to a split/skill, you need “read” permissions for the Dictionary subsystem and for the split/skill.
- To add, delete or modify the name assigned to a split/skill, you need “write” permissions for the Dictionary subsystem and for the split/skill.

## Before using split/skill names

The following items should be read and understood before working with split/skill names in the Dictionary:

- It is advised that you be consistent with the names given by your switch administrator.
- If you assign a name, the split/skill number no longer appears in split/skill reports or windows. The split/skill name appears instead.
- If you make changes to split/skill names when viewing a report that includes those splits/skills, you must exit the report and rerun it to see the changes.

## Adding a split/skill name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Splits/Skills**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to name a split/skill.
4. Select **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**.

## Viewing a split/skill name

### Procedure

1. From theController window, select **Commands** > **Dictionary**.

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Splits/Skills**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to view a split/skill.
4. Select **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 the split/skill names

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Splits/Skills**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to view all split/skill names.
4. Select **ACD**.

   CMS Supervisor displays the Dictionary Split/Skill String Values window.
5. From the **Actions** menu, select **List all**.

## Modifying a split/skill name

### Procedure

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

   CMS Supervisor displays the Dictionary window.

2. In the**Operations** list, highlight **Splits/Skills**.
3. In the **ACD** field, enter the ACD or ACD Group on which you want to modify the split/skill name.
4. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Splits/Skills**.
3. In the **ACD** field, enter the ACD or ACD Group on which the split/skill name to delete resides.
4. Select **OK**.

   CMS Supervisor displays the Dictionary Split/Skill String Values 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.

# Standard database items

Standard database items store ACD data and are used by CMS in its default reports.

You cannot change or delete standard database items because this is a read-only section of the Dictionary. You can view the standard information about each database item, the description for that item, and the tables in which the item appears.

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.

# Permissions for standard database items

To view the standard database items, you need "read" permissions for the Dictionary subsystem.

# Viewing a standard database item

## 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 database items alphabetically

### 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**.

# Tenant names

The Tenants window is used to assign tenant names, numbers, and description. The tenant names appear in reports making the reports easier to understand.

## Permissions for tenant names

Depending on the procedure that you want to perform, you need the following permissions:

- To view the name that is assigned to a tenant, you need read permissions for the Dictionary subsystem and for the tenant partition
- Tenant users cannot add, delete, or modify tenant names.

## Before using tenant names

You must install the tenancy feature package first. The administrator must already have planned out the division of the following resources on the given ACD: trunk groups, splits/skills, agent logids, Call work codes, and VDNs.

## Adding a tenant name

### 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**.

## Viewing a tenant name

### 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

### 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**.

## Modifying a tenant name

### 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

### 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 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.

# Trunk group names

The Trunk Groups window is used to assign names to ACD trunk groups. The trunk groups names appear in reports making the reports easier to understand.

## Permissions for trunk group names

Depending on the procedure that you want to perform, you need the following permissions:

- To view the name that is assigned to a trunk group, you need “read” permissions for the Dictionary subsystem and for the trunk group.
- To add, delete, or modify the name assigned to a trunk group, you need “write” permissions for the Dictionary subsystem and for the trunk group.

## Before using trunk group names

The following items should be read and understood before working with trunk groups names in the Dictionary:

- When naming trunk groups, you may want to be consistent with the names given to trunk groups and splits/skills by your switch administrator.
- If you assign a trunk group name, the name is displayed on trunk group reports or windows 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 rerun it to see the changes.

# Adding a trunk group name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to name a trunk group.
4. Select **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**.

# Viewing a trunk group name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to view a trunk group name.
4. Select **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

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to list all trunk group names.
4. Select **OK**.

   CMS Supervisor displays the Dictionary Trunk Groups window.
5. From the **Actions** menu, select **List all**.

# Modifying a trunk group name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Trunk Groups**.
3. In the **ACD** field, enter the ACD on which you want to modify a trunk group name.
4. Select **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

## 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. Select **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.

# Trunk string values

Trunk string values are the descriptive words such as IDLE, HOLD, or QUEUED on trunk reports. These words are displayed in the data fields of the report. They are not displayed as headings. From the Trunk String Values window, the default values can be changed to any values that meet the needs of your contact center. If you do not assign different trunk string values, the default values are used. Any changes that you make to the trunk string values affect what you see in the corresponding fields on trunk reports.

## Permissions for trunk string values

Depending on the procedure that you want to perform, you need the following permissions:

- To view the trunk string values, you need “read” permissions for the Dictionary subsystem.
- To modify a trunk string value, you need “write” permissions for the Dictionary subsystem.

## Viewing and modifying trunk string values

### Procedure

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

   CMS Supervisor retrieves and displays the information for the specified trunk group, if valid.
2. In the **Operations** list, highlight **Trunk String Values**.
3. Select **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 that is next to the name that you want to change.

   See Trunk string values field descriptions on page 97 for more information on the fields in the Dictionary Trunk String Values window.

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

## Trunk string values field descriptions

The following table describes the trunk string value fields.

| Name | Description |
|---|---|
| **Trunk State** | To change any of the trunk state default names, enter the new descriptive word next to any of the following:<br>• **IDLE** - The trunk is waiting for a call.<br>• **SEIZED** - A call is holding the trunk, either incoming or outgoing.<br>• **QUEUED** - An ACD call has seized the trunk, is queued to a split/skill, and is waiting for an agent to become available.<br>• **CONN** - The caller and an agent are connected on a call.<br>• **DABN** - The caller has abandoned the call.<br>• **FBUSY** - The caller receives a forced busy signal.<br>• **FDISC** - The caller receives a forced disconnect.<br>• **HOLD** - The agent has put the caller on hold.<br>• **MBUSY** - The trunk is out of service for maintenance purposes.<br>• **RINGING** - The call is ringing at an agent's voice terminal.<br>• **UNKNOWN** - CMS does not recognize the trunk state. |
| **Queue Type** | To change the queue type default names, enter the 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).<br>• **MAIN** - The call is queued to a split/skill as a result of a `queue to main split/skill` vector command.<br>• **BACKUP** - The call is queued to a split/skill as a result of a vector command other than `queue to main split/skill`. |
| **Call Priority (Non-Vectoring)** | To change the call priority (non-vectoring) default names, enter the 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.)<br>• **YES** - The call occupying the trunk has priority entering the trunk. |

*Table continues…*

| Name | Description |
|---|---|
| | • **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 the 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 `queue to split/skill` or `check split/skill` 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).<br>• **LOW** - The call occupying the trunk is queued to a split or skill at the lowest priority level.<br>• **MED** - The call occupying the trunk is queued to a split or skill at the second lowest priority level.<br>• **HIGH** - The call occupying the trunk is queued to a split or skill at the second highest priority level.<br>• **TOP** - The call occupying the trunk is queued to a split or skill at the highest priority level. |
| **Call Direction** | To change the call-direction default names, enter the new descriptive word next to **IN** or **OUT**.<br>• **IN** - The trunk is on an incoming call.<br>• **OUT** - The trunk is on an outbound call. |
| **All Trunks Busy** | To change the all trunks busy default names, enter the new descriptive word next to **YES** or **NO**.<br>• **YES** - All trunks in the trunk group are busy (in use or maintenance).<br>• **NO** - Not all trunks in the trunk group are busy. |

# VDN names

From the VDNs window, you can assign names to VDNs so that names instead of numbers appear on VDN reports and VDN administration windows. VDN names should reflect the configuration of your ACD and convey one or more of the following:

- The VDN's purpose; 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.

## Permissions for VDN names

Depending on the procedure that you want to perform, you need the following permissions:

- To view the name that is assigned to a VDN, you need “read” permissions for the Dictionary subsystem and for the VDN.
- To add, delete, or modify the name that is assigned to a VDN, you need “write” permissions for the Dictionary subsystem and for the VDN.

## Before using VDN names

The following items should be read and understood before working with VDN names in the Dictionary:

- The VDNs window is available only if the Call Vectoring feature is installed and activated on your switch.
- VDNs must be created on the switch and assigned for measurement via CMS.
- To get a list of VDNs that can be named, run the vector configuration report. While all VDNs can be named, it is recommended that only those VDNs that are used are then named instead of all of the VDNs. This will conserve system resources.
- If you make changes to the VDN names when a report that includes those VDNs is running, you must exit the report and rerun it to see the changes.
- When naming VDNs, you may want to be consistent with the names given to VDNs by your switch administrator.
- If a name is assigned to a VDN, it will appear on VDN reports and windows instead of the VDN number.

## Adding a VDN name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **VDNs**.
3. In the **ACD** field, enter the ACD on which you want to name a VDN.
4. Select **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**.

## Viewing a VDN name

### Procedure

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

   CMS Supervisor displays the Dictionary window.

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

   Supervisor displays the Dictionary VDNs window.

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

# Modifying a VDN name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **VDNs**.
3. In the **ACD** field, enter the ACD on which you want to modify the name of a VDN.
4. Select **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

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **VDNs**.
3. In the **ACD** field, enter the ACD on which the VDN to delete resides.
4. Select **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.

# Vector names

From the Vectors window, you can assign names to vectors so that the names instead of the vector numbers are displayed on vector reports and administration windows. Vector names should 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; for example, vdn2001, vdn3001, and vdn4001.
- The splits or skills to which the vector sends calls; for example, sales1, sales2, AUDIX system.

## Permissions for vector names

Depending on the procedure that you want to perform, you need the following permissions:

- To view the name that is assigned to a vector, you need “read” permissions for the Dictionary subsystem and for the vector.
- To add, delete, or modify the name that is assigned to a vector, you need “write” permissions for the Dictionary subsystem and for the vector.

## Before using vector names

The following items should be read and understood before working with vector names in the Dictionary:

- The Vectors window is available only if the Call Vectoring feature is installed and activated on the 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 a name is assigned to a vector, it appears on reports and windows instead of the vector number.
- If you make changes to vector names when a report that includes those vectors is running, you must exit the report and rerun it to see the changes.

# Adding a vector name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to name a vector.
4. Select **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**.

# Viewing a vector name

## Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to view a vector name.
4. Select **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

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to list all vector names.
4. Select **OK**.

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

# Modifying a vector name

### Procedure

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

   CMS Supervisor displays the Dictionary window.
2. In the **Operations** list, highlight **Vectors**.
3. In the **ACD** field, enter the ACD on which you want to modify a vector name.
4. Select **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

### Procedure

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

CMS Supervisor displays the Dictionary window.

2. In the **Operations** list, highlight **Vectors**.
3. In the **ACD** field, enter the ACD on which the vector name to delete resides.
4. Select **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 VDN is removed from the Dictionary.

# Dictionary reports

In the Dictionary window, 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 are not available to tenant users. Tenant users are unable to see these reports in the user interface.

## Permissions for 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 or skills using the Dictionary Splits/Skills Operation input window. When you assign a split or 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 or 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 or 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**

   To send the report to a printer other than the default printer in the report window, select **Print Report** 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**

7. Select **OK**.

   Depending on the option that you selected, the report is either sent to a printer or displayed on the screen.

# Chapter 5: Using Reports

## Background

This section describes CMS Supervisor reports and provides procedures in generating and administering them. The procedures are general in scope so as to provide usability for all reports run through the Reports subsystem. For more information on specific reports and usage, see the *Avaya CMS Supervisor Installation and Getting Started* and *Avaya CMS Supervisor Reports* manuals.

CMS collects data from ACD activity and stores it in one of the CMS databases. The data reflects the activity of your contact center and can be viewed through CMS reports that cover such areas as:

- Splits/Skills
- Trunks
- Trunk Groups
- Agents
- Agent Groups
- VDNs
- Vectors

This section contains the following topics:


- About reports on page 110
- The Reports subsystem on page 111
- Generating a report on page 112
- Printing a report on page 113
- Printing a Historical report on page 113
- Changing the print setup on page 114
- Restarting a report on page 114

# About reports

Reports consist of standard reports, custom reports, and designer reports. Standard reports are shipped as part of the CMS system. Custom reports are created by contact center administrators through the CMS ASCII interface. Designer Reports are created through CMS Supervisor .

See the *Avaya Call Management System Custom Reports* and *Avaya CMS Supervisor Report Designer* manuals for more information on creating custom and designer reports.

**Note:**

- In CMS R18, administrators can administer additional time zones for daily, weekly, and monthly archiving. One additional time zone is allowed for an entire ACD and one additional time zone is allowed per tenant partition within the ACD.
- Time zone selection can be applied for interval, daily, weekly, and monthly reporting.
- Customers can select time zones for exception reporting.
- By dividing an ACD into multiple tenant partitions using the multi-tenancy support in CMS R18, customers can associate a specific time zone to a tenant partition instead of the entire ACD.

## Interfaces for reports

The following list displays which interfaces are used in the creation of reports and which ones can be used for viewing these reports:

- In CMS R18, real-time, historical, and integrated reports can be viewed using CMS Supervisor web.
- Most standard reports can also be viewed through the CMS ASCII interface. The exceptions to this are the CMS Supervisor integrated reports, reports containing charts, and others.
- Custom reports are created through the CMS ASCII interface, but can be viewed through both the CMS ASCII interface and CMS Supervisor.
- Designer reports can only be created and viewed through CMS Supervisor.

## Types of reports

The following types of reports can be generated:

- Standard real-time
- Standard historical
- Standard integrated
- Custom (CMS) real-time
- Custom (CMS) historical

- Designer (CMS Supervisor) real-time
- Designer (CMS Supervisor) historical
- Designer (CMS Supervisor) integrated
- Exceptions
- Forecast (available as an add-on feature, only CMS)

## What reports summarize

Use CMS Supervisor reports to summarize the status of:

- Any measured subset of the ACD, including agents, splits/skills, trunks/trunk groups, VDNs, vectors, call work codes, and call records
- Agent administration
- Contact center administration
- Dictionary
- Exceptions
- Maintenance

# The Reports subsystem

Most reports are found in the Reports subsystem found under the **Commands** item on the menu bar. This section provides the general procedure for running reports in this subsystem. Reports may be run by selecting the **Real-Time**, **Historical**, or **Integrated** tab from the Select a Report window.

Other reports are available on the Reports tab found on the main window of the following subsystems:

- Dictionary
- Exceptions
- Agent Administration
- Call Center Administration
- Maintenance

The reports for the subsystems listed above are not available in the main Reports interface.

Procedures on running reports through the areas other than the Reports subsystem are covered in their respective sections. The following procedures provide information on working with reports from the Reports subsystem.

# Choosing a report

## Procedure

1. Select **Commands** > **Reports** from the Controller window.

   CMS Supervisor displays the Select a Report window.

2. Determine the type of report to be run by select the appropriate tab: **Real-Time**, **Historical**, or **Integrated**.
3. From the **Run Report for ACD** field, select the ACD to serve as the data source for the report.
4. Select a category from the **Category** field.
5. Select a report from the **Report** field.
6. For historical interval, daily, weekly, and monthly reports, select a time zone from the Time Zone field.

   You can select from a series of available time zones. The value “default” denotes the time zone of the ACD.

   **Note:**

   For daily, weekly and monthly reports, the user does not receive data in a report for all the available time zones displayed in the drop-down menu for the time zone field. The user only sees data in the report for the time zone that the user has set up with the Data Summarization Time Zone screen.

7. Select **OK**.

   CMS Supervisor displays a report input window. The input fields vary according to the report and its type.

   To continue this process, see the following section, Generating a report on page 112.

# Generating a report

## About this task

Once a report type has been selected by following the previous procedure, information must be entered to define the parameters of the report.

## Procedure

1. To specify an object for the report, such as an agent, vector, VDN, and so forth, perform one of the following actions:
   - Manually enter the name or number of the object for the report.
   - Select the **Browse** button to view available objects.
   - Select the **History** list to select an input used previously.

2. Select **OK** to run the report with the specified object.

   The type of report selected is displayed with information related to the object that was specified.

   **Note:**

   In the new CMS systems, a timer value, administrable by the customer, has been introduced for limiting the time the historical database spends on a report query. See section Administering Report Properties on page 369 for more information on this topic.

# Printing a report

## About this task

Once a report has been generated, a Real-Time or Integrated report can be printed.

## Procedure

1. Select **Reports** > **Print** from the menu bar of the report window.

   Windows displays the Print window .

2. Select the printer and options for this report:
   - Select the printer destination by selecting a printer in the **Name** drop-down list box.
   - Select the number of copies of this report to be printed in the **Print to file** field.
   - Use the **Properties** button to change options specific to the selected printer. This could include image resolution, orientation, and other options.

3. Select **OK**.

   The report is printed based on the options selected.

   To print a report to a file on the local system, place a check mark in the **Print to file** check box. Set the printer to **Generic/Text Printer**. Failing to select the **Generic/Text Printer** will cause the **Print to file** check box to be ignored and the report is sent to the selected printer.

# Printing a Historical report

## About this task

Once a report has been generated, a Historical report can be printed.

## Procedure

Follow the steps listed in Generating a report on page 112 and Printing a report on page 113.

When specifying an object, such as an agent, vector, VDN, and so forth, for a report, the **Destination** group of controls can be seen on the lower half of the dialog box. This allows the report to be viewed on the screen or sent to the printer specified. Selecting the printer button in this area

allows specification of a different printer as well as setting all printer and print job options. This button is not available on Real-time and Integrated reports.

## Changing the print setup

### About this task

Once a report has been printed to the screen, the settings for margins, page numbering, and table borders can be altered.

### Procedure

1. Select **Reports** > **Page Setup** from the report window menu bar.

   CMS displays the Page Setup dialog box.

2. Select the settings for page margins, page numbers, and table borders, as needed.
3. Select **OK** to save these settings.

   The new settings will be applied to the next report that is printed.

## Restarting a report

### About this task

**Important:**

Work-state drill-down reports cannot be restarted.

### Procedure

1. Select **Restart** from the **Reports** menu.

   The report window closes and the input window that is used to specify the object of the report is displayed again.

2. Enter the requested information in the input window and select **OK**.

   CMS displays the report window with the newly updated information for the selected object.

## Restarting a report in CMS Supervisor Web

### Procedure

Use one of the following procedures to restart a report in CMS Supervisor Web:

- Click **Set Input**, change the input values, and restart the report.
- Reload the page running the report to restart the report by reusing the inputs from the previous session. Otherwise, the report prompts you for inputs again.

# Chapter 6: Scripting CMS Operations

## Scripting CMS operations

Scripting enables the automation of tasks such as running reports, exporting report data, and other operations.

## 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.
- 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 379.

## 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 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 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 117.

# 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 118 |
| **Logging Level** | The extent to which script-related activities and outputs are logged, according to the following criteria:<br>• **Minimum** - Logged activities are limited to those errors and messages from CMS Supervisor which would otherwise be displayed when the scripts are run manually.<br>• **Normal** - Logged activities include those recorded at the **Minimum** setting, plus the following information: task start time; task end time; name of the script.<br>• **Maximum** - Logged activities include all those recorded at **Minimum** and **Normal** settings, plus additional error messages which may be useful for debugging a script. |
| **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.

# 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.

   See The Reports subsystem on page 111 for this procedure.

   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.

   For more information, see The Reports subsystem on page 111.

   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 other Supervisor operations

This section provides information on the procedures used to create and save scripts for actions not associated with reports.

## Actions not associated with reports

Actions not associated with reports 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.

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 2:**

| 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 Replacewindow. | The file already exists. | Select one of the following actions at the bottom of the window:<br>• **Add** (default) - Adds the new script to the end of the existing script<br>• **Replace** - Deletes the existing script and create a new script file<br>• **Cancel** - Closes the Add or Replace window and returns to the Save as Script twindow<br>• **Help** - Displays the help topic for the current window. |

# Chapter 7: Administering Contact Center Agents

## Administering contact center agents

This section provides information on using the Agent Administration window.

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. These procedures include instructions for administering agents in an Automatic Call Distribution (ACD) with and without the Expert Agent Selection (EAS) feature.

## About starting or stopping an agent trace

This section provides the procedure for starting and stopping the tracing of agents. Tracing an agent records the activities of the agent, state changes, and time when these events occurred. The agent trace report displays this information when it is run. The agent trace report can help you to evaluate how well agents use their time.

### Before starting or stopping an agent trace

The following items should be read and understood before working with agent traces:

- Traces can be activated for a limited number of agents across all ACDs from one CMS server. This limit depends on the platform model. You can find this limit in *Avaya Call Management System Overview and Specification*.
- The maximum number of agent trace records that can be stored is documented in *Avaya Aura® Communication Manager System Capacities Table*. The oldest record is discarded and overwritten by the newest record when the file reaches the allocated maximum number of records.
- Turning a trace off 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 record. See Data Storage Allocation on page 274 for more information on this window.

- Starting and stopping agent traces requires that the Data Collection feature is currently activated.
- An agent trace must be started before the Agent Trace report can be run.
- Scripts can open and use the Agent Activate Trace window. You can also schedule the script. See Chapter 6: Scripting CMS operations on page 115, for more information on scripting.
- The Agent Activate Trace window can be set on a timetable. See Chapter 14: Using timetables and shortcuts on page 377, for more information.

## Permissions for starting or stopping an agent trace

Depending on the procedure that you want to perform, you need the following permissions:

- To start or stop an agent trace, the user ID used to log in to this Supervisor session requires “write” permission for the Agent Administration subsystem.
- To view an agent trace report, the user ID used to log in to this Supervisor session requires “read” permission for the Reports subsystem.

## Starting or stopping an agent trace

### Procedure

1. From the Controller window, select **Commands** > **Agent Administration**.

   Supervisor displays the Agent Administration window.

   On Communication Manager systems with EAS:

   On Communication Manager systems without EAS:

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.

# Viewing current agent trace states

### About this task

This section provides the procedure for viewing all agent traces that are set to either **On** or **OFF**.

### Procedure

1. From the Controller Window, select **Commands** > **Agent Administration**.

   Supervisor displays the Agent Administration window.

   On Communication Manager systems with EAS:

   On Communication Manager systems without EAS:

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** - Displays all disabled agent traces.
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.

# About listing agents traced

This section provides the procedure for listing agents and dates for which agent trace data is available on reports. As with most operations, it is possible to run these operations through scripts and timetables.

## Before listing agents traced

To view data through this operation, an agent trace must be activated for one or more agents. Also, agents for whom traces are activated must log in so that CMS creates agent trace records.

## Permissions for listing agents traced

Depending on the procedure that you want to perform, you need the following permissions:

- To list all agents traced, the user ID used to start this Supervisor session must have “write” permission for the Agent Administration subsystem.

# Listing agents traced

## Procedure

1. From the Controller window, select **Commands** > **Agent Administration**.

   CMS Supervisor displays the Agent Administration window.

2. In the **Operations** list, highlight **List Agents Traced**.
3. In the **ACD** field, select the ACD for which agents being traced will be listed.
4. Select **OK**.

   **Note:**

   The procedure for viewing agent trace records varies according to the information that you enter in the fields of the List Agents Traced window. 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.

   CMS Supervisor displays the List Agents Traced window.

5. Use the following descriptions to determine how information is entered in the **Agents** and **Date** fields:

   - Use the **Agents** field to specify none, one, or more agents to use in displaying agent trace records.

     Leave this field blank to show all agent trace records for the dates entered in the **Date** field.

     Only those agents with login IDs in the Dictionary can be entered in the **Agents** field.

     This field can accept multiple values. Multiple values must be separated by a semicolon (;).

   - Use the **Date** field to specify no date, a single date, multiple dates, or a range of dates.

     Leave this field blank to show all agent trace records for the agents entered in the **Agents** field.

     This field can accept multiple dates or a range of dates. Multiple dates must be separated by a semicolon (;).

   Leave both the **Agents** and **Date** fields blank to have 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.

   Supervisor displays a secondary window listing the dates and agents for which agent trace data is available, sorted by date.

# About changing agent skills

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

## Before changing agent skills

The following items should be read and understood before changing agent skills:

- The **Change Agent Skills** item is only available for ACDs on which EAS is activated.
- When agent skills are changed, the change is made to the Communication Manager system and remains in effect until another change is made through Supervisor or the Communication Manager system itself.
- When agent skills are changed, you cannot exit the Change Agent Skills window until the ACD responds to the requested agent changes.
- A template can be any existing agent profile where the skill settings of the profile are applied to other agent profiles. You can specify multiple agents individually and by using ranges. Entries must be separated with semicolons. You are limited to 250 characters in this field. After you apply the skill settings, all of the agents specified will have the same skills, levels, interrupt types and percents as the agent profile being used as a template. It is assumed you have the same level of permissions for all agents specified in the change.
- Skill 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. Because of this, agents who frequently have calls on hold may have skill changes remain pending for a longer time than expected.
- Changing agent skills should only be done through Supervisor as it checks if the agent has the appropriate permissions for the newly assigned skills. The CMS ASCII interface does not perform permission checking which can result in agents belonging to skills to which the Supervisor does not have permissions.

## Permissions for changing agent skills

Depending on the procedure that you want to perform, you need the following permissions:

- If you are a tenant user and the tenancy feature is enabled, you need permissions to modify the agent and the agent skills belonging to the tenant to which you are assigned.
- To view agent skill assignments, the user ID used to log in to this Supervisor session requires “read” permission for the Agent Administration subsystem.
- To change agent skills, the user ID used to log in to this Supervisor session requires “write” permission for the Agent Administration subsystem.

## Changing agent 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 **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.

| If... | Then... |
|---|---|
| You want to change which calls an agent receives first | Select a different method in the **Call Handling Preference** group box. Calls can be distributed to the selected agent based on:<br>• **Skill Level**<br>• **Greatest Need**<br>• **Percent Allocation**<br>The **Skill Level** for the agent is shown in the **Assigned Skills** list. **Percent Allocation** is only available if Avaya Business Advocate is enabled on the Communication Manager system. |
| You want to change the skill that is used to queue an agent's direct agent calls | Perform one of the following actions:<br>• Select a new skill from the **Direct Agent Calls** drop-down list.<br>• 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.<br>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. |
| You want to change the level/ type that is associated with skill that is already assigned | Perform the following procedure:<br>a. In the **Assigned Skills** list, select the level of the skill for which you want to change the value. Note that if you have a Skill Level Call Handling Preference, an arrow indicates the agent's Top Skill assignment.<br>b. Select a new value for the skill level from the **Level** drop-down list in the **Agent Skills and Skill Levels** group.<br>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.<br>c. Select **OK**. |
| You want to change the interrupt type associated with skill that is already assigned for Communication Manager version 6.0 and up | Perform the following procedure:<br>a. In the **Assigned Skills** list, select the interrupt type of the skill for which you want to change the value.<br>b. Select a new value for the interrupt type from the interrupt type drop-down list in the **Agent Skills and Skill Levels** group.<br>c. Select **OK**. |

*Table continues…*

| If... | Then... |
|---|---|
| You want to remove skills that are assigned to this agent or template | Perform the following procedure:<br>a. In the **Assigned Skills** field, select the skills to remove from the agent.<br>b. Select the **Delete Skills** button.<br>Note that if an agent has only one assigned skill, this skill cannot be deleted. |
| You want to add skills to this agent or template | Select the **Add Skills** button. 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. When you are finished adding skills, select the **OK** button in the Add Agent Skills window. |
| You have Avaya Business Advocate and want to specify a new percent allocation | Perform the following procedure:<br>a. In the **Call Handling Preference** group, select **Percent Allocation**.<br>Note that the **Percent Allocation** field is unavailable if a reserve level has already been specified for an agent or template.<br>b. Select the **YES** button from the warning window. This indicates that you want to enable the Percent Allocation feature.<br>If an agent or template has **Percent Allocation** call handling preference, the total percent allocation for all standard skills must equal 100%.<br>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. |
| You want to make an **Direct Agent Calls First** the **Top Skill** for this agent | Perform the following procedure:<br>a. 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.<br>b. Select the **Make Top Skill** button. |
| You want to apply the changes to multiple agents | Perform the following procedure:<br>a. Select the **Use for one or more Agents** check box.<br>b. 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.<br>c. Select **OK**.<br>Changes are submitted to the CMS server. If a move is pending, you are notified that the operation will not occur until |

*Table continues…*

| If... | Then... |
|---|---|
| | 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.<br><br>If an error in 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.<br><br>d. Select **OK**.<br><br>If the change is successfully made, Supervisor displays a successful message in the status bar.<br><br>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.<br><br>e. Select **OK**.<br><br>Supervisor closes the Change Agent Skills window. |
| You are finished making changes | Perform one of the following actions:<br><br>• Select **OK** in the Select Agent/Template window. This action saves the changes that you made to the agent skills.<br><br>• Select **Cancel** in the Select Agent/Template window. This action cancels any changes that you made. |
| You want to make skill assignment changes for other agents or templates | Perform the following actions:<br><br>a. Select another agent or template in the Select Agent/Template window.<br><br>b. Return to Step 5 on page 130 and continue with the procedure. |

# Change agent skills in CMS Supervisor Web

Use this administrative procedure to change, add, or delete agent skills for a single agent in CMS Supervisor Web. These features are only available to users with Feature Access Agent Administration read permission. You can modify agent skill assignments only if you have Feature Access Agent Administration write permission.

**Related links**

Changing agent skills on page 134
Adding agent skills on page 134
Deleting agent skills on page 135

# Changing agent skills

### About this task

Use this task to change skills of agents. You can only modify the **Level** and **Interruptible AUX** fields if you have write permissions for the skill. Tenant users must have write permission for the agent.

### Before you begin

Ensure that you select an active ACD. If the ACD link is inactive, you cannot modify the agent skills.

### Procedure

1. Select the ACD for which you want to change the agent skills.
2. In **Agent**, enter an agent name or ID and select the agent.

   The **Agent** drop-down list is limited to a fixed number of results and provides additional choices when you enter the agent name or ID.
3. In **Call Handling Preference**, click one of the following:
   - **Skill Level**
   - **Greatest Need**
   - **Percent Allocation**
4. In the Agent Skills window, click the item that you want to change and select the required values for **Level** and **Interruptible AUX**.
5. In the **Select additional agents** field, do the following:
   a. Type the agent name or ID, or a range of IDs to populate Search Results. Separate multiple names, IDs, or ranges using semicolons.
   b. Add the agents from Search Results to Selected Agents.

   This step is an optional step to select additional agents.

   The default maximum number of agents that you can add to Selected Agents is 99.
6. Click **Apply**.

   The system displays the result of this action.

### Related links

Change agent skills in CMS Supervisor Web on page 133

# Adding agent skills

### About this task

Use this task to add agent skills. You can only modify the **Level** and **Interruptible AUX** fields if you have write permissions for the skill. Tenant users must have write permission for the agent.

### Before you begin

Ensure that you select an active ACD. If the ACD link is inactive, you cannot modify agent skills.

### Procedure

1. Select the ACD for which you want to add the agent skills.
2. In **Agent**, enter an agent name or ID and select the agent.

   The **Agent** drop-down list is limited to a fixed number of results and provides additional choices when you enter the agent name or ID.
3. Click the add icon available in the Agent Skills window.

   The Add Skill window displays.
4. Select values for the following and click **OK**:
   - **Skill**
   - **Level**
   - **Interruptible AUX**

   The **Skill** drop-down list is limited to a fixed number of results and provides additional choices when you type the name or ID.
5. In the **Select additional agents** field, do the following:
   a. Type the agent name or ID, or a range of IDs to populate Search Results. Separate multiple names, IDs, or ranges using semicolons.
   b. (Optional) Add the agents from Search Results to Selected Agents.

   The maximum number of agents that you can add to Selected Agents is 99.
6. Click **Apply**.

   The system displays the result of this action.

**Related links**

Change agent skills in CMS Supervisor Web on page 133

## Deleting agent skills

### About this task

Use this task to delete agent skills. You can only remove skills if you have write permission for the skill. Tenant users must have write permission for the agent.

### Before you begin

Ensure that you select an active ACD. If the ACD link is inactive, you cannot modify agent skills.

### Procedure

1. Select the ACD for which you want to delete the agent skills.

2. In **Agent**, enter an agent name or ID and select the agent.

   The **Agent** drop-down list is limited to a fixed number of results and provides additional choices when you enter the agent name or ID.

3. Locate the entry for the skill in the Agent Skills window.
4. Click the remove icon next to the selected entry to delete the agent skill.

   The direct agent skill cannot be removed. If an agent is assigned only one skill, the skill cannot be removed.

5. In the **Select additional agents** field, do the following:

   a. Type the agent name or ID, or a range of IDs to populate Search Results. Separate multiple names, IDs, or ranges using semicolons.

   b. (Optional) Add the agents from Search Results to Selected Agents.

   .

   The maximum number of agents that you can add to Selected Agents is 99.

6. Click **Apply**.

   The system displays the result of this action.

**Related links**

Change agent skills in CMS Supervisor Web on page 133

# About changing skills for multiple agents

This section provides the procedure for changing skills for more than one agent 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 the skills.

## Before changing skills for multiple agents

The following items should be read and understood before beginning work with the Multi-Agent Skill Change window:

- When agent skills are changed, the change is made to the Communication Manager system and remains in effect until another change is made through Supervisor or the Communication Manager system.
- You cannot exit from the Multi-Agent Skill Change window until the Communication Manager system responds to the requested changes.
- Skill 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, skill changes can remain pending for a longer time than expected.

## Permissions for changing skills for multiple agents

Depending on the procedure that you want to perform, you need the following permissions:

- To view agent skill assignments, the user ID used to log in to this Supervisor session requires “read” permission for the Agent Administration subsystem.
- To change agent skills, the user ID used to log in to this Supervisor session requires “write” permission for the Agent Administration subsystem and for the skills to which agents are assigned.

## Changing skills for multiple agents

### 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 agent skills.
3. In the **Operations** list, highlight the **Multi-Agent Skill Change** item.
4. Select **OK**.

   Supervisor displays the Multi-Agent Skill Change window.
5. 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.

   Clicking the left mouse button on the column headings sorts the contents between ascending and descending order.

   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 the 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 on the agent at the beginning of the range, holding down the `Shift` key, and then clicking the agent at the bottom of the range.

Use the drag-and-drop method to move the agents from the window for their current skill to a new skill in the Skill List window.

Another way of moving agents from one skill to another is to open a window for the new, target skill by double-clicking that skill in the Skill List window. You can then drag-and-drop agents between the two skill windows.

Note that holding down the `Ctrl` key while dragging and dropping agents will add, not move, the agent or agents to the new skill.

Supervisor displays the Move Agents Between Skills window with the **Agents** field showing the following:

- The agents you moved
- The call-handling preferences of the agents
- The reserve level or skill level of each agent
- The service objective of each agent
- The percent allocation for the skill of each agent. Percent allocation is only available on Communication Manager systems with Avaya Business Advocate.
- The interrupt type for the skill of each agent. Interrupt type is only available on Communication Manager Version 6.0 and up.

The **Move** group displays information showing the skills involved in moving this agent. 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.

7. In the Move Agents Between Skills window, perform one of the following actions to complete 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.
   - For Communication Manager Version 6.0 and up, select the interrupt type for the new skill for the selected agents.
8. Select **OK**.

   If one or more agent moves fail, Supervisor displays a status window showing the reasons for failure. Otherwise, the status window notifies you that the change is pending.

# Multi-Agent skill change in CMS Supervisor Web

Use this administrative procedure to add, move, or delete skills for multiple agents in CMS Supervisor Web . This feature is only available to users with Feature Access Agent Administration write permission.

**Related links**

Adding skills for multiple agents on page 139
Moving skills for multiple agents on page 139
Deleting skills for multiple agents on page 140

# Adding skills for multiple agents

### Before you begin

Ensure that you select an active ACD. If the ACD link is inactive, you cannot modify agent skills.

### Procedure

1. In **Operation**, click **Add**.
2. Select the ACD for which you want to add skills for multiple agents.
3. Select values to assign to multiple agents by using the drop-down list for **Skill**, **Level**, and **Interruptible AUX**.

   The drop-down list for **Skill** is limited to a fixed number of results. You must type the name or ID to display additional results.
4. In the **Agents** field, type the agent name or ID, or a range of IDs to populate Search Results. Separate multiple names, IDs, or ranges using semicolons.
5. Add the agents from Search Results to Selected Agents.

   The maximum number of agents that you can add to Selected Agents is 32.
6. Click **Apply**.

   The system displays the result of this action.

**Related links**

Multi-Agent skill change in CMS Supervisor Web on page 138

# Moving skills for multiple agents

### Before you begin

Ensure that you select an active ACD. If the ACD link is inactive, you cannot modify agent skills.

### Procedure

1. In **Operation**, click **Move**.
2. Select the ACD for which you want to move skills for multiple agents.
3. Click the drop-down list for **From Skill** to select the skill that you want to move.

   The drop-down list is limited to a fixed number of results. Type the name or ID to display additional results.

4. Use the drop-down list for **To Skill**, **Level**, and **Interruptible AUX** to select the new skill values to assign to multiple agents.

   The drop-down list for **To Skill** is limited to a fixed number of results. Type the name or ID to display additional results .

5. In the **Agents** field, type the agent name or ID, or a range of IDs to populate Search Results. Separate multiple names, IDs, or ranges using semicolons.
6. Add the agents from Search Results to Selected Agents.
7. Click **Apply**.

   The system displays the result of this action.

**Related links**

Multi-Agent skill change in CMS Supervisor Web on page 138

# Deleting skills for multiple agents

### Before you begin

Ensure that you select an active ACD. If the ACD link is inactive, you cannot modify agent skills.

### Procedure

1. In **Operation**, click **Delete**.
2. Select the ACD for which you want to delete skills for multiple agents.
3. Use the drop-down list for **Skill** to select the skill to delete for multiple agents.

   The drop-down list is limited to a fixed number of results. Enter the name or ID to display additional results.

4. In the **Agents** field, type the agent name or ID, or a range of IDs to populate Search Results. Separate multiple names, IDs, or ranges using semicolons.
5. Add the agents from Search Results to Selected Agents.
6. Click **Apply**.

   The system displays the result of this action.

**Related links**

Multi-Agent skill change in CMS Supervisor Web on page 138

# 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 for changing 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 About moving extensions between splits on page 142 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 141. |
| 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.

# About moving 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 for moving 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.

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 for running 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**.
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 8: Administering The Contact Center

## Administering the contact center

This section provides the procedures to perform operations to configure the contact center.

Depending on the type of Communication Manager system and the features that are enabled on it, the items on the **Call Center Administration** menu will vary.

## Before administering the contact center

If an ACD Group is selected as the current ACD in the Dictionary window, only those operations that are valid for the ACD Group will appear in the **Operations** list.

## ACD Groups

An ACD Group is an administrator-assigned collection of ACDs.

### Before using ACD groups

The following items should be read and understood before you work with ACD Groups

#### Availability

- If you add an ACD Group, you will need to log out of Supervisor and log back in to see this group as a choice in the appropriate dialogs.

#### Capacities/Performance

- A maximum of 12 ACD Groups can exist on an Avaya CMS server.
- Each ACD Group can contain zero to eight ACDs.
- CMS must be in single-user mode in order to add or delete 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 created, ACD Groups will be assigned an ACD ID number from 27 through 38. This number is automatically assigned by CMS and cannot be altered.

- ACD Groups will not disallow an ACD being added as a member based on its version or feature set.
- 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.
- Names must begin with an alphabetic character and can be up to 20 characters long. Valid characters are alphanumerical (a-z, A-Z, 0-9), underscore (_), blank ( ), comma (,), period (.), single quote ('), and plus (+). Multiple values are not allowed.

### Synonyms

- Overlapping ACD Groups (groups having common member ACDs), could result in synonym conflict within the members of an ACD Group if poorly administered. Because of this capability, entity IDs in overlapping ACD Groups must be mutually exclusive.
- Entity synonyms must be unique for an ACD Group and across all of the ACDs that are members of the ACD Group.

### 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 was created on a CMS server where the Global Dictionary feature was authorized, the data can only be restored on a CMS server that also has this feature authorized. If the Global Dictionary feature 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.

## ACD Group capabilities

This optional feature provides the following capabilities:

- Easy administration of synonyms in the Dictionary across multiple ACDs. A synonym assigned to a CMS entity for 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 of “Sales”, this synonym is assigned to skill 102 for all ACDs within that group. This feature should be utilized when a contact center uses multiple ACDs that require the same synonyms across all of the ACDs 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
- The reporting of data from multiple ACDs through the use of custom reports. Reports for ACD Groups collect, aggregate, and display contact 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 or ordered through the Avaya Professional Services Organization. For example, the reporting aspect of this feature can be used to view data for a CMS entity across multiple ACDs such as a skill, a specific agent login ID, and so forth.

## ACD Groups feature interfaces

The ACD Groups feature is available through two interfaces:

- Call Center Administration - This subsystem is used for administrators to create, modify, and delete ACD Groups.
- Dictionary - This subsystem is used by CMS users who need to view ACD Groups, their contents, and to assign ACD Group synonyms.

## Permissions for ACD groups

- To create, modify, and delete ACD Groups, a CMS user must have the “read” and “write” permissions for the Call Center Administration subsystem.
- If a CMS user only requires the ability to view ACD Groups and the member ACDs, “read” permission is required for the Dictionary subsystem.
- To assign synonyms to an ACD group, a CMS user requires the “read” and “write” permissions for the Dictionary subsystem as well as the ACD Group and its member ACDs.

## Adding an ACD Group

### About this task

This topic provides the procedure for creating an ACD Group. After an ACD Group is created, member ACDs can then be added. See Adding an ACD to an ACD Group on page 149 for more information.

### Before you begin

Before performing this procedure, you should ensure that you have read and understood Before using ACD groups on page 146.

### Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.

   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.

## Listing all ACD Groups

### 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.

### Procedure

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

   Supervisor displays the Call Center Administration window.

2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.

   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.

## Adding an ACD to an ACD Group

### About this task

This topic provides the procedure for adding an ACD as a member of an existing ACD Group. This procedure can only be performed after an ACD Group has been created. See Adding an ACD Group on page 148 for more information.

### Before you begin

Before performing this procedure, you should ensure that you have read and understood Before using ACD groups on page 146.

### Procedure

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

   Supervisor displays the Call Center Administration window.

2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.

   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 on page 150.
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.

## Viewing the contents of an ACD Group

### 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 ACD Groups in the Dictionary on page 43.

### Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.

   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 all ACD Groups on page 149 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.

## Deleting an ACD from an ACD Group

### About this task

This topic provides the procedure for removing an ACD from an ACD Group.

### Before you begin

Before performing this procedure, you should ensure that you have read and understood Before using ACD groups on page 146.

### Procedure

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

   Supervisor displays the Call Center Administration window.

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

3. Select **OK**.

   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 all ACD Groups on page 149.

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 on page 150.

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 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.

## Modifying an ACD Group

### About this task

This topic provides the procedure for modifying the name of an existing ACD Group.

### Procedure

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

   Supervisor displays the Call Center Administration window.

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

3. Select **OK**.

   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 all ACD Groups on page 149.

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 Before using ACD groups on page 146 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 Group

### About this task

This topic provides the procedure for deleting an existing ACD Group.

### Before you begin

Before performing this procedure, you should ensure that you have read and understood Before using ACD groups on page 146.

### Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **ACD Groups**.
3. Select **OK**.

   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 all ACD Groups on page 149.
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 codes

A call work code is a number that represents a particular call type or activity to track in the contact center, for example, promotional ads, complaints, or repeat orders. Agents use the dial pad on their voice terminal to enter call work codes. This information is sent to CMS for management reporting and can then be viewed in the call work code and call record historical reports.

**Note:**

Some telephony applications that are used on PCs require that digits be entered through the software interface instead of the dial pad on the voice terminal.

## Before using call work codes

The following items should be read and understood before beginning to work with call work codes:

- Call work codes must be positive integers with 1 to 16 digits. Names can be assigned in the Dictionary to call work codes that consist of nine digits or less. It is recommended that a fixed number of digits be used consistently for all call work codes. The use of a consistent number of digits makes 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 before they can be used. 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 274 for more information.
- Daily, weekly, and monthly standard historical reports are available for call work codes. Call work codes also appear on the standard historical call record report. See the *Avaya CMS Supervisor Reports* document for more information.
- For standard call work code reports, the codes are assigned in the Call Work Codes window.
- To have a name refer to a call work code in a report instead of its numerical code, the name must first be assigned in the Dictionary.

## Permissions for call work codes

Depending on the procedure to be performed, the following permissions are needed:

- To view call work codes, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem.
- To add or delete call work codes, the user ID used to log in to this Supervisor session requires “read” and “write” permission for the Call Center Administration subsystem.

## Adding call work codes

### About this task

This section provides the procedure for adding a call work code for use in a contact center.

### Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. Select **OK**.

   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.

# Viewing call work codes

## About this task

This section provides the procedure for viewing an existing call work code.

## Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. Select **OK**.

   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

## About this task

This section provides the procedure for listing all existing call work codes.

## Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. Select **OK**.

   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.

## Deleting call work codes

### About this task

This section provides the procedure for deleting a call work code from the CMS database.

### Procedure

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

   Supervisor displays the Call Center Administration window.
2. In the **Operations** list, highlight **Call Work Codes**.
3. Select **OK**.

   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.

# VDN skill preferences

A Vector Directory Number (VDN) is an extension number that enables calls to connect to a vector for processing. A VDN is not assigned an equipment location, but is assigned to a vector. 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, by itself, may be dialed to access the vector from any extension that is connected to the switch.

Calls use VDN skills for routing based on the preferences that are assigned. The skill preferences are used in the assigned vector as 1st, 2nd, and 3rd.

This section describes the procedures to change the first, second, and third skill preferences assigned to a VDN. You can also list the currently assigned skill preferences for VDNs as well as list all the VDNs that currently have skill preferences assigned to them.

## Before using VDN skill preferences

The following items should be read and understood before working with VDN skill preferences:

- You can only work with VDN skill preferences on a Communication Manager system and the Expert Agent Selection (EAS) feature is present and activated.
- When VDN skill preferences are changed through Supervisor, the change takes place immediately on the Communication Manager system. This can affect the processing of calls at the time of the change.
- If the changes to VDN skill preferences should occur at a specific time, they can be run through scripts that can then be scheduled through a third-party scheduling application.

## Permissions for VDN skill preferences

Depending on the procedure that you want to perform, you need the following permissions:

- To view current VDN skill preferences, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem and the affected VDNs.
- To change VDN skill preferences, the user ID used to log in to this Supervisor session requires “write” permission for the Call Center Administration subsystem and the affected VDNs.

## Changing VDN skill preferences

### About this task

This section provides the procedure for changing skill preferences for a VDN. This feature is only available on Communication Manager systems with the Expert Agent Selection (EAS) feature.

### Procedure

1. From the CController 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** ields 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.

# Viewing VDN skill preferences

## About this task

This section provides the procedure for viewing skill preferences for a VDN. This feature is only available on Communication Manager systems with the Expert Agent Selection (EAS) feature.

## 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

## About this task

This section provides the procedure for listing all skill preferences for a VDN. This feature is only available on switches with the Expert Agent Selection (EAS) feature.

## 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.

# Split/skill call profiles

Call profiles are settings for a split or 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 time that is allowed 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.

## Before using split/skill call profiles

The following items should be read and understood before 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 and represents a unit of wait time. The number of seconds for the second through the ninth increment must be at least 1 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.
- Making changes to the service level field after data was collected with a different service level value causes reports to give inaccurate data for the **Percent within Service Level** value. 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.

## Permissions for split/skill call profiles

Depending on the procedure that you want to perform, you need the following permissions:

- To view split/skill call profiles, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem and all affected splits and skills.

- To add, delete, or change a split/skill call profile, the user ID used to log in to this Supervisor session requires “write” permission for the Call Center Administration subsystem and all affected splits and skills.

# Adding split/skill call profiles

## About this task

The section provides the procedure for adding a split/skill call profile.

## Procedure

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

   Supervisor displays the Call Center Administration window.

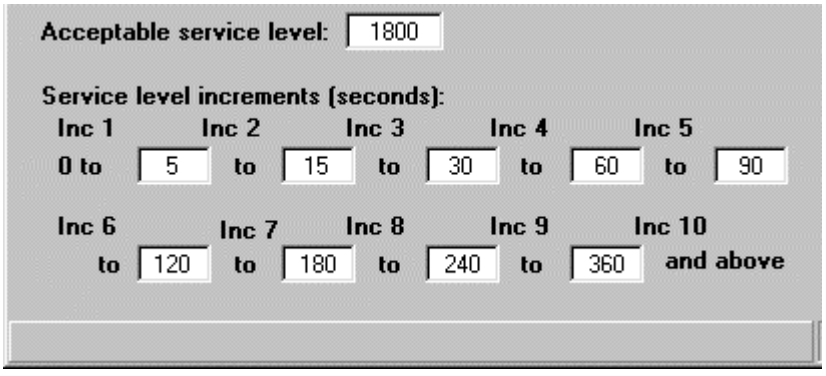
2. In the **ACD** field, select the ACD on which the new split/skill call profile will be created.
3. In the **Operations** list, highlight **Split/Skill Call Profile Setup**.
4. Select **OK**.

   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 objective speed of answer for the splits or skills.

   This field represents the number of seconds for the speed of answer and can accept values from `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 half-hour intrahour interval or `3600` for an hour-long intrahour interval. You must enter a value in this field.

   The following example displays how an administrator might set up a split/skill call profile:

   The **Acceptable service level** field, has been 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 addressed after the acceptable service level of `1800` seconds, the call is then tracked in a different CMS database category.

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.

   If these fields are not supplied with data, `0` is used for all service level increments and all calls appear in the first increment on the split/skill call profile report.

8. Select **Actions** > **Add**.

   The status bar displays a message stating if the operation succeeded or failed.

# Viewing an existing split/skill call profile

## About this task

This section provides the procedure for viewing a split/skill call profile that already exists.

## 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 existing split/skill call profile resides.
3. In the **Operations** list, highlight **Split/Skill Call Profile Setup**.
4. Select **OK**.

   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.

# Modifying a split/skill call profile

## About this task

This section provides the procedure for modifying a call profile for a split or skill.

## 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 split/skill call profile to modify resides.
3. In the **Operations** list, highlight **Split/Skill Call Profile Setup**.
4. Select **OK**.

   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. Enter the new values in the **Acceptable service level** or the **Service Level Increments (seconds)** fields.
8. From the **Actions** menu, select **Modify**.

   The status bar displays a `Successful` message when the operation completes.

# Deleting a split/skill call profile

## About this task

This section provides the procedure for deleting a split/skill call profile.

## 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 split/skill call profile to delete resides.
3. In the **Operations** list, highlight **Split/Skill Call Profile Setup**.

   Supervisor displays the Split/Skill Call Profile Setup window.
4. In the **Split(s)/Skill(s)** field, enter the split or skill on which the call profile to delete resides.
5. 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.

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

   Supervisor deletes the specified split/skill call profile and displays a `Successful` message in the status bar.

# Trunk group assignments

A trunk group is a group of circuits that are assigned the same dialing digits, either a telephone number or a Direct-Inward-Dialing (DID) prefix. Trunk groups can be assigned to Vector Directory Numbers (VDNs) or non-vector-controlled splits.

## Before using trunk group assignments

The following items should be read and understood before working with trunk group assignments:

- Automatic-in trunk groups, such as those that are used as Listed Directory Numbers, must be assigned to VDNs or splits through an administration tool for the Communication Manager system.
- DID or dial-repeating trunks, such as those that toll-free numbers are assigned to, are not assigned to VDNs or splits since the Central Office (CO) passes VDN digits or the split extension number to the Communication Manager system. Because of this, toll-free numbers do not appear during these procedures.
- Vector-controlled splits cannot have trunk groups assigned to them because they can only receive calls through vector processing.
- The Trunk Group Assign window used in these procedures cannot be used to change trunk group assignments. Changing trunk group assignments is done through an administration tool for the Communication Manager system.

## Permissions for trunk group assignments

To view trunk group assignments, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem and for all affected trunk groups, splits, and VDNs.

# Viewing all trunk group assignments

## About this task

This section provides the procedure for viewing all trunk group assignments.

## 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 trunk group assignments are to be viewed.
3. In the **Operations** list, highlight **Trunk Group Assignments**.
4. Select **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

## About this task

This section provides the procedure for viewing the assigned VDN or split for a single trunk group.

## 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 for which trunk group assignments are to be viewed.
3. In the **Operations** list, highlight **Trunk Group Assignments**.
4. Select **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

### About this task

This section provides the procedure for viewing the trunk group that is assigned to a specific VDN or split.

### 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 for which trunk group assignments are to be viewed.
3. In the **Operations** list, highlight **Trunk Group Assignments**.
4. Select **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.

# Trunk group members report

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 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 for trunk group members report

To run a trunk group members report, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem and all affected trunk groups.

## Running a trunk group members report

### Procedure

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

   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. Select **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** - 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.

# VDN-to-vector assignments

A Vector Directory Number (VDN) is an extension number that enables incoming calls to be connected to a vector for processing. The VDN by itself may be dialed to access the vector from any extension that is connected to the switch. Initial assignment of a VDN to a vector is done on the Communication Manager system, but can later be changed using CMS or Supervisor.

## Before using VDN-to-vector assignments

The following items should be read and understood before working with VDN-to-vector 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 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 completes before the next assignment change request is scheduled.

## Permissions for VDN-to-vector assignments

Depending on the procedure that you want to perform, you need the following permissions:

- To view VDN-to-vector assignments, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem and for all affected VDNs and vectors.
- To modify VDN-to-vector assignments, the user ID used to log in to this Supervisor session requires “write” permission for the Call Center Administration subsystem and for all affect VDNs and vectors.

## Viewing all VDN-to-vector assignments

### About this task

This section provides the procedure to view all VDN-to-vector assignments.

### 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 for which VDN-to-vector assignments are to be viewed.
3. In the **Operations** list, highlight **VDN Assignments**.
4. Select **OK**.

   Supervisor displays the VDN Assignments window.
5. Select **Actions** > **List all** from the menu bar.

   Supervisor displays a secondary window that lists all VDNs for which this user ID has “read” permission.

## Listing VDNs associated with a vector

### About this task

This section provides the procedure for listing the VDNs that are associated with a specific vector.

### 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 vector resides.
3. In the **Operations** list, highlight **VDN Assignments**.
4. Select **OK**.

   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.

   Supervisor displays a secondary window that lists all VDNs assigned to the specified vector.

# 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 time that is allowed 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 VDN call profile reports to determine the number of calls that were addressed in each increment.

# Before using VDN call profiles

The following items should be read and understood before work is done 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 greater 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 greater.
- Making changes to the service level field after data was collected with another service level value causes reports to give inaccurate data for the **Percent within Service Level** value. 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.

# Permissions for VDN call profiles

Depending on the procedure that you want to perform, you need the following permissions:

- To view a VDN call profile, the user ID used to log in to this Supervisor session requires “read” permission for the Call Center Administration subsystem and all affected VDNs.
- To add, delete, or change a VDN call profile, the user ID used to log in to this Supervisor session requires “write” permission for the Call Center Administration subsystem and all affected VDNs.

# Adding a VDN call profile

## About this task

This section provides the procedure for adding a VDN call profile to an ACD.

## 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 VDN call profile will be added.
3. In the **Operations** list, highlight **VDN Call Profile Setup**.
4. Select **OK**.

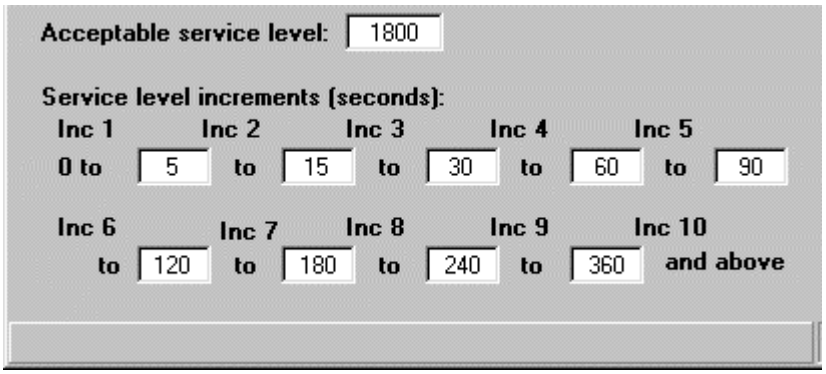
   Supervisor displays the VDN Call Profile Setup window.

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 maximum number of seconds in which a VDN call should be addressed.

   This value can range from `0` to `3600`. However, the value should be no larger than the number of seconds in the intrahour interval that is set on

   CMS , for example, `1800` for a half-hour intrahour interval or `3600` for an hour-long intrahour interval.
7. In each **Service Level Increments (seconds)** field, enter a progressively larger number of seconds in each **To** field.

   The following example shows how an administrator might set up a VDN call profile:




   The **Acceptable service level** field, is set to `1800` seconds to correspond with the intrahour interval that is used on the CMS server.

   **Inc 1** is set to a range of `0 to 5` seconds. **Inc 2** ranges is set to a range of `5 to 15` seconds. If the call is not resolved, CMS continues to process the call through the other service-level increments until **Inc 10**. The **Inc 10** service-level increment is used in this example for those calls that extend beyond 360 seconds. If a call is not addressed 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.

# Viewing an existing VDN call profile

## About this task

This section provides the procedure for viewing a VDN call profile that already exists on an ACD.

## 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 VDN call profile will be added.
3. In the **Operations** list, highlight **VDN Call Profile Setup**.
4. Select **OK**.

   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.

# Modifying a VDN call profile

## About this task

This section provides the procedure for modifying a VDN call profile that already exists on an ACD.

## 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 VDN call profile will be modified.
3. In the **Operations** list, highlight **VDN Call Profile Setup**.
4. Select **OK**.

   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. Enter new values in the appropriate fields:
   - Enter a new value in the **Acceptable service level** field to match the intrahour interval that is set on the CMS server.
   - Enter new ranges of time in the **Service Level Increments (seconds)** fields as needed.
8. Select **Actions** > **Modify** from the menu bar.

   The status bar displays a `Successful` message when the operation completes.

## Deleting a VDN call profile

### About this task

This section provides the procedure for deleting an existing VDN call profile on an ACD.

### Procedure

1. Controller window, select **Commands** > **Call Center Administration**

   Supervisor displays the **OK** window.
2. In the **ACD** field, select the ACD on which the VDN call profile will be deleted.
3. In the **Operations** list, highlight **VDN Call Profile Setup**.
4. Select **OK**.

   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.

# Vector configuration report

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 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 for 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 Supervisor 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 vector configuration reports

### About this task

This section provides the procedure for running a vector configuration report.

### Procedure

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

   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. Select **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** - 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.

# Data summarization time zone

## About this task

To allow alternative time zone reporting for daily, weekly, and monthly data, you must administer the desired time zones for CMS to aggregate the data based on the additional time zone. The user requires this administration to run daily, weekly, or monthly reports for a specific time zone. You can administer only one time zone per ACD and an additional time zone per tenant per ACD if tenancy is installed. CMS must be in single-user mode to carry out this task. You must have permissions for the tenant to administer a time zone for the tenant.

**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.

## 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, perform the following operations as explained in the table below:

# 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 `Already exists` 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 `Does not exist` 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 9: Administering Exceptions

## Administering exceptions

This section provides the procedures for administering exceptions, running the Real-time Exception Log report, and running other exception reports for the following exception areas:

- Agent
- Split/skill
- Trunk group
- VDN
- Vector
- Data Collection
- Malicious call trace
- Real-time exceptions log

## About 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. Exceptions are gathered on agents, splits/skills, trunk groups, VDNs, vectors, and unusual events such as Malicious Call Trace and disruptions in data collection. This section describes the operations, prerequisites, and rules for administering exceptions and the different types of exception reports that are available.

You can administer exceptions and generate reports for VDNs and vectors if your company has purchased the Call Vectoring feature.

You can administer exceptions and generate reports for skills if your company has purchased the Expert Agent Selection (EAS) feature.

### 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 of an ACD activity exceeds an occurrence threshold that is defined for your contact 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 contact center. When the current 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, an agent timed exception could be configured to occur whenever an agent spends more than 5 minutes in the AUX work mode. Then, when an agent spends longer than 5 minutes in the AUX work mode, an exception is triggered for that agent. 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 may set the time limit at 20 seconds for any call to wait in queue before being answered. You may 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 longer than 20 seconds within an interval.

Timed occurrence boundaries for this type of exception apply to ACD activity 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 1 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.

## Notification

The status bar of the Supervisor Controller window shows the current exception total for both the peg count and time exceptions. This exception total is for all of the ACDs for which you have permission to view exceptions. The exception count is cleared at the end of each interval and can display a maximum number of 9999.

The PC on which Supervisor is running is, by default, configured to beep each time an exception occurs. Changing this setting can be done by selecting **Options** > **General** on the Supervisor menu bar.

### Exception capacities

CMS requires that you define the storage space on the server to record the activities of the contact center. The recording of exceptions also uses this storage space. The limits for recording exceptions are provided in the *Avaya Aura® Communication Manager System Capacities Table*. The following items provide information on the way CMS handles recording of exceptions:

- CMS can store exception records of each element on all ACDs. There are exception records stored for elements like agents, split/skill, trunk groups, VDNs, and vectors across all ACDs .
- You can retrieve the stored exception records from ACDs. The exception retrieval capacity is the number of days in the past for which you can retrieve exceptions. This is determined by the following criteria:
  - The number of exception records that are allocated for storage in the **Data Storage** operation in the System Setup window.
  - 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.

## Before using exceptions

The following items should be read and understood before you begin working with exceptions:

- If an ACD Group is selected as the current ACD in the Exceptions window, only those operations that are valid for the ACD Group will appear in the **Operations** list.

When exception thresholds are configured, the following rules must be followed:

- 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.
- When at least one exception is added to an entity, any future additions must be made by using the **Modify** item on the **Actions** menu.
- When exceptions are being modified, the **Find one** menu item should always be used to retrieve the current settings for the exception before any changes are made.
- 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 exceptions

The following table describes the permission settings that are required in order for a user to access exception information:

| Does the user have “read” permission for the Exceptions feature? | … and “exceptions” permission for splits/skills, trunk groups, ACDs, vectors, and VDNs? | Then, the user can use the following exception information: |
|---|---|---|
| yes | yes | • Exception reports<br>• Messages in the Real-Time Exception Log<br>• Real-time notification of exceptions |
| yes | no | • Exceptions reports |
| no | yes | • Real-time notification of exceptions |
| no | no | • No exceptions features available to this user |

Setting the exception permissions for these entities can be done through **Tools** > **User Permissions** on the Supervisor Controller window.

### Other permissions

To set up or change the method in which the system checks for exceptions, the user ID used to log in to this Supervisor session requires the “write” permission for the Exceptions feature.

To be notified of a malicious call exception, the user ID used to log in to this Supervisor session requires the “exception” permission for the appropriate contact center entity.

# Exception notification

An exception notification is a beep that is sounded by Supervisor when an exception is encountered. By default, this occurs when the user who is currently logged in to Supervisor has the “exceptions” permission for the entity on which the exception occurred. If you do not want Supervisor to beep when an exception occurs, follow the procedure in this section.

## Changing exception notification

### About this task

This section provides the procedure for changing whether the beep notification is sounded when an exception occurs.

### 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, place a check mark in the **Use Sound** check box.
   - To turn off exception notification, remove the check mark in the **Use Sound** check box.
4. Select **OK**.

# Agent exceptions

Agent exceptions can occur for many different activities in relation to an agent. These can include the amount of time on a call or in a work state, the number of calls that an agent has in queue, and other activities. This section provides the procedure for configuring if and when these exceptions are checked by CMS.

## Before using agent exceptions

The following items should be read and understood before 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.
- The agent exceptions record for a split/skill are not created by default in the CMS database when the split/skill is created. If a split/skill does not have agent exceptions, an **Add** action must be taken to create the associated agent exceptions record.

# Permissions for 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 split/skills as well as the “exceptions” permission for the affected splits/skills.

# Adding agent exceptions

## About this task

This section provides the procedure for adding agent exceptions for a split/skill.

## Procedure

1. From the Controller window, select **Commands** > **Exceptions** on the menu bar.

   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. Select **OK**.

   Supervisor displays the Agent Exceptions Administration window.

   This window appears with all fields blank when first opened.

   **Note:**

   This is a scrolling dialog box that contains more exceptions than those shown in the above graphic. Use the scroll bar on the right side of the dialog box to view the other exceptions.

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. Perform the following actions in the specified fields for each **Exception type** that you want to monitor:

**Active** - Select this check box to enable the exception and allow it to run and adhere to the parameters that are given in the other fields. Leaving this check box blank disables the exception and CMS will not attempt to track the activity for this exception.

**Time Limit** - Enter the time limit in seconds (0 to 28800) for those exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity depending on the type of exception. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field. This field requires an entry and cannot be left blank.

**Threshold** - Enter the number of acceptable occurrences of this activity (0 to 999). Any occurrences beyond this number will generate an exception. If you want CMS to create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.

7. When all necessary time limits and thresholds have been entered, select **Actions** > **Add** from the menu bar.

   The exception configuration data will be saved for this split/skill and the status bar displays a “Successful” message.

# Modifying agent exceptions

## About this task

This section provides the procedure for modifying the existing agent exception configuration for a split/skill.

## Procedure

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

   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. Select **OK**.

   Supervisor displays the Agent Exceptions Administration window.

   This window appears with all fields blank when first opened.

**Note:**

This is a scrolling dialog box that contains more exceptions than those shown in the above graphic. Use the scroll bar on the right side of the dialog box to view the other exceptions.

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. Perform the following actions in the specified fields for each **Exception type** that you want to monitor:

   **Active** - Place a check mark in this check box to enable the exception and allow it to run and adhere to the parameters that are given in the other fields. Leaving this check box blank disables the exception and CMS will not attempt to track the activity for this exception.

   **Time Limit** - Enter the time limit in seconds (0 to 28800) for those exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity depending on the type of exception. If this limit is surpassed, CMS counts this activity and compares it against the **Threshold** field. This field requires an entry and cannot be left blank.

   **Threshold** - Enter the number of acceptable occurrences of this activity (0 to 999). Any occurrences beyond this number will generate an exception. If you want CMS to create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.
8. When all necessary time limits and thresholds have been modified, select **ActionsModify** from the menu bar.

   Supervisor updates the data for this split/skill and displays a `Successful` message in the status bar.

# Deleting agent exceptions

## About this task

This section provides the procedure for deleting the agent exceptions for a split/skill.

## Procedure

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

   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. Select **OK**.

   Supervisor displays the Agent Exceptions Administration window.

   **Note:**

   This is a scrolling dialog that contains more exceptions than those shown in the above graphic. Use the scroll bar on the right side of the dialog to view the other exceptions.
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 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, 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 definitions

The following table provides the definitions for the different agent exceptions:

| Exception | Definition |
|---|---|
| **Time Available** | The time that an agent spends in AVAIL (this is idle time). |
| **Time on inbound ACD call (minimum)** | The minimum time that an agent spends on an ACD call. |
| **Time on inbound ACD call (maximum)** | The maximum time that an agent spends on an ACD call. |
| **Time in after-call work (maximum)** | The maximum time that an agent spends on after-call work. |
| **Time on inbound ACW call (maximum)** | The maximum time that an agent spends on an inbound call during after-call work. |

*Table continues…*

| Exception | Definition |
|---|---|
| **Number of inbound ACW calls/agent** | The total number of inbound calls that an agent can receive during after-call work. This exception can only be triggered once per interval. |
| **Time on outbound ACW call (maximum)** | The maximum time that an agent spends on an outbound call during after-call work. |
| **Number of outbound ACW calls/agent** | The total number of outbound calls that an agent can make during after-call work. This exception can only be triggered once per interval. |
| **Time in AUX work (maximum)** | The maximum time that an agent spends doing auxiliary work. |
| **Time on inbound AUX call** | The maximum time that an agent spends on an inbound call during auxiliary work. |
| **Number of inbound AUX calls/agent** | The total number of inbound calls that an agent can receive during auxiliary work. This exception can only be triggered once per interval. |
| **Time on outbound AUX call (maximum)** | The maximum time that an agent spends on an outbound call during auxiliary work. |
| **Number of outbound AUX calls/agent** | The total number of outbound calls that an agent can place during auxiliary work. This exception can only be triggered once per interval. |
| **Time in AUX with Reason Code X (maximum)** | The maximum time that agents can spend doing auxiliary work with Reason Code X (X is from 0 to 9 or 0 to 99). |
| **Login Identification** | Select **Active** to receive a notification of a login violation. 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 at 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 (minimum)** | The minimum time that an agent spends on an outbound ACD call. |
| **Time on outbound ACD call (maximum)** | The maximum time that an agent spends on an outbound ACD call. |
| **Number calls transferred** | The maximum number of calls that an agent can transfer. |
| **Time ACD call spent on hold (maximum)** | The maximum time that an agent can put an ACD call 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 (maximum)** | 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 (maximum)** | 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 | Definition |
|---|---|
| **Time ACD call spends ringing (maximum)** | The maximum time that a split/skill or direct agent ACD call can ring at agent's voice terminal before an exception is triggered. |
| **Ringing call automatically redirected from agent** | Select **Active** to be notified when an agent lets an ACD call ring at the voice terminal long enough for the switch to automatically redirect the call. You must have the Redirection on No Answer feature activated on the Communication Manager system to use this exception. |
| **Time on direct agent call (maximum)** | The maximum number of seconds that an agent spends on a direct agent ACD call. |
| **Number calls in direct agent queue (maximum)** | The maximum number of direct agent ACD calls that an agent can have waiting in queue. |
| **Time call waited in direct agent queue (maximum)** | The maximum time that any call waits in the direct agent queue. |
| **Number calls abandoned from direct agent queue (maximum)** | The maximum number of direct agent ACD calls that can leave the direct agent queue by abandoning before an exception is triggered. 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 (maximum)** | The maximum number of seconds that an agent spends on an external outbound call during after-call work. |
| **Number of external outbound ACW calls/agent (maximum)** | The maximum number of external outbound calls that an agent can make while in after-call work. This exception can only be triggered once per interval. |
| **Time on external outbound AUX calls (maximum)** | The maximum number of seconds an agent spends on an external outbound call during auxiliary work. |
| **Number external outbound AUX calls/ agent (maximum)** | The maximum number of external outbound calls that an agent can make during auxiliary work. This exception can only be triggered once per interval. |
| **Agent logged out with active/held calls** | Select **Active** 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 codes** Agent entered invalid call work codes | An exception that is pegged for CWC 0 (an agent types an unadministered call work code). This exception should be turned off if you are collecting call work codes in call records only. |

# Split/skill exceptions

Using split/skill exceptions can help identify those splits/skills that need to be adjusted to achieve more efficiency in the contact center.

Split/skill exceptions can assist you in the identification of problems in the following areas:

- 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

## Before using split/skill exceptions

The following items should be read and understood before working with split/skill exceptions:

- To administer exceptions for skills, your company must have purchased Expert Agent Selection (EAS). However, this feature is not needed to administer exceptions for splits.
- The split/skill exceptions configuration is not created by default in the CMS database when the split/skill is created. If a split/skill does not have an exceptions configuration, an **Add** action must be taken to create it.

## Permissions for 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 splits/skills as well as the “exceptions” permission for all affected splits/skills.
- 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 splits/skills as well as the “exceptions” permission for all affected splits/skills

## Adding split/skill exceptions

### About this task

This section provides the procedure for adding split/skill exception configurations.

### Procedure

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

   Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the split/skill to receive the new exception configuration.

3. In the **Operations** list, highlight **Split/Skill Exceptions**.
4. Select **OK**.

   Supervisor displays the Split/Skill Exception Administration window.
5. In the **Split(s)/Skill(s)** field, enter the name or number of the split/skill for which an exceptions configuration is to be created.
6. For each **Exception type** that should be monitored, the following fields must be configured:
   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.
   - **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
   - **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.
7. When all necessary time limits and thresholds have been entered, select **Actions** > **Add** from the menu bar.

   Supervisor saves the data for this split/skill and the status bar displays a `Successful` message.

# Modifying split/skill exceptions

## About this task

This section provides the procedure for modifying existing split/skill exception configurations.

## Procedure

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

   Supervisor displays the Exceptions window.
2. In the **ACD**field, select the ACD that contains the split/skill and its exception configuration.
3. In the **Operations** list, highlight **Split/Skill Exceptions**.
4. Select **OK**.

   Supervisor displays the Split/Skill Exception Administration window.
5. In the **Split(s)/Skill(s)** field, enter the name or number of the split/skill for which its exceptions configuration is to be modified.
6. From the menu bar, select **Actions** > **Find one**.

Supervisor locates the exception configuration for the specified split/skill and the displays the data in the appropriate fields. If exception configuration data cannot be found, the status bar displays `0 matches found`.

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. Make the necessary changes in the following fields for each **Exception type** that requires modification:
   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.
   - **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
   - **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.
8. When all necessary time limits and thresholds have been entered, select **Actions** > **Modify** from the menu bar.

   Supervisor saves the data for this split/skill and the status bar displays a `Successful` message.

# Deleting split/skill exceptions

## About this task

This section provides the procedure for deleting existing split/skill exception configurations.

## Procedure

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

   Supervisor displays the Exceptions window.
2. In the **ACD** field, select the ACD that contains the split/skill and its exception configuration.
3. In the **Operations** list, highlight **Split/Skill Exceptions**.
4. Select **OK**.

   Supervisor displays the Split/Skill Exception Administration window.
5. In the **Split(s)/Skill(s)** field, enter the name or number of the split/skill 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 split/skill and the displays the data in the appropriate fields. If exception configuration data cannot be found, the status bar displays `0 matches found`.

   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, select **Actions** > **Delete**.

   Supervisor deletes the exception configuration for this split/skill from the CMS database and a displays a `Successful` message in the status bar.

## Split/skill exception definitions

The following table provides the definitions for the different split/skill exceptions.

| Field | Description |
|---|---|
| **Time call has waited in queue** | The total acceptable amount of time any call in queue remains unanswered before an occurrence is counted against the threshold limit. |
| **Number calls waiting** | The maximum number of calls waiting in queue at any one time. |
| **Number calls abandoned** | The total number of acceptable abandoned calls. This exception can only be triggered once per interval. |
| **Average speed of answer (seconds)** | The maximum acceptable amount of time in seconds that a call waits in that split/skill queue before an agent answers. This exception can only be triggered once per interval. |
| **Number intraflowed-out calls** | The maximum acceptable number of calls that intraflow out from or in to a split or skill. This exception can only be triggered once per interval. |
| **Number intraflowed-in calls** | The acceptable number of calls that can intraflow in to the split or 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 or skill. This exception can only be triggered once per interval. |
| **Number calls handled as backup** | The acceptable number of calls that this split or skill can handle as a backup for another split or skill. This exception can only be triggered once per interval. |
| **Number calls transferred** | The acceptable number of calls that can be transferred from this split or skill. This exception can only be triggered once per interval. |

*Table continues…*

| Field | Description |
|---|---|
| **Number calls offered while queue full** | The acceptable number of calls that can be offered to the split or 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 **MED** 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** | The maximum acceptable amount of time in seconds that is calculated for the rolling average speed of answer (ASA) for a split/skill. This exception can only be triggered once per interval. The ASA for the measured split/skill is sent to CMS by way of the ASA message. An occurrence is counted (in seconds) when CMS receives an ASA that exceeds the time limit that is specified for a split/skill. 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 contact center.

## Before using trunk group exceptions

The following items should be read and understood before working with trunk group exceptions:

- An Audio Difficulty exception is associated with each trunk group. This exception is always provided for all Communication Manager systems that support event counts and it cannot be disabled. For this reason, this exception is not available on the Trunk Group Exception Administration window.

# Permissions for 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.

# Adding trunk group exceptions

## About this task

This section provides the procedure for adding an exception configuration for a trunk group.

## Procedure

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

   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, highlight **Trunk Group Exceptions**.
4. Select **OK**.

   Supervisor displays the Trunk Group Exception Administration window.

5. In the **Trunk Groups** field, enter the name or number of the trunk group for which an exceptions configuration is to be created.
6. For each **Exception type** that should be monitored, the following fields must be configured:
   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.
   - **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
   - **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.
7. When all necessary time limits and thresholds have been entered, select **Actions** > **Add** from the menu bar.

Supervisor saves the data for this trunk group and the status bar displays a `Successful` message.

# Modifying trunk group exceptions

## About this task

This section provides the procedure for modifying an existing exception configuration for a trunk group.

## Procedure

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

   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, highlight **Trunk Group Exceptions**.
4. Select **OK**.

   Supervisor displays the Trunk Group Exception Administration window.

5. In the **Trunk Groups** field, enter the name or number of the trunk group for which exception configuration is to be modified.
6. From the menu bar, select **Actions** > **Find one**.

   Supervisor locates the exception configuration data for the specified trunk group and displays it in the appropriate fields. If data cannot be found for this trunk group, the status bar displays `0 matches found`.

   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. For each **Exception type** that should be monitored, the following fields must be configured:
   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.
   - **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
   - **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.

8. When all necessary time limits and thresholds have been entered, select **Actions** > **Modify** from the menu bar.

   Supervisor updates the data for this trunk group and the status bar displays a `Successful` message.

# Deleting trunk group exceptions

## About this task

This section provides the procedure for deleting existing trunk group exception configurations.

## Procedure

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

   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, highlight **Trunk Group Exceptions**.
4. Select **OK**.

   Supervisor displays the Trunk Group Exception Administration window.

5. In the **Trunk Groups** field, enter the name or number of the trunk group for which the exception configuration is to be deleted.
6. From the menu bar, select **Actions** > **Find one**.

   The exception configuration is found for the specified trunk group and the data displays in the appropriate fields. If exception configuration data cannot be found, the status bar will display `0 matches found`.

   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, select **Actions** > **Delete**.

   The exception configuration for this trunk group is deleted from the CMS database and a `Successful` message displays in the status bar.

# Trunk group exception definitions

The following table provides the definitions for the different trunk group exceptions:

| Field | Description |
|---|---|
| **Time trunk in use (min)** | The minimum acceptable time in seconds that a trunk in the trunk group can 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 in the trunk group 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 in the trunk group can be in the maintenance busy state. |
| **Length of time all trunks busy** | The maximum acceptable time that all trunks in the trunk group can be busy at once. This exception can only be triggered once per interval. |
| **Number of trunks in use** | The maximum acceptable number of trunks that can be in use at the same time in the trunk group. An exception is reached each time the allowed number of trunks in use exceeds the threshold within the interval. |
| **Number of trunks maintenance busy** | The maximum acceptable number of trunks that can be in the maintenance busy state in the trunk group. An exception is reached each time the allowed number of trunk that are in the maintenance busy state exceeds the threshold within the interval. |

# VDN exceptions

Use Vector Directory Number (VDN) exceptions to assist in the identification of problems in the following areas:

- The amount of time calls that remain in the vector or at 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 and if they are successful

## Before using VDN exceptions

The following items should be read and understood before working with VDN exceptions:

- To administer VDN exceptions, your company must have purchased and installed the Call Vectoring feature.
- Because of the routing that is permitted by the `go to vector` command, the **Time in Vector** exception may include the time that a call spends in more than one vector.
- CMS begins to monitor 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 circumstances is encountered:
  - The call routes to another vector through a `go to vector` step.

- The call is sent through a `route to` or `adjunct routing` step to a non-VDN extension that is internal to the local Communication Manager system.

- If a large number of VDNs exist in the Dictionary (over 2000), there can be lengthy waiting periods when you browse for VDNs through Supervisor.
- Some exception types require that an appropriate step exists in the vector to which the VDN is assigned. For example, to get exceptions on unsuccessful **Lookahead Interflow Attempts**, the vector for the VDN must have at least one `route to` step that routes calls to a vector on a remote switch.

## Permissions for 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.

## Adding VDN exceptions

### About this task

This section provides the procedure for adding an exceptions configuration to a VDN.

### Procedure

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

   Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the VDN that will receive the new exceptions configuration.
3. In the **Operations** list, highlight **VDN Exceptions**.
4. Select **OK**.

   Supervisor displays the VDN Exception Administration window.

5. In the **VDNs** field, enter the name or number of the VDN for which the exceptions configuration is to be created.
6. For each **Exception type** that should be monitored, the following fields must be configured:

   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.

- **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
- **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.

7. When all necessary time limits and thresholds have been entered, select **Actions** > **Add** from the menu bar.

   Supervisor saves the data for this VDN exception configuration and the status bar displays a `Successful` message.

# Modifying VDN exceptions

## About this task

This section provides the procedure for modifying an existing exception configuration for a VDN.

## Procedure

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

   Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the VDN and its exception configuration.
3. In the **Operations** list, highlight **VDNs**.
4. Select **OK**.

   Supervisor displays the VDN Exception Administration window.

5. In the **VDNs** field, enter the name or number of the VDN for which exception configuration is to be modified.
6. From the menu bar, select **Actions** > **Find one**.

   Supervisor locates the exception configuration data for the specified VDN and displays it in the appropriate fields. If exception configuration data cannot be found for this VDN, the status bar displays `0 matches found`.

   To have all VDNs returned in this step, leave the **VDNs** field blank before performing the **Find one** action. 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. For each **Exception type** that should be monitored, the following fields must be configured:

   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.

- **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
- **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.

8. When all necessary time limits and thresholds have been entered, select **Actions** > **Modify** from the menu bar.

   Supervisor updates the exception configuration data for this VDN and the status bar displays a `Successful` message.

# Deleting VDN exceptions

## About this task

This section provides the procedure for deleting existing VDN exception configurations.

## Procedure

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

   Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the VDN and its exception configuration.
3. In the **Operations** list, highlight **VDN Exceptions**.
4. Select **OK**.

   Supervisor displays the VDN Exception Administration window.

5. In the **VDNs** field, enter the name or number of the VDN 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. If exception configuration data cannot be found, the status bar displays `0 matches found`.

   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, select **Actions** > **Delete**.

   Supervisor deletes the exception configuration for this VDN from the CMS database and displays a `Successful` message in the status bar.

# VDN exception definitions

The following table provides the definitions for the different VDN exceptions:

| Name | Description |
|---|---|
| **Time in Vector** | The maximum acceptable time in seconds that a call should spend in vector processing. This exception can only be triggered once per interval. |
| **Time at agent (minimum)** | The minimum acceptable time in seconds that a call to this VDN is connected to an agent. This exception can only be triggered once per interval. |
| **Time at agent (maximum)** | The maximum acceptable time in seconds that a call to this VDN is connected to an agent. This exception can only be triggered once per interval. |
| **Number of calls abandoned while in vector** | The maximum acceptable number of calls to this VDN that are abandoned before being answered during an interval. This exception can only be triggered once per interval. |
| **Number of calls forced busy** | The maximum acceptable number of calls to this VDN that receive a busy signal from the switch during an interval. This exception can only be triggered once per interval. |
| **Number of calls disconnected** | The maximum acceptable number of calls that are disconnected during vector processing during an interval. 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 from the `busy` command are not included. This exception can only be triggered once per interval. |
| **Number of calls in an ACD split/ skill queue** | The maximum acceptable number of call to this VDN that are in a split/skill queue. |
| **Number of calls that flowed into VDN** | The maximum number of calls during an interval that enter this VDN by a `route-to` or `adjunct routing link` vector step, or a transfer from a local extension. This exception can only be triggered once per interval. |
| **Number of calls that flowed out of VDN** | The maximum acceptable number of calls that are routed from this VDN during an interval to another VDN or external destination. This exception can only be triggered once per interval. |
| **Number of calls that interflowed out of VDN** | The maximum acceptable number of calls that are routed from this VDN to an external destination during an interval. This exception can only be triggered once per interval. |
| **Number of calls handled by backup split or skill** | The maximum acceptable number of calls to this VDN that are 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 |

*Table continues…*

| Name | Description |
|---|---|
| | a backup split/skill. This exception cannot trigger more than once per interval. |
| **Number of unsuccessful look ahead interflow attempts** | The maximum acceptable number of calls to this VDN that fail to interflow to another Communication Manager system during an interval. The `route-to vector` command causes a call to interflow. This exception can only be triggered once per interval. |
| **Number of unsuccessful adjunct routing attempts** | The maximum acceptable number of failures of a call to this VDN to connect to an adjunct host computer during an interval. The failure of an `adjunct route link` vector command causes an unsuccessful adjunct routing attempt. 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. |
| **Rolling Average Speed of Answer** | The acceptable amount of time, in seconds, that is calculated for the rolling average speed of answer for a VDN. This exception can only be triggered once per interval. |

# Vector exceptions

When vector exceptions are configured and activated, CMS monitors for these exceptions when a call enters the vector and continues monitoring until the call connects to an agent, is abandoned, or is routed to another destination.

Vector exceptions can assist in the identification of 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 forced busy while in the vector
- Numerous unsuccessful routing attempts

## Before using vector exceptions

The following items should be read and understood before working with vector exceptions:

- Calls may generate some exceptions for a vector, even after the vector has given routing control to the adjunct by an `adjunct routing` vector command.
- Some exception types require that an appropriate step exists in the vector. For example, to get exceptions on unsuccessful Look Ahead Interflow attempts, the vector must have at least one `route to` step which routes calls to a remote Communication Manager system.

# Permissions for 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.

# Adding vector exceptions

## About this task

This section provides the procedure for adding an exceptions configuration for a vector.

## Procedure

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

   Supervisor displays the Exceptions window.

2. In the **ACD** field, select the ACD that contains the vector that will receive the new exceptions configuration.
3. In the **Operations** list, highlight **Vector Exceptions**.
4. Select **OK**.

   Supervisor displays the Vector Exceptions Administration window.

5. In the **Vectors**: field, enter the name or number of the vector for which an exceptions configuration is to be created.
6. For each **Exception type** that should be monitored, the following fields must be configured:
   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.
   - **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
   - **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.
7. When all necessary time limits and thresholds have been entered, select **Actions** > **Add** from the menu bar.

Supervisor saves the data for this vector exception configuration and the displays a `Successful` message in the status bar.

# Modifying vector exceptions

## About this task

This section provides the procedure for modifying an existing exception configuration for a vector.

## Procedure

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

   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. Select **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 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 have all vectors returned when performing this step, leave the **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. For each **Exception type** that should be monitored, the following fields must be configured:

   - **Active** - Place a check mark in this check box to enable the exception allowing it to run and adhere to the parameters given in the other fields. Leaving this check box blank will disable the exception and CMS will not attempt to track the activity for this exception.
   - **Time Limit** - Set the time limit in seconds (0-28800) for exception types that use a time limit. This value is used as the minimum or maximum amount of time for an activity. If this limit is surpassed, CMS will count this activity and compare it against the **Threshold** field. This field is requires an entry and cannot be left blank.
   - **Threshold** - Enter the number of acceptable occurrences of this activity (0-999). Any occurrences beyond this number will generate an exception. If CMS should create an exception on the very first instance, enter `0` in this field. This field requires an entry and cannot be left blank.

8. When all necessary time limits and thresholds have been entered, select **Actions** > **Modify** from the menu bar.

Supervisor updates the exception configuration data for this vector and the status bar displays a `Successful` message.

# Deleting vector exceptions

## About this task

This section provides the procedure for deleting existing vector exception configurations.

## Procedure

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

   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. Select **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 provides the definitions for the different vector exceptions:

| Name | Description |
|---|---|
| **Time in vector (max)** | The maximum acceptable time in seconds that a call is in vector processing. This exception cannot trigger more than once per interval. |

*Table continues…*

| Name | Description |
|---|---|
| **Number calls abandoned while in vector** | The maximum acceptable number of calls that are abandoned during vector processing in an interval. This exception cannot trigger more than once within an interval. |
| **Number of calls forced busy** | The maximum acceptable number of calls that encountered a `forced busy` step in a vector during an interval. This exception cannot trigger more than once per interval. |
| **Number calls disconnected** | The maximum acceptable number of calls that are disconnected during vector processing during an interval. 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. This exception cannot be triggered more than once per interval. |
| **Number of calls in an ACD split/ skill queue** | The maximum acceptable number of calls to this vector that are in a split/skill queue. |
| **Number of unsuccessful look ahead interflow attempts** | The maximum acceptable number of calls to this vector that fail to interflow to another Communication Manager system during an interval. The `route-to` vector command causes a call to interflow. This exception cannot trigger more than once per interval. |
| **Number of unsuccessful adjunct routing attempts** | The maximum acceptable number of failures for a call in this vector to connect to an adjunct host computer during an interval. The failure of an `adjunct route link` vector command causes an unsuccessful adjunct routing attempt. This exception cannot trigger more than one exception per interval. |

Supervisor sends the malicious call trace report to the specified output method.

# Real-time exceptions log

The real-time exception log lists the last ten exceptions in chronological order, with the oldest exception listed first. The log displays all types of exceptions for which the user has the “exception” permission, such as agent, split/skill, trunk group, VDN, and vector.

## Before using real-time exceptions log

The following items should be read and understood before working with the real-time exceptions log:

- When the log is first opened, the most recent exception is on the last line in the window. As long as the window remains open, the log automatically scrolls to display each new exception record. If the scroll bar is used to view the older records at the top of the log, automatic scrolling for new exceptions stops until the user scrolls back to the bottom of the log.

- Each exception record in the log supplies 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 a specific agent, split/skill, or VDN that was involved in the exception.

  If names for these elements were assigned in the Dictionary, these will display instead. If the names are longer than the space that is allowed in the exception record, the names will be truncated.
  - The information about an activity that fell outside of the exception conditions that you set.

  Therefore, for a peg count exception, the exception record shows the occurrence threshold that you set, even though the number of occurrences may be substantially greater. For a timed exception, the exception record shows the time limit that you set, not the actual duration of an 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 that the new exception can be recorded.

## Running the real-time exceptions log

### About this task

This section provides the procedure for running the real-time exceptions log.

### Procedure

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

   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 Exceptions Log**.
4. Select **OK**.

   Supervisor displays the Real-time Exception Log window.

# Exception reports

You can generate reports on any ACD activities, and when you set parameters through options on the **Exceptions Commands** menu.

# Running the agent exceptions by location report

## 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, select **Commands** > **Exceptions**.

   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. Select **OK**.

   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, `10/06/01`.
   - 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 is a required field.

   This field accepts the specification of multiple agents. Multiple values must be separated by a semicolon (;).

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** - 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. Select **OK**.

    Supervisor sends the report to the specified output option.

# Running the data collection exceptions report

## About this task

Use the data collection exceptions report to view any event that affects the storage of contact 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 collections 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, select **Commands** > **Exceptions**.

   Supervisor displays the Exceptions window.
2. Select the **Reports** tab.
3. In the **Reports** list, highlight **Data Collection Exceptions**.
4. Select **OK**.

   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, `10/06/01`.
   - 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 accepts multiple values. Multiple ACDs must be separated by a semicolon (;).

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** - 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. Select **OK**.

   Supervisor sends the data collection exceptions report to the specified output option.

# Running the malicious call trace report

## About this task

The Malicious Call Trace feature provides a way for a terminal user to notify a predefined set of users that he or she 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 or 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 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 Supervisor session requires the “exception” permission for the split/skill that received the malicious call.

### Procedure

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

   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. Select **OK**.

   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, `10/06/01`.
   - 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** - 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. Select **OK**.

## Running the split/skill exceptions report

### 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 exception 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, select **Commands** > **Exceptions**.

   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. Select **OK**.

   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, `10/06/01`.
   - 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 splits/skills 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 splits/skills 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** - 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. Select **OK**.

    Supervisor sends the report to the specified output option.

# Running the trunk group exceptions report

## About this task

Use the trunk group exceptions report 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 exception 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, select **Commands** > **Exceptions**.

   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. Select **OK**.

   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, `10/06/01`.
   - 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** - 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. Select **OK**.

    Supervisor sends the report to the specified output option.

# Running the VDN exceptions report

## 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, select **Commands** > **Exceptions**.

   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. Select **OK**.

   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, `10/06/01`.
   - 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** - 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. Select **OK**.

    Supervisor sends the report to the specified output option.

# Running the vector exceptions report

## 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 exception 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, select **Commands** > **Exceptions**.

   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. Select **OK**.

   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, `10/06/01`.
   - 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** - 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. Select **OK**.

    Supervisor sends the report to the specified output option.

# Chapter 10: Administering User Permissions

## Administering user permissions

The User Permissions subsystem is used to create CMS user IDs as well as assigning and administering user permissions such as “read”, “write”, and “exception” permissions for ACDs, splits/skills, trunk groups, VDNs, and vectors.

The default CMS administrator user ID, “cms”, provides access to the entire system. Using the cms ID, user IDs can be created for each person requiring access to the CMS system and set with the permissions necessary to perform job duties. Users should not share an ID since logging in with the same ID at multiple terminals uses more system resources than if each user had different IDs.

## Before using the User Permissions subsystem

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 will appear in the **Operations** list.

## Example of user permissions

**Important:**

Any user ID (normal or administrator) given “write” access to the User Permission feature will be able to alter their own permissions for all CMS subsystems.

The following table displays an example of permissions that would be necessary for a split supervisor:

| If the contact center has one split called... | And assigned to it are... | The split 1 supervisor requires read/write permissions for... |
|---|---|---|
| Split 1 | Trunk groups 22 and 23 | Split 1<br>Trunk groups 22 and 23<br>Dictionary<br>Exceptions |

## User data

In order for users to use Supervisor, they must first be created through the User Data feature. Afterwards, users can use their assigned ID to log in through Supervisor and CMS. User IDs should only be created for those persons who will be using Supervisor as a part of their job duties in administering the contact center.

The User Data window is used for the following actions:

- Assign a CMS user ID.
- Specify a default CMS printer for a user ID.
- Specify a user ID as Normal or Administrator.
- Administer the maximum number of open simultaneous windows allowed for a user ID.
- Set the minimum refresh rate for real-time reports for a user ID.
- Set the default logon ACD for a user ID.

# About adding a CMS user

## Before adding a CMS user

The following items should be read and understood before adding a user:

- A user ID must be created before any permissions can be assigned to it.
- Users added using an operating system utility, such as useradd, instead of the Supervisor User Data window will not be able to run CMS without assuming the role of a valid user by using the **su** command. Users created using an operating system utility will have a shell type of /usr/bin/ksh. The User Data window does not display users that were created using an operating system utility.
- Users added through the User Data window will automatically have CMS launch when they log in. The shell for these users will be `/usr/bin/cms`.
- The User Data window can be run through scripts and timetables.

## Permissions for adding a CMS user

Depending on the procedure to be performed, the following permissions must be observed:

- To display the User Data window and view user information, the user ID used to log in to this Supervisor session requires “read” permission for the subsystem.

- To add, delete, or modify users through the User Data window, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.
- Tenant users do not have write permissions to the User Permissions sub system and thus cannot add, delete, or modify any users.

# Adding a CMS user

## Procedure

1. From the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

   The **Vector Access** and **VDN Access** menu items are listed if the Call Vectoring feature has been purchased.

2. In the **ACD** field, 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 the other ACDs.

3. In the **Operations** list, highlight **User Data**.

4. Select **OK**.

   Supervisor displays the User Permissions User Data window.

5. In the **User ID** field, enter the new user ID to be created. The user ID must adhere to the following rules:

   - The user ID can be three to eight characters.
   - User IDs cannot contain certain diacritical, accented, special characters, or blanks (for example, á, ñ, ç, |, ©). If a user ID is entered with an invalid character, Supervisor displays an error message.

   This is a required field.

6. In the **User Name**, **Room number**, and **Telephone number** fields, enter the appropriate information for this user.

   These fields are optional and may be left blank.

7. In the **Default printer name** field, select a default CMS printer from the drop-down list box for this user ID.

   This field is optional and my be left as **(none)**.

8. For **Login type**, select the role of this user ID:

   - **Normal user** - Select this type to designate those users whose job responsibilities “do not” include maintenance, configuration, and updating of CMS .

   This role of user has only the “read” permission for the following features:

   - Agent Administration

- Custom Reports/Report Designer
- Dictionary
- Exceptions
- Forecast
- Maintenance
- Reports
- Timetable
- **Administrator** - Select this type to designate those users who job responsibilities include maintenance, configuration, or updating of CMS . This user role is assigned “read” and “write” permissions for all features.

  **Important:**

  Changing the role of the user after creation will not change any permissions assigned to the user. All permission changes need to be done manually.
- **Tenant user** — Select this type to provide a tenant user limited access to CMS administration and reporting data. A newly created tenant user ID will have read, write, and exceptions permissions for his/her Login ACD only. The administrator can add read, write, and exceptions permissions for one or more ACDs besides the Login ACD.

9. In the **Maximum user window count (1-12)** field, enter the number of windows that the user may have open simultaneously. The default for this field is `4`.

   **Important:**

   Allowing many users to have multiple windows open will consume more CMS processor resources.

10. In the **Minimum refresh rate (seconds)** field, enter the number of seconds `(3-600)` in which data for real-time reports is retrieved again from the database and displayed for this user ID.

    **Important:**

    Faster refresh rates consume more CMS processor resources.

11. In the **Login ACD** field, select the ACD which will be used to login this user ID. The user can change the current ACD after logging in, but each time the user logs in, the current ACD defaults to the value entered in this field.

    This is a required field and cannot be left with the default value of **(none)**.

    If an ACD is selected in this field for log in and the user does not have any permissions for it, Supervisor displays an error message.

12. Select **Actions** > **Add** from the menu bar.

    The user ID is created on the ACD specified earlier in the User Permissions dialog box. If the user ID already exists, Supervisor displays an `Already exists` message in the status bar.

**Caution:**

The password of the new user is blank at this time. SSH connections to the CMS server require that the password of the user is set. Refer to Changing a user's password on page 374 if users are going to connect to the CMS server using SSH.

# About viewing CMS users

## Before viewing CMS users

The following items should be read and understood before attempting to view users through the User Data window:

- The default values in the User Data window should be cleared before attempting to perform a **Find one** or **List all** action unless these values should be included in the search.

## Permissions for viewing CMS users

Depending on the procedure to be performed, the following permissions must be observed:

- To display the User Data window and view user information, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify users through the User Data window, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions sub system.
- Tenant users cannot view other users. Their access to User Permissions is limited to viewing their own user data and is found under the Tenant Access Permissions tab under the **Tools** drop down.

## Viewing CMS users

### Procedure

1. From the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

   The **Vector Access** and **VDN Access** menu items are listed if the Call Vectoring feature has been purchased.

2. In the **Operations** list, highlight **User Data**.
3. Select **OK**.

   Supervisor displays the User Permissions User Data window.

4. Using the menu bar, select **Edit** > **Clear All**.

   The information in all fields is removed. This includes the default information that appears when this window is first displayed.

5. There are two possible methods in searching for and displaying CMS user information:

   - **List all** - Selecting this item from the **Actions** menu will display a secondary window displaying all users whose settings match those in the fields of this window. 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** - Selecting this item from the **Actions** menu will take the information currently in all the fields of this dialog and query the database for users with matching settings. For example, having a `6` in the **Maximum user window count (1-12)** field with all other fields blank and selecting **Find one** will result in a search for all CMS users having a `6` for their **Maximum user window count**. If multiple users are found, each can be viewed by selecting the **Next** and **Previous** items under the **Actions** menu.

   When using the **Find one** command, partial text strings are not supported in the search. Therefore, to view the settings for a user ID, the complete name must be entered in the **User ID** field.

   If multiple users are found using the **Find one** action, the **Next** action will not become disabled at the last user, but instead cause the first user found to be displayed again.

# About modifying CMS users

## Before modifying CMS users

The following items should be read and understood before modifying users through the User Data window:

- If a user's login ACD is removed and the user tries to log into CMS , an acknowledgment tells the user either to contact the CMS administrator or to change the login ACD.
- Changing the login type for a user from **Administration** to **Normal** or vice versa does not change the permissions for that user ID. Permissions must be changed manually.
- The Login ID of a tenant user cannot be changed to a Normal user or an Administration user from the **User Permissions** screen. The login id of a tenant user can only be removed.
- 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.

## Permissions for modifying CMS users

Depending on the procedure to be performed, the following permissions must be observed:

- To display the User Data window and view user information, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify users through the User Data window, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.
- Tenant users can only view their own user data and cannot add, delete or modify themselves or any other users.

## Modifying CMS users

### Procedure

1. From the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

   The **Vector Access** and **VDN Access** menu items are listed if the Call Vectoring feature has been purchased.
2. In the **Operations** list, highlight **User Data**.
3. Select **OK**.

   Supervisor displays the User Permissions User Data window.
4. Clear all field default values by selecting **Edit** > **Clear All** from the menu bar.
5. In the **Login type (select only one)** field, select the login type for the user that will be modified.
6. Enter the name of the user to modify in the**User ID** field.
7. Select **Actions** > **Find one**.

   The settings for the specified user ID will populate their associated fields.

   If the user ID was not found, try selecting the other login type in the **Login type (select only one)** field.
8. Modify the settings for this user as needed.
9. After all necessary modifications have been made, select **Actions** > **Modify**.

   The settings for this user are updated and the status bar will display a `Successful` message.

# About deleting CMS users

## Before deleting CMS users

The following items should be read and understood before deleting users through the User Data window:

- Deleting a user ID added through the User Data window of CMS will remove that ID and its associated permissions from CMS and the operating system.
- Deleting a user who had custom reports, designer reports, or timetables, will result in an acknowledgment window asking if those items should be moved to your user ID. If they are moved and there is a conflict between the assigned names, a prompt window will appear allowing the moved items to be renamed. If not moved, any custom reports, designer reports, and timetables will be deleted along with the user ID.

## Permissions for deleting CMS users

Depending on the procedure to be performed, the following permissions must be observed:

- To display the User Data window and view user information, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify users through the User Data window, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions sub system.
- Tenant users can only view their own user data and cannot add, delete or modify themselves or any other users.

## Deleting CMS users

### Procedure

1. From the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

   The **Vector Access** and **VDN Access** menu items are listed if the Call Vectoring feature has been purchased.

2. In the **Operations** list, highlight **User Data**.
3. Select **OK**.

   Supervisor displays the User Permissions User Data window.

4. Using the menu bar, select **Edit** > **Clear All**.

   The information in all fields is removed. This includes the default information that appears when this window is first displayed.

5. In the **Login type (select only one)** field, select the login type of the user that will be deleted.
6. Enter the name of the user in the **User ID** field.

   If the user ID is not known, the other fields of this dialog box can be used to enter information that can return all users having matching information. For example, the **User Name** and **Room number** fields can have information entered in them.
7. After user-identifying data has been entered in the fields, select **Actions** > **Find one** from the menu bar.

   The status bar will return the number of matches found. Select **Actions** > **Next** to navigate to the next user in the list, if necessary.
8. When the dialog box displays the correct user, select **Actions** > **Delete** from the menu bar.

   The identified user is deleted from the system and the status bar displays a `Successful` message.

# ACD access

The ACD Access window is used to view and modify the user permissions for a selected real or pseudo ACD. This window can also be used to turn exception notification on or off for a selected ACD.

## Before using the ACD Access window

The following items should be read and understood before working with ACD access permissions:

- By default, a newly-created user is granted “read”, “write”, and “exceptions” permissions for all real and pseudo ACDs.
- A newly created tenant user is, by default, granted read, write, and exceptions permissions only to the login ACD of the tenant user. An administration user can allow the tenant user to gain access to another ACD if required.
- User permissions for ACD access are stored separately from the user ID created through the Before adding a CMS user on page 217 procedure. Because of this, user permissions for the ACD 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.
- If the “read” and “write” permissions are disabled for a user, then the user will not be able to access any splits/skills, trunk groups, vectors, or VDNs in that ACD. If “read” is enabled and “write” is disabled, the user will not be able to modify splits/skills, trunk groups, vectors, or VDNs in that ACD.

- If the permissions for the default login ACD of a user are removed, the user must have another login ACD assigned.
- A user must be created through the User Data window before any ACD permissions can be assigned.
- Users should only have the ACD permissions necessary to perform job duties. Assigning only those necessary user permissions will ensure the best system performance.
- In some instances, it may be necessary to restrict a user from viewing information on an ACD. To do so, either delete the permissions definition for the user or remove all permissions for the necessary ACDs. Deleting the ACD permissions definition for a user will save more disk space.

## Permissions for the ACD Access window

Depending on the procedure that you want to perform, you need the following permissions:

- To view user permission settings in the ACD Access window, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify user permission settings in the ACD Access window, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.

## Adding ACD access

### About this task

This section provides the procedure for adding ACD access permissions for a CMS user. Since a user permission definition for ACD access is created by default when the user ID is created, this procedure is only necessary if that permission definition has been deleted.

To add a user permission definition for an ACD:

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight ACD Access.
3. Select **OK**.

   Supervisor displays the User Permissions ACD Access window.

4. In the **User ID** field, enter the ID of the user for whom to create an ACD permissions definition.

   This field is required.

5. In the **ACD** field, enter the names or numbers for one or more ACDs that this user will be able to access (real, pseudo, or group).

   Multiple values in this field must be separated with a semicolon (;).

6. Place a check mark in the permissions that will be assigned to this user:
   - **Read** - User can view but not modify information for the specified ACDs.
   - **Write** - User can modify information on the specified ACDs. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified ACDs.
7. After assigning the necessary permissions, select **Actions** > **Add** from the menu bar.

   The ACD permissions for this user are saved.

   It is possible to add permission definitions for multiple users at one time. To do so, enter multiple CMS users in the **User ID** field and separate them with semicolons (;). The ACDs specified in the **ACDs** field and the selected permissions are then created for these user IDs when the **Add** action is performed.

# Viewing ACD access

## About this task

This section provides the procedure for viewing the ACD access permissions for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.
2. In the **Operations** list, highlight ACD Access.
3. Select **OK**.

   Supervisor displays the User Permissions ACD Access window.
4. In the **User ID** field, enter the ID of the CMS user for which the permissions for ACDs are to be viewed.

   This field is required.

   When searching for the user permissions definitions on specific ACDs, these ACDs can be entered in the **ACDs** field. Multiple entries must be separated by a semicolon (;).
5. From the menu bar, select **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.

   If more than one ACD is returned, use the **Next** action to view the permission definitions for the other ACDs.

# Listing all ACD access

## About this task

This section provides the procedure for listing the ACD permission definitions for all CMS users.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight ACD Access.
3. Select **OK**.

   Supervisor displays the User Permissions ACD Access window.

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

   All user permission definitions are displayed with their corresponding ACDs. Only those ACDs for which you have “read” permission will be shown.

# Modifying ACD access

## About this task

This section provides the procedure for modifying the ACD permission definitions for a CMS user.

If all ACD permissions are to be denied for a user, deleting the permissions definition for the user will save more disk space and accomplish the same goal.

**Important:**

If the “read” permissions is denied for the ACD that the user logs into, that user will no longer be able to log on. A new default login ACD must be set for the user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight ACD Access.
3. Select **OK**.

   Supervisor displays the User Permissions ACD Access window.

4. In the **User ID** field, enter the ID of the CMS user for which the permissions for ACDs are to be modified.

   When searching for the user permissions definitions on specific ACDs, these ACDs can be entered in the **ACDs** field. Multiple entries must be separated by a semicolon (;). These entries can include real ACDs, pseudo-ACDs, or ACD Groups.

5. From the menu bar, select **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.

   If more than one ACD is returned, use the **Next** action to view the permission definitions for the other ACDs.

6. Once the correct permission definition is displayed in the window, change the permissions by adding or removing check marks in the **Read**, **Write**, or **Exceptions** check boxes.
7. Once the permissions have been changed to the necessary settings, select **Actions** > **Modify** from the menu bar.

   The user permissions definition for this ACD is updated and the status bar displays a `Successful` message.

# Deleting ACD access

## About this task

This section provides the procedure for deleting the ACD permission definition for a CMS user.

**Important:**

If the user permissions definition is deleted for the ACD that the user logs into, that user will no longer be able to log on. A new default login ACD must be set for the user. Deleting the permissions definition does not restrict the permissions for the user, but actually deletes the user from the specified ACD. This action does not affect the user ID created through the User Data feature.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight ACD Access.
3. Select **OK**.

   Supervisor displays the User Permissions ACD Access window.

4. In the **User ID** field, enter the ID of the CMS user for which the permissions for ACDs are to be modified.

   When searching for the user permissions definitions on specific ACDs, these ACDs can be entered in the **ACDs** field. Multiple entries must be separated by a semicolon (;). These entries can include real ACDs, pseudo-ACDs, or ACD Groups.

5. From the menu bar, select **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.

If more than one ACD is returned, use the **Next** action to view the permission definitions for the other ACDs.

6. Once the correct permission definition is displayed in the window, select **Actions** > **Delete** from the menu bar.

   The ACD permissions definition for this user is deleted and the status bar displays a `Successful` message.

7. Once the permissions have been changed to the necessary settings, select **Actions** > **Modify** from the menu bar.

   The user permissions definition for this ACD is updated and the status bar displays a `Successful` message.

# Feature access

The Feature Access window is used to view and modify the permissions available to a CMS user ID for the following features:

- Agent Administration
- Call Center Administration
- Custom Reports
- Dictionary
- Exceptions
- Forecast
- Maintenance
- Reports
- CMS System Setup
- Timetable
- User Permissions
- UNIX® System
- Tenant

The permissions assigned to a user will affect the appearance of the Supervisor Controller window. For example, a user without permissions for the Dictionary feature will not have a corresponding toolbar button on the Controller window.

## Before using the Feature Access window

The following items should be read and understood before working with Feature Access permissions:

- A new Tenant feature is added to the Feature Access window. The administrator has both read and write permissions to the Tenant feature by default. A normal user does not have read and write permissions to the Tenant feature by default. A tenant user has restricted feature access. The tenant user cannot turn on the Forecast, Maintenance, and System Setup features and does not have access to the UNIX shell.
- 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 the administrator or services personnel.
- If the Feature Access permissions for a user are modified, the changes do not take effect until the user logs off and back on again.
- A user ID must be created through the User Data feature before that user can have Feature Access permissions assigned.
- Default Feature Access permissions are assigned when a user ID is created. The Administrator type of user ID has permissions for all features. The Normal type of user ID is given “read” permissions for all features except User Permissions, System Setup, Call Center Administration, and Forecasting. User ID types are set through the User Data feature.
- Assigning a user the “write” permission for the User Permissions feature allows that user to change permissions for all users.
- A user ID cannot have “write” permissions without also having “read” permissions.
- If a user does not have “read” permission for a feature, that feature will not be displayed as a toolbar button or menu item in the Supervisor Controller window.
- Assigning only the necessary access permissions ensures the best system performance.

## Permissions for the Feature Access window

Depending on the procedure that you want to perform, you need the following permissions:

- To view the Feature Access window, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify settings through the Feature Access window, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.

# Viewing Feature Access user permissions

## About this task

This section provides the procedure for viewing Feature Access permissions for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Feature Access**.
3. In the **ACD** field, select the ACD or ACD Group on which you want to view user permissions for its feature set.
4. Select **OK**.

   Supervisor displays the User Permissions Feature Access window.

5. In the **User ID** field, enter the ID of an existing CMS user.

   This field can accept more than one user ID. Multiple IDs must be separated by a semicolon (;).

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

   Supervisor will display the permissions for the first user found. If multiple user IDs were entered, the status bar will display the number of matches found.

   If multiple matches were found, use the **Actions** > **Next** command to navigate through the user IDs and their permissions.

# Listing all Feature Access user permissions

## About this task

This section provides the procedure for listing the Feature Access permissions for all CMS users on an ACD or ACD Group.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Feature Access**.
3. In the **ACD** field, select the ACD or ACD Group on which you want to view user permissions for its feature set.
4. Select **OK**.

   Supervisor displays the User Permissions Feature Access window.

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

   Supervisor displays a secondary window listing all users and their associated feature permissions.

## Modifying Feature Access user permissions

### About this task

This section provides the procedure for modifying Feature Access permissions for a CMS user on an ACD or ACD Group.

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Feature Access**.
3. In the **ACD** field, select the ACD or ACD Group on which the user permissions for its feature set will be modified.
4. Select **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, select **Actions** > **Find one**.

   Supervisor will display the permissions for the user.

   A check mark in a check box signifies that the associated feature permission is enabled for the user.

7. Change the **Read** and **Write** permissions as necessary by placing or removing check marks in the check boxes for each feature.
8. When the necessary changes have been made to the user feature permissions, select **Actions** > **Modify** from the menu bar.

   The user permissions definition for this ACD is updated and the status bar displays a `Successful` message.

# Main Menu Addition Access

The Main Menu Addition Access feature is used to control which custom menu items appear on the CMS Main Menu for a user. Custom menu items are created through the Main Menu Addition feature which is located in the System Setup screen from the CMS ASCII interface.

These menu items cannot be created through Supervisor.

The custom menu items display on the CMS Main Menu which is seen through either Terminal Emulator, a telnet session to the CMS server, or the CMS console. The custom menu items do not display in the Supervisor Controller window.

## Before using Main Menu Addition Access

The following items should be read and understood before working with Main Menu Addition Access:

- If the assigned Main Menu Addition Access permission for a user is disabled, the custom menu item will not be displayed on the CMS Main Menu for that user.
- If a the Main Menu Addition Access permission is changed for a user, those changes will not take effect until the user logs out and back in again.
- A user ID must be created through the User Data feature before assignments or changes can be made to that user ID through the Main Menu Addition Access feature.
- Main Menu additions must be created through System Setup before these custom menu items can be assigned to users.

## Permissions for Main Menu Addition Access

Depending on the procedure that you want to perform, you need the following permissions:

- To view Main Menu Addition Access user configurations, the user ID used to log in to CMS requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify Main Menu Addition Access user configurations, the user ID used to log in to CMS requires “write” permission for the User Permissions subsystem.

## Viewing Main Menu Addition Access

### About this task

This section provides the procedure for viewing CMS user configurations for Main Menu Addition Access.

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Main Menu Addition Access**.
3. Select **OK**.

   Supervisor displays the User Permissions Main Menu Addition Access window.

4. In the **User ID** field, enter a CMS user ID that has been previously defined through the User Data feature.

   This field can accept the entry of multiple users at one time. Multiple entries must be separated by a semicolon (;).

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

   Supervisor retrieves the Main Menu Addition Access information for the specified CMS user ID and displays this information in the remaining fields.

   If multiple users were specified in the **User ID** field, the other users and their configurations can be seen by using **Actions** > **Next** from the menu bar.

# Listing all Main Menu Addition Access

## About this task

This section provides the procedure for listing all Main Menu Addition Access configurations that have been assigned to CMS users.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Main Menu Addition Access**.
3. Select **OK**.

   Supervisor displays the User Permissions Main Menu Addition Access window.

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

   Supervisor displays a secondary window listing all CMS users that have custom menu items assigned and the permissions for those custom menu items.

# Assigning or modifying Main Menu Addition Access

## About this task

This section provides the procedure for assigning or modifying a custom Main Menu item for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Main Menu Addition Access**.
3. Select **OK**.

Supervisor displays the User Permissions Main Menu Addition Access window.

4. In the **User ID** field, enter a CMS user ID that has been previously defined through the User Data feature.

   This field can accept the entry of multiple users at one time. Multiple entries must be separated by a semicolon (;).

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

   Supervisor retrieves the Main Menu Addition Access information for the specified CMS user ID and displays this information in the remaining fields.

   If multiple users were specified in the **User ID** field, the other users and their configurations can be seen by using **Actions** > **Next** from the menu bar.

6. In the **Addition** field, enter the custom menu item to be assigned or modified for the specified CMS user.

7. In the **Access** check box, place a check mark to enable this custom menu item or remove the check mark to disable this menu item for the specified CMS user.

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

   The user configuration is updated and the status bar displays a `Successful` message.

   Only the current CMS displayed in the **User ID** field is modified. If other user IDs are available through using the **Next** command, each one will require the **Modify** action for assignments to be applied.

# About Tenant Access

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 UNIX system login identification.
- **Tenant number** must be between 1 and 250.
- **Read**, **Write**, or **Exceptions** fields only allow **y** or **n**.

## Tenant Access window

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 `Already exists` 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 `Does not exist` 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 `Does not exist` 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. |

*Table continues…*

| Field | Description |
|---|---|
| **Previous** | After doing a **Find one** search resulting in more than one match, this selection displays the previous match. |

# Split/Skill access

This section provides the procedures for working with user permissions regarding splits/skills.

For users providing administration for splits/skills or running split/skill reports, it is necessary for them to have the proper split/skill permissions to perform their job functions.

Split/skill exceptions notification is also configured through this interface. Users who are given the “Exceptions” permission will be notified of split/skill exceptions when they occur.

## Before using split/skill access

The following items should be read and understood before working with split/skill permissions:

- The tenant user cannot be given permissions to splits/skills unless the splits/skills are assigned to the tenant to which the tenant user is assigned.
- The permissions for the splits/skills cannot be greater than the permissions given to the tenant to which the splits/skills belong.
- The tenant user has the permissions for the tenant to which the splits/skills belong.
- A CMS user ID must be created through the User Data feature before split/skill permissions can be assigned.
- When a new user ID is created through the User Data feature, split/skill permission definitions for that user are not created. This is done to conserve disk space. When a split/skill permissions definition does not exist for a user ID, CMS will deny “read” and “write” access to splits/skills.
- A user ID must first have permissions for the ACD on which the split/skill resides before split/skill permissions can be assigned. If a user ID is assigned split/skill permissions and does not have the appropriate ACD permissions, Supervisor displays an error message.
- A user ID cannot be assigned the “write” permission without first having the “read” permission.
- Assigning only those permissions that are necessary for each user ID ensures the best system performance.

# Permissions for split/skill access

Depending on the procedure that you want to perform, you need the following permissions:

- To view split/skill user permissions, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify split/skill user permissions, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.

# About adding split/skill user permissions

This section provides the procedure for adding a split/skill permissions definition for a CMS user.

## Before adding split/skill user permissions

The following items should be read and understood before adding a split/skill permissions definition for a CMS user:

- If a user does not have corresponding ACD permissions for the permissions set for them on the split/skill, Supervisor displays an error message.
- When the permissions definition for a user is created, the split/skill permissions do not take effect until the user logs off and back on again.

## Adding split/skill user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Split/Skill Access**.
3. In the **ACD** field, select the ACD or ACD Group containing the split/skill for which the user will be given permissions.
4. Select **OK**.

   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 name or number of the split/skill for which the user will have permissions assigned.

   This field can accept multiple splits/skills. Multiple entries must be separated by a semicolon (;).

   Multiple splits/skills can be entered by using a range, for example, `1-256`.

7. Place a check mark in the permissions that will be assigned to this user:
   - **Read** - User can view but not modify information for the specified splits/skills including reports.
   - **Write** - User can modify information on the specified splits/skills. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified splits/skills.

   Only the split/skill exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.
8. After assigning the necessary permissions, select **Actions** > **Add** from the menu bar.

   The split/skill permissions for this user are saved.

   It is possible to add permission definitions for multiple splits/skills at one time. To do so, enter multiple splits/skills in the **Splits/Skills** field and separate them with semicolons (;).

# About viewing split/skill user permissions

This section provides the procedure for viewing the split/skill permissions definition for a CMS user.

## Before viewing split/skill user permissions

The following items should be read and understood before viewing split/skill permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions Split/Skill Access window.

## Viewing split/skill user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.
2. In the **Operations** list, highlight **Split/Skill Access**.
3. In the **ACD** field, select the ACD or ACD Group containing the split/skill for which all permission definitions will be shown.
4. Select **OK**.

   Supervisor displays the User Permissions Split/Skill Access window.
5. In the **User ID** field, enter the name of the user for which the split/skill permissions definition is to be viewed.

6. If the specific split/skill to view for this user is known, enter the name or number of the split/skill in the **Splits/Skills** field. To have all splits/skills returned for this user ID, leave this field blank.

   This field can accept multiple splits/skills. Multiple entries must be separated by a semicolon (;).

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

   Supervisor queries the database and displays the number of matches found for this user ID in the status bar.

# About listing all split/skill user permissions

This section provides the procedure for listing all of the user permission definitions for a split/skill.

## Listing all split/skill user permissions

### Before you begin

The following items should be read and understood before listing all split/skill permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions Split/Skill Access window.

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Split/Skill Access**.
3. In the **ACD** field, select the ACD or ACD Group containing the split/skill for which all permission definitions will be shown.
4. Select **OK**.

   Supervisor displays the User Permissions Split/Skill Access window.

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

   Supervisor displays a secondary window listing all user permissions for splits/skills on the specified ACD.

   A filter can be created when listing all user split/skill permission definitions. This filter is based on any information contained in the **User ID** and **Splits/Skills** fields on this dialog box when the **List all** action is performed.

   For example, to view all of the user permission definitions for skill 26, enter `26` in the **Splits/Skills** field before performing the **List all** action. This will cause only the user permission definitions for skill 26 to display. If more information is entered into the other fields of this dialog box, the results will be more restricted. If information for the user ID, splits/skills, and

permissions are entered, the **List all** command will only return those permission definitions which match all of the information.

# About modifying split/skill user permissions

This section provides the procedure for modifying the split/skill permissions definition for a CMS user.

## Before modifying split/skill user permissions

The following items should be read and understood before modifying split/skill permissions:

- When the permissions definition for a user is modified, the change does not take effect until the user logs off and back on again.
- If a user does not have corresponding ACD permissions for the permissions set for them on the split/skill, Supervisor displays an error message.
- The wildcard characters “*” and “?” cannot be used in the User Permissions Split/Skill Access window.

## Modifying split/skill user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Split/Skill Access**.
3. In the **ACD** field, select the ACD or ACD Group containing the split/skill for which the user has a permissions definition.
4. Select **OK**.

   Supervisor displays the User Permissions Split/Skill Access window.

5. In the **User ID** field, enter the name of the user for which the split/skill permissions definition is to be modified.
6. If the specific split/skill to view for this user is known, enter the name or number of the split/skill in the **Splits/Skills** field. For all splits/skills to be returned for this user ID, leave this field blank.

   This field can accept multiple splits/skills. Multiple entries must be separated by a semicolon (;).

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

   Supervisor queries the database and displays the number of matches found for this user ID in the status bar.

   If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct split/skill.

8. Change the permissions for the user on this split/skill as needed:
   - **Read** - User can view but not modify information for the specified splits/skills including reports.
   - **Write** - User can modify information on the specified splits/skills. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified splits/skills.

     **Important:**

     If all permissions are to be removed for this user ID, it saves more server disk space to delete this permission definition rather than disabling all permissions. See Deleting split/skill user permissions on page 242 for more information.

   Only the split/skill exceptions made active through the Exceptions feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.
9. After the necessary permission changes have been completed, select **Actions** > **Modify** from the menu bar.

   The permissions definition for this user ID and split/skill is updated. The status bar displays a `Successful` message.

# Deleting split/skill user permissions

## About this task

This section provides the procedure for deleting the split/skill permissions definition for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.
2. In the **Operations** list, highlight **Split/Skill Access**.
3. In the **ACD** field, select the ACD or ACD Group containing the split/skill for which the user has a permissions definition.
4. Select **OK**.

   Supervisor displays the User Permissions Split/Skill Access window.
5. In the **User ID** field, enter the name of the user for which the split/skill permissions definition is to be deleted.
6. If the specific split/skill to view for this user is known, enter the name or number of the split/skill in the **Splits/Skills** field. To return all split/skills for this user ID, leave this field blank.
7. From the menu bar, select **Actions** > **Find one**.

Supervisor queries the database and displays the number of matches found for this user ID in the status bar.

If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct split/skill.

8. From the menu bar, select **Actions** > **Delete**.

   Supervisor deletes the permissions definition for this user ID and the associated split/skill. The status bar displays a `Successful` message upon completion of the action.

   This action does not delete the permission definitions for all splits/skills for this user, only the one displayed in the **Splits/Skills** field.

# Trunk group access

Trunk group permissions allow users to view data for trunk group reports, view trunk group configuration information, and change trunk group configurations. The User Permissions Trunk Group Access window is also used to configure which users receive exception notifications.

## Before using the Trunk Group Access window

The following items should be read and understood before working with trunk group permissions:

- The tenant user cannot be given permissions to trunk groups unless the trunk groups are assigned to the tenant to which the tenant user is assigned.
- The tenant user must have the permissions for the tenant to which the trunk groups belong.
- The permissions for the trunk groups cannot be greater than the permissions given to the tenant to which the trunk groups belong.
- A CMS user ID must be created through the User Data feature before it can be assigned trunk group permissions.
- When a new user ID is created through the User Data feature, trunk group permission definitions for that user are not created. This is done to conserve disk space. When a trunk group permissions definition does not exist for a user ID, CMS will deny “read” and “write” access to trunk groups.
- A user ID must first have permissions for the ACD on which the trunk group resides before trunk group permissions can be assigned. If a user ID is assigned trunk group permissions and does not have the appropriate ACD permissions, Supervisor displays an error message.
- A user ID cannot be assigned the “write” permission without first having the “read” permission.
- Assigning only those permissions that are necessary for each user ID ensures the best system performance.

# Permissions for the Trunk Group Access window

Depending on the procedure that you want to perform, you need the following permissions:

- To view trunk group user permissions, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify trunk group user permissions, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.

# About adding trunk group user permissions

This section provides the procedure for adding a trunk group permissions definition for a CMS user.

## Before adding trunk group user permissions

The following items should be read and understood before adding a trunk group permissions definition for a CMS user:

- If a user does not have corresponding ACD permissions for the permissions set for them on the trunk group, Supervisor displays an error message.
- When the permissions definition for a user is created, the trunk group permissions do not take effect until the user logs off and back on again.

## Adding trunk group user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Trunk Group Access**.
3. In the **ACD** field, select the ACD containing the trunk group for which the user will be given permissions.
4. Select **OK**.

   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 name or number of the trunk group for which the user will have permissions assigned.

   This field can accept multiple trunk groups. Multiple entries must be separated by a semicolon (;).

7. Place a check mark in the permissions that will be assigned to this user:
   - **Read** - User can view but not modify information for the specified trunk groups including reports.
   - **Write** - User can modify information on the specified trunk groups. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified trunk groups.

   Only the trunk group exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.
8. After assigning the necessary permissions, select **Actions** > **Add** from the menu bar.

   The trunk group permissions for this user are saved.

   It is possible to add permission definitions for multiple trunk groups at one time. To do so, enter multiple trunk groups in the **Trunk Groups** field and separate them with semicolons (;).

# About viewing trunk group user permissions

This section provides the procedure for viewing the trunk group permissions definition for a CMS user.

## Before viewing trunk group user permissions

The following items should be read and understood before viewing trunk group permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions Trunk Group Access window.

## Viewing trunk group user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.
2. In the **Operations** list, highlight **Trunk Group Access**.
3. In the **ACD** field, select the ACD containing the trunk group for which the user has a permissions definition.
4. Select **OK**.

   Supervisor displays the User Permissions Trunk Group Access window.
5. In the **User ID** field, enter the name of the user for which the trunk group permissions definition is to be viewed.

6. If the specific trunk group to view for this user is known, enter the name or number of the trunk group in the **Trunk Groups** field. To have all trunk groups returned for this user ID, leave this field blank.

   This field can accept multiple trunk groups. Multiple entries must be separated by a semicolon (;).

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

   The database is queried and the number of matches found for this user ID displays in the status bar.

# About listing all trunk group user permissions

This section provides the procedure for listing all of the user permission definitions for a trunk group.

## Before listing all trunk group user permissions

The following items should be read and understood before listing all trunk group permission definitions for users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions Trunk Group Access window.

## Listing all trunk group user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Trunk Group Access**.

3. In the **ACD** field, select the ACD containing the trunk group for which all permission definitions will be shown.

4. Select **OK**.

   Supervisor displays the User Permissions Trunk Group Access window.

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

   Supervisor displays a secondary window listing all user permissions for trunk groups on the specified ACD.

   A filter can be created when listing all user trunk group permission definitions. This filter is based on any information contained in the **User ID** and **Trunk Groups** fields on this dialog box when the **List all** action is performed.

   For example, to view all of the user permission definitions for trunk group 4, enter `4` in the **Trunk Groups** field before performing the List all action. This will cause only the user permission definitions for trunk group 4 to display. If more information is entered into the other fields of this dialog box, the results will be more restricted. If information for the user ID,

trunk groups, and permissions are entered, the **List all** command will only return those permission definitions which match all of the information.

# About modifying trunk group user permissions

This section provides the procedure for modifying the trunk group permissions definition for a CMS user.

## Before modifying trunk group user permissions

The following items should be read and understood before modifying trunk group permissions:

- When the permissions definition for a user is modified, the change does not take effect until the user logs off and back on again.
- If a user does not have corresponding ACD permissions for the permissions set for them on the trunk group, Supervisor displays an error message.
- The wildcard characters “*” and “?” cannot be used in the User Permissions Trunk Group Access window.

## Modifying trunk group user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Trunk Group Access**.
3. In the **ACD** field, select the ACD containing the trunk group for which the user has a permissions definition.
4. Select **OK**.

   Supervisor displays the User Permissions Trunk Group Access window.

5. In the **User ID** field, enter the name of the user for which the trunk group permissions definition is to be modified.
6. If the specific trunk group to view for this user is known, enter the name or number of the trunk group in the **Trunk Groups** field. To have all trunk groups returned for this user ID, leave this field blank.

   This field can accept multiple trunk groups. Multiple entries must be separated by a semicolon (;).

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

   The database is queried and the number of matches found for this user ID displays in the status bar. The first match found populates the fields of this dialog box.

   If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct trunk group.

8. Change the permissions for the user on this trunk group as needed:
   - **Read** - User can view but not modify information for the specified trunk groups including reports.
   - **Write** - User can modify information on the specified trunk groups. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified trunk groups.

     **Important:**

     If all permissions are to be removed for this user ID, it saves more server disk space to delete this permission definition rather than disabling all permissions.

   Only the trunk group exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.
9. After the necessary permission changes have been completed, select **Actions** > **Modify** from the menu bar.

   The permissions definition for this user ID and trunk group is updated. The status bar displays a `Successful` message upon completion.

# Deleting trunk group user permissions

## About this task

This section provides the procedure for deleting the trunk group permissions definition for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.
2. In the **Operations** list, highlight **Trunk Group Access**.
3. In the **ACD** field, select the ACD containing the trunk group for which the user has a permissions definition.
4. Select **OK**.

   Supervisor displays the User Permissions Trunk Group Access window.
5. In the **User ID** field, enter the name of the user for which the trunk group permissions definition is to be deleted.
6. If the specific trunk group to view for this user is known, enter the name or number of the trunk group in the **Trunk Groups** field. To return all trunk groups for this user ID, leave this field blank.
7. From the menu bar, select **Actions** > **Find one**.

The database is queried and the number of matches found for this user ID displays in the status bar. The first match found populates the fields of this dialog box.

If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct trunk group.

8. From the menu bar, select **Actions** > **Delete**.

   The permissions definition for this user ID and the associated trunk group is deleted. The status bar displays a `Successful` message upon completion of the action.

   This action does not delete the permission definitions for all trunk groups for this user, only the one displayed in the **Trunk Groups** field.

# Vector access

Vector permissions allow users to view data for vector reports, view vector configuration information, and change vector configurations. The User Permissions Vector Access window is also used to configure which users receive exception notifications.

This feature is not available if the Vectoring product has not been purchased and installed.

## Before using vector access

The following items should be read and understood before working with vector permissions:

- The tenant user cannot be given permissions to vectors unless the vectors are assigned to the tenant to which the tenant user is assigned.
- The tenant user must have the permissions for the tenant to which the vectors belong.
- The permissions for the vectors cannot be greater than the permissions given to the tenant to which the vectors belong.
- A CMS user ID must be created through the User Data feature before it can be assigned vector permissions.
- When a new user ID is created through the User Data feature, vector permission definitions for that user are not created. This is done to conserve disk space. When a vector permissions definition does not exist for a user ID, CMS will deny “read” and “write” access to vectors.
- A user ID must first have permissions for the ACD on which the vector resides before vector permissions can be assigned. If a user ID is assigned vector permissions and does not have the appropriate ACD permissions, Supervisor displays an error message.
- A user ID cannot be assigned the “write” permission without first having the “read” permission.
- Assigning only those permissions that are necessary for each user ID ensures the best system performance.

- A user must be given the “Exceptions” permission in order to be notified of vector exceptions that occur.

# Permissions for vector access

Depending on the procedure that you want to perform, you need the following permissions:

- To view vector user permissions, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify vector user permissions, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.

# About adding vector user permissions

This section provides the procedure for adding a vector permissions definition for a CMS user.

## Before adding vector user permissions

The following items should be read and understood before adding a vector permissions definition for a CMS user:

- If a user does not have corresponding ACD permissions for the permissions set for them on the vector, Supervisor displays an error message.
- When the permissions definition for a user is created, the vector permissions do not take effect until the user logs off and back on again.

## Adding vector user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Vector Access**.
3. In the **ACD** field, select the ACD containing the vector for which the user will be given permissions.
4. Select **OK**.

   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 number of the vector for which the user will have permissions assigned.

   This field can accept multiple vectors. Multiple entries must be separated by a semicolon (;).

7. Place a check mark in the permissions that will be assigned to this user:
   - **Read** - User can view but not modify information for the specified vectors including reports.
   - **Write** - User can modify information on the specified vectors. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified vectors.

   Only the vector exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.
8. After assigning the necessary permissions, select **Actions** > **Add** from the menu bar.

   The vector permissions for this user are saved.

   It is possible to add permission definitions for multiple vectors at one time. To do so, enter multiple vectors in the **Vectors** field and separate them with semicolons (;).

# About viewing vector user permissions

This section provides the procedure for viewing the vector permissions definition for a CMS user.

## Before viewing vector user permissions

The following items should be read and understood before viewing vector permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions Vector Access window.

## Viewing vector user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.
2. In the **Operations** list, highlight **Vector Access**.
3. In the **ACD** field, select the ACD containing the vector for which the user has a permissions definition.
4. Select **OK**.

   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. If the specific vector to view for this user is known, enter the name or number of the vector in the **Vectors** field. To have all vectors returned for this user ID, leave this field blank.

This field can accept multiple vectors. Multiple entries must be separated by a semicolon (;).

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

   The database is queried and the number of matches found for this user ID displays in the status bar.

# About listing all vector user permissions

This section provides the procedure for listing all of the user permission definitions for a vector.

## Before listing all vector user permissions

The following items should be read and understood before listing all vector permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions Vector Access window.

## Listing all vector user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Vector Access**.
3. In the **ACD** field, select the ACD containing the vector for which all permission definitions will be shown.
4. Select **OK**.

   Supervisor displays the User Permissions Vector Access window.

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

   Supervisor displays a secondary window listing all user permissions for vectors on the specified ACD.

   A filter can be created when listing all user vector permission definitions. This filter is based on any information contained in the fields on this dialog box when the **List all** action is performed.

   For example, to view all of the user permission definitions for vector 1, enter `1` in the **Vectors** field before performing the **List all** action. This will cause only the user permission definitions for vector 1 to display. If more information is entered into the other fields of this dialog box, the results will be more restricted. If information for the user ID, vectors, and permissions are entered, the **List all** command will only return those permission definitions which match all of the information.

# About modifying vector user permissions

This section provides the procedure for modifying the vector permissions definition for a CMS user.

## Before modifying vector user permissions

The following items should be read and understood before modifying vector permissions:

- When the permissions definition for a user is modified, the change does not take effect until the user logs off and back on again.
- If a user does not have corresponding ACD permissions for the permissions set for them on the vector, Supervisor displays an error message.
- The wildcard characters “*” and “?” cannot be used in the User Permissions Vector Access window.

## Modifying vector user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Vector Access**.
3. In the **ACD** field, select the ACD containing the vector for which the user has a permissions definition.
4. Select **OK**.

   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 modified.
6. If the specific vector to view for this user is known, enter the name or number of the vector in the **Vectors** field.

   To have all vectors returned for this user ID, leave this field blank. This field can accept multiple vectors. Multiple entries must be separated by a semicolon (;).

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

   The database is queried and the number of matches found for this user ID displays in the status bar. The first match found populates the fields of this dialog box.

   If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct vector.

8. Change the permissions for the user on this vector as needed:

   - **Read** - User can view but not modify information for the specified vectors including reports.

- **Write** - User can modify information on the specified vectors. This permission requires that the user also have the “read” permission.
- **Exceptions** - User will receive notification of exceptions occurring on the specified vectors.

**Important:**

If all permissions are to be removed for this user ID, it saves more server disk space to delete this permission definition rather than disabling all permissions.

Only the vector exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.

9. After the necessary permission changes have been completed, select **Actions** > **Modify** from the menu bar.

   The permissions definition for this user ID and vector is updated. The status bar displays a `Successful` message upon completion.

# Deleting vector user permissions

## About this task

This section provides the procedure for deleting the vector permissions definition for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **Vector Access**.
3. In the **ACD** field, select the ACD containing the vector for which the user has a permissions definition.
4. Select **OK**.

   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 deleted.
6. If the specific vector to view for this user is known, enter the name or number of the vector in the **Vectors** field. To return all vectors for this user ID, leave this field blank.
7. From the menu bar, select **Actions** > **Find one**.

   The database is queried and the number of matches found for this user ID displays in the status bar. The first match found populates the fields of this dialog box.

   If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct vector.

8. From the menu bar, select **Actions** > **Delete**.

   The permissions definition for this user ID and the associated vector is deleted. The status bar displays a successful message upon completion of the action.

   This action does not delete the permission definitions for all vectors for this user, only the one displayed in the **Vectors** field.

# VDN access

Vector Directory Number (VDN) permissions allow users to view data for VDN reports, view VDN configuration information, and change VDN configurations. The User Permissions VDN Access window is also used to configure which users receive exception notifications.

This feature is not available if the Vectoring product has not been purchased, installed, and enabled on the corresponding ACD.

## Before using VDN access

The following items should be read and understood before working with VDN permissions:

- The tenant user cannot be given permissions to VDNs unless the VDNs are assigned to the tenant to which the tenant user is assigned.
- The tenant user must have the permissions for the tenant to which the VDNs belong.
- The permissions for the VDNs cannot be greater than the permissions given to the tenant to which the VDNs belong.
- A CMS user ID must be created through the User Data feature before it can be assigned VDN permissions.
- When a new user ID is created through the User Data feature, VDN permission definitions for that user are not created. This is done to conserve disk space. When a VDN permissions definition does not exist for a user ID, CMS denies “read” and “write” access to VDNs.
- A user ID must first have permissions for the ACD on which the VDN resides before VDN permissions can be assigned. If a user ID is assigned VDN permissions and does not have the appropriate ACD permissions, Supervisor an error message.
- A user ID cannot be assigned the “write” permission without first having the “read” permission.
- Assigning only those permissions that are necessary for each user ID ensures the best system performance.
- A user must be given the “exceptions” permission in order to be notified of VDN exceptions that occur.

# Permissions for VDN access

Depending on the procedure that you want to perform, you need the following permissions:

- To view VDN user permissions, the user ID used to log in to this Supervisor session requires “read” permission for the User Permissions subsystem.
- To add, delete, or modify VDN user permissions, the user ID used to log in to this Supervisor session requires “write” permission for the User Permissions subsystem.

# About adding VDN user permissions

This section provides the procedure for adding a VDN permissions definition for a CMS user.

## Before adding VDN user permissions

The following items should be read and understood before adding a VDN permissions definition for a CMS user:

- If a user does not have corresponding ACD permissions for the permissions set for them on the VDN, Supervisor displays an error message.
- When the permissions definition for a user is created, the VDN permissions do not take effect until the user logs off and back on again.

## Adding VDN user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **VDN Access**.
3. In the **ACD** field, select the ACD containing the VDN for which the user will be given permissions.
4. Select **OK** .

   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 name or number of the VDN for which the user will have permissions assigned.

   This field can accept multiple VDNs. Multiple entries must be separated by a semicolon (;).

7. Place a check mark in the permissions that will be assigned to this user:
   - **Read** - User can view but not modify information for the specified VDNs including reports.
   - **Write** - User can modify information on the specified VDNs. This permission requires that the user also have the “read” permission.

- **Exceptions** - User will receive notification of exceptions occurring on the specified VDNs.

  Only the VDN exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.

8. After assigning the necessary permissions, select **Actions** > **Add** from the menu bar.

   The VDN permissions for this user are saved.

   It is possible to add permission definitions for multiple VDNs at one time. To do so, enter multiple VDNs in the **VDNs** field and separate them with semicolons (;).

# About viewing VDN user permissions

This section provides the procedure for viewing the VDN permissions definition for a CMS user.

## Before viewing VDN user permissions

The following items should be read and understood before viewing VDN permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions VDN Access window.

## Viewing VDN user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **VDN Access**.
3. In the **ACD** field, select the ACD containing the VDN for which the user has a permissions definition.
4. Select **OK** .

   Supervisor displays the User Permissions VDN Access window.

5. In the **User ID** field, enter the name of the user for which the VDN permissions definition is to be viewed.
6. If the specific VDN to view for this user is known, enter the name or number of the VDN in the **VDNs** field. To have all VDNs returned for this user ID, leave this field blank.

   This field can accept multiple VDNs. Multiple entries must be separated by a semicolon (;).

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

   The database is queried and the number of matches found for this user ID is displayed in the status bar.

# About listing all VDN user permissions

This section provides the procedure for listing all of the user permission definitions for a VDN.

## Before listing all VDN user permissions

The following items should be read and understood before listing all VDN permission definitions for CMS users:

- The wildcard characters “*” and “?” cannot be used in the User Permissions VDN Access window.

## Listing all VDN user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **VDN Access**.
3. In the **ACD** field, select the ACD containing the VDN for which all permission definitions will be shown.
4. Select **OK** .

   Supervisor displays the User Permissions VDN Access window.

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

   Supervisor displays a secondary window listing all user permissions for VDNs on the specified ACD.

   A filter can be created when listing all user VDN permission definitions. This filter is based on any information contained in the **User ID** and **VDNs** fields on this dialog box when the **List all** action is performed.

   For example, to view all of the user permission definitions for VDN 10, enter `10` in the **VDNs** field before performing the **List all** action. This will cause only the user permission definitions for VDN 10 to display. If more information is entered into the other fields of this dialog box, the results will be more restricted. If information for the user ID, VDNs, and permissions are entered, the **List all** command will only return those permission definitions which match all of the information.

# About modifying VDN user permissions

This section provides the procedure for modifying the VDN permissions definition for a CMS user.

This feature is available if the following items are true:

- The Vectoring feature has been purchased and installed.

- VDN permission checking is enabled.

## Before modifying VDN user permissions

The following items should be read and understood before modifying VDN permissions:

- When the permissions definition for a user is modified, the change does not take effect until the user logs off and back on again.
- If a user does not have corresponding ACD permissions for the permissions set for them on the VDN, Supervisor displays an error message.
- The wildcard characters “*” and “?” cannot be used in the User Permissions VDN Access window.

## Modifying VDN user permissions

### Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **VDN Access**.
3. In the **ACD** field, select the ACD containing the VDN for which the user has a permissions definition.
4. Select **OK** .

   Supervisor displays the User Permissions VDN Access window.

5. In the **User ID** field, enter the name of the user for which the VDN permissions definition is to be modified.
6. If the specific VDN to view for this user is known, enter the name or number of the VDN in the **VDNs** field.

   To have all VDNs returned for this user ID, leave this field blank.

   This field can accept multiple VDNs. Multiple entries must be separated by a semicolon (;).

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

   The database is queried and the number of matches found for this user ID displays in the status bar. The first match found populates the fields of this dialog box.

   If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct VDN.

8. Change the permissions for the user on this VDN as needed:
   - **Read** - User can view but not modify information for the specified VDNs including reports.
   - **Write** - User can modify information on the specified VDNs. This permission requires that the user also have the “read” permission.
   - **Exceptions** - User will receive notification of exceptions occurring on the specified VDNs.

**Important:**

If all permissions are to be removed for this user ID, it saves more server disk space to delete this permission definition rather than disabling all permissions.

Only the VDN exceptions made active through the **Exceptions** feature will provide notification to the user. See Chapter 9: Administering exceptions on page 176 for more information.

9. After the necessary permission changes have been completed, select **Actions** > **Modify** from the menu bar.

   The permissions definition for this user ID and VDN is updated. The status bar displays a `Successful` message upon completion.

# Deleting VDN user permissions

## About this task

This section provides the procedure for deleting the VDN permissions definition for a CMS user.

## Procedure

1. On the Controller window, select **Tools** > **User Permissions**.

   Supervisor displays the User Permissions window.

2. In the **Operations** list, highlight **VDN Access**.
3. In the **ACD** field, select the ACD containing the VDN for which the user has a permissions definition.
4. Select **OK** .

   Supervisor displays the User Permissions VDN Access window.

5. In the **User ID** field, enter the name of the user for which the VDN permissions definition is to be deleted.
6. If the specific VDN to view for this user is known, enter the name or number of the VDN in the **VDNs** field. To return all VDNs for this user ID, leave this field blank.
7. From the menu bar, select **Actions** > **Find one**.

   The database is queried and the number of matches found for this user ID displays in the status bar. The first match found populates the fields of this dialog box.

   If multiple matches are found, use the **Next** and **Previous** items found under the **Actions** menu to navigate to the correct VDN.

8. From the menu bar, select **Actions** > **Delete**.

   The permissions definition for this user ID and the associated VDN is deleted. The status bar displays a `Successful` message upon completion of the action.

This action does not delete the permission definitions for all VDN for this user, only the one displayed in the **VDNs** field.

# Tenant user restricted access

- Special Agent/Agent Group restriction: Tenant users can only access agents and tenant specific agent groups pertaining to the tenant for which the user has permissions.
- Special CWC restriction: Tenant users can only access the CWCs pertaining to the tenant for which the user has permissions.
- Reports restriction: The report data is restricted to show only data for ACDs for which the tenant user has permissions.
- Dictionary restriction: Dictionary menu items and screens corresponding to Agent Groups and ACD Groups are not accessible by tenant users since tenant users are only allowed to access permissible tenant partitions of a single ACD.
- Call Center Administration restriction: Tenant users cannot access Call Center Administration for ACD Groups or Vector Contents.
- Tenant Administration restriction: Even if a tenant user is granted write permission for the Tenant feature, the tenant user is not allowed to write actions such as Add and Delete for the tenant assignments.
- User Permissions restriction: Tenant users cannot have write permissions to the User Permissions feature. Tenant users cannot view permission information for other users. Tenant users can only see permission information for themselves.

  For tenant users, the **User Permissions** menu item under **Tools** in the Controller window is replaced by the **Tenant Access Permissions** menu item.

  The Tenant Access Permissions window provides the tenant user with the following screens:

  - Access Permissions Tenant Access: This screen provides the **Find one** and **List all** options to the tenant user for determining the tenant access permissions assigned to the user.
  - Access Permissions Tenant Vector Access: This screen provides the **Find one** and **List all** options to the tenant user for determining the vector access permissions assigned to the user.
  - Access Permissions Tenant ACD Access: This screen provides the **Find one** and **List all** options to the tenant user for determining the ACD access permissions assigned to the user.
  - Access Permissions Tenant Trunk Group Access: This screen provides the **Find one** and **List all** options to the tenant user for determining the trunk group access permissions assigned to the user.
  - Access Permissions Tenant VDN Access: This screen provides the **Find one** and **List all** options to the tenant user for determining the VDN access permissions assigned to the user.

- Access Permissions Tenant Split/Skill Access: This screen provides the **Find one** and **List all** options to the tenant user for determining the split/skill access permissions assigned to the user.
- Access Permissions Tenant User Data: This screen provides the user data information about the tenant user.
- Access Permissions Tenant Feature Access: This screen provides the feature access information about the tenant user.
- Access Permissions Tenant Main Menu Addition Access: This screen provides the main menu addition access information about the tenant user.

# Administering tenants

Use the **Tenant Administration** item in the **Commands** menu or the toolbar button of CMS Supervisor to administer tenants in the contact center. If you do not install the Tenancy feature, the **Tenant Administration** item and the toolbar button do not display in CMS Supervisor.

## Supervisor Tenant Administration sub menu

Click **Commands** > **Tenant Administration** to navigate to the Tenant Admin sub menu window. The **Operations** tab in the Tenant Admin sub menu window comprises 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

**Important:**

- A tenant number has to be between 1 and 250.
- Agents can have up to 16 digits based on Communication Manager releases.

The 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 `Already exists` 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 `Does not exist` 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. |
| **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 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 `Already exists` 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 `Does not exist` 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. |
| **Previous** | After doing a **Find one** search resulting in more than one match, this selection displays the previous match. |

# Tenant trunk group assignment

**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 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 `Already exists` 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 `Does not exist` on the status line. The user must have write |

*Table continues…*

| Field | Description |
|---|---|
| | 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

**Important:**

- A tenant number has to be between 1 and 250.
- VDNs can have up to 16 digits based on Communication Manager releases.

The 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 `Already exists` 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 `Does not exist` 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. |

*Table continues…*

| Field | Description |
|---|---|
| **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

**Important:**

- A tenant number must be between 1 and 250.
- Vector numbers are between 1 and 8000.

The 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 `Already exists` 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 `Does not exist` 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 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. |

## Tenant Call Work Code assignment

**Important:**

- A tenant number has to be between 1 and 250.
- Each Call Work Code (CWC) can have up to 16 digits.

The 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 `Already exists` 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 `Does not exist` 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 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 agent groups assignment

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 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 `Already exists` 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 `Does not exist` 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 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 `Already exists` 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 administration reports

Select **Commands** > **Tenant Administration** to navigate to the Tenant Admin sub menu window. Select the **Reports** tab in the Tenant Admin sub menu window to access the tenant administration reports.

## Tenant administration tenant agent group members report

You can generate reports of the tenant agent group members that you created for the tenants defined in the system.

## Tenant administration tenant agent groups report

You can generate reports of the tenant agent groups that you created for the tenants defined in the system.

# Chapter 11: Configuring CMS System Settings

## Configuring CMS system settings

This section provides procedures on viewing and changing the setup of the CMS system configured during the initial installation. These configuration values are used in adjusting the state of the system and the collection, storage, and retrieval of data. Making changes to these configuration settings can affect system performance, disk space usage, and data collection.

## Before configuring CMS system settings

If an ACD Group is selected as the current ACD in the System Setup window, only those operations that are valid for the ACD Group will appear in the **Operations** list.

## CMS state

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 on to the CMS server at a time.

The single-user mode is necessary when changes must be made to the following systems and procedures:

- Change Master ACD
- Data storage allocation
- Storage intervals
- Restore specific types of data
- Migrate specific types of data

The CMS State window can be used to select which ACD serves as the master for time synchronization. The time displayed on the Controller window originates from the master ACD.

## Before using CMS State

The following items should be read and understood before changing the CMS state:

- Viewing data in the Data Storage Allocation, Storage Intervals, and Restore Data windows can be done through both the multi-user and single-user modes.
- To add to or modify configuration settings for the Data Storage Allocation, Storage Intervals, and Restore Data windows requires that the CMS state is set to single-user mode.
- If a log out is performed while CMS is still in the single-user state, at least ten seconds must pass before a logon can be performed.
- When in single-user mode, CMS continues to collect data for all ACDs with the data collection feature enabled.

## Permissions for CMS State

Depending on the procedure that you want to perform, you need the following permissions:

- To view the CMS state or the master ACD, the user ID used to log on to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To modify the CMS state or the master ACD, the user ID used to log on to this Supervisor session requires “write” permission for the CMS System Setup feature.

## Changing the CMS state

### About this task

This section provides the procedure for changing the state of the CMS system to single-user or multi-user mode.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **CMS State**.
3. Select **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

#### About this task

This section provides the procedure for selecting the master ACD which will be used for time synchronization.

**Important:**

Changing the master ACD requires that you turn data collection off.

#### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **CMS State**.
3. Select **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.

# Data collection

The Data Collection window is used to enable and disable the storing of data for real ACDs. When data collection is disabled, no contact center data is recorded during the current interval. Also, reports run to include this time period will not accurately reflect the activities in the contact center.

## Before using Data collection

The following items should be read and understood before working with the data collection feature:

- When data collection is enabled, 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 enabled for the current ACD in order to activate an agent trace or do any switch administration from CMS.
- When data collection is disabled, 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 disabled, it is best to wait for the current interval to be archived so that data loss is minimized.

## Permissions for Data collection

Depending on the procedure that you want to perform, you need the following permissions:

- To view Data Collection settings, the user ID used to log on to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To modify the Data Collection settings, the user ID used to log on to this Supervisor session requires “write” permission for the CMS System Setup feature.

## Changing the data collection state

### About this task

This section provides the procedure for enabling or disabling data collection for an ACD.

### Procedure

1. On the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **Data Collection**.
3. Select **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.

# Data Storage Allocation

The Data Storage Allocation window is used to specify the amount of historical data saved by CMS and the duration for which it is saved. The amount of data saved and the duration for which it is saved affects disk space on the server and is limited by the configuration of the system. Data storage parameters are initially set during installation.

## Before using Data Storage Allocation

The following items should be read and understood before working with Data Storage Allocation:

- A full maintenance backup should be performed before changing the Data Storage Allocation configuration.
- If changes to the Communication Manager system are made through the **swsetup** command on the CMS console, the settings for Data Storage Allocation should be checked to ensure that storage is set for any new or modified entities. For example, enable the Call Vectoring feature requires data storage space for VDNs and vectors. Changing the release of the Communication Manager system may change the number of measured entities allowed and affect the storage allocation for each entity.
- Disable data collection for all real ACDs before making modifications through Data Storage Allocation.
- Set the CMS state to single-user mode before making modifications through Data Storage Allocation.
- 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.
- For reference, print out the Data Storage Allocation window before modifications are made.
- If a Data Storage Allocation window is modifying data, 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.
- Activating a feature such as vectoring requires not only changing switch parameters but also requires the allocation of space for VDNs and vectors which did not have space previously allocated.
- The amount of free space available on the server limits the maximum amount of storage space usable through Data Storage Allocation. Use the Free Space Allocation window to view the utilization of disk space before making changes to Data Storage Allocation. 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 has not been purchased and installed, 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 - 62 days
  - Daily - 1825 days (5 years)
  - Weekly - 520 weeks (10 years)
  - Monthly - 120 months (10 years)

## Permissions for Data Storage Allocation

Depending on the procedure that you want to perform, you need the following permissions:

- To view Data Storage Allocation settings, the user ID used to log on to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To modify Data Storage Allocation settings, the user ID used to log on to this Supervisor session requires “write” permission for the CMS System Setup feature.

## Viewing Data Storage Allocation

### About this task

This section provides the procedure for viewing the Data Storage Allocation parameters.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS 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. Select **OK**.

   Supervisor displays the Data Storage Allocation window.

## About modifying Data Storage Allocation

This section provides the definitions of the fields displayed in the Data Storage Allocation window and suggestions for determining the necessary values. The data storage configuration is performed on a per-ACD basis. In a multi-ACD environment, data storage allocation should not be set too high as it can exceed disk capacity for storing information for the other ACDs.

Data storage allocation needs vary among installations. Base your CMS data storage needs on these criteria:

- The available disk space on your CMS system
- The number of real and pseudo-ACDs on the CMS system
- The size of the real ACDs and all pseudo-ACDs, such as number of agents, trunks, and so forth.
- The length of time for data to be stored. For example, 30 days versus 100 days versus two years.

## Before modifying data storage allocation

Before modifying the configuration of the Data Storage Allocation window, the following must occur:

- Data collection for all real ACDs must be disabled.
- The CMS state must be set to single-user mode.
- A full maintenance backup should be performed before changing the Data Storage Allocation configuration.

## Data Storage Allocation fields

The following table lists the fields found on the Data Storage Allocation window. Several of these data storage parameter limits are documented in Avaya Aura® Communication Manager System Capacities Table.

| Name | Description |
|---|---|
| **Data Item** | Lists the maximum number of splits/skills, trunk groups, trunks, call work codes, vectors, and VDNs allowed for the system. |
| **# of Items** | The number of splits/skills, trunk groups, trunks, call work codes, vectors, and VDNs for which data storage space should be allocated.<br>When this window is initially displayed, these fields display the number of currently administered data items. These numbers should include expected growth. For example, a `30` in this field for **Split(s)/Skill(s)** indicates that storage space is allocated for 30 splits/skills. The system may have only 25 splits/skills in existence, but this number allows for future growth. |
| **Days of Intrahour** | The number of days where the system stores intrahour data for splits/skills, agents, trunk groups, trunks, call work codes, vectors, and VDNs.<br>Each entity can have a different number of days associated with it.<br>A `0` (zero) in this field causes the system to discard intrahour data which also means that no daily, weekly, or monthly data can be collected.<br>When data collection reaches the end of the length of time specified, the data is combined, archived, and appended into daily information. |
| **Days of Daily** | The number of days for which the system stores daily data for splits/skills, agents, trunk groups, trunks, call work codes, vectors, and VDNs. |

*Table continues…*

| Name | Description |
|---|---|
| | Each entity can have a different number of days associated with it.<br><br>A 0 (zero) in this field causes the system to discard daily data which also means that no daily or weekly data can be collected.<br><br>When data collection reaches the end of the length of time specified, the data is combined, archived, and appended into weekly information. |
| **Weeks of Weekly** | The number of weeks for which the system stores weekly data for splits/skills, agents, trunk groups, trunks, call work codes, vectors, and VDNs.<br><br>Each entity can have a different number of weeks associated with it.<br><br>A 0 (zero) in this field causes the system to discard weekly data.<br><br>When data collection reaches the end of the length of time specified, the data is combined, archived, and appended into monthly information. |
| **Months of Monthly** | The number of months for which the system stores monthly data for splits/skills, agents, trunk groups, trunks, call work codes, vectors, and VDNs.<br><br>Each entity can have a different number of months associated with it.<br><br>A 0 (zero) in this field causes the system to discard monthly data.<br><br>When data collection reaches the end of the length of time specified, the data is deleted. |
| **Shift n times (1, 2, 3, or 4)** | The shift start and stop times for each shift of agents (up to four shifts) for the specified ACD. This information is used to calculate the amount of space to be reserved for this historical agent table.<br><br>Shifts may overlap.<br><br>If you specify a shift that starts before the data collection start time or ends after the data collection stop time, you receive an error message. The data collection start and stop times are found in the Storage Intervals window in **System Setup**.<br><br>CMS rounds shift times to the nearest interval. For example, if you use 30-minute intervals and specify a shift from 8:15 to 5:15, CMS assumes that this shift is from 8:00 to 5:30.<br><br>Shift must be at least one minute in length.<br><br>Specify 24-hour shifts according to the following example:<br><br>8:00AM to 7:59AM<br><br>This information is used throughout CMS . |
| **Maximum agents logged in** | The maximum number of agents logged in during the shift |
| **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.<br><br>This number should include those agents or extensions that are members of multiple splits/skills. For this field, each split/skill the agent belongs to |

*Table continues…*

| Name | Description |
|---|---|
| | counts as a split/skill member. Using this method of determining members results in a higher number than the number of agents.<br><br>For Communication Manager systems without Expert Agent Selection (EAS), this value represents the maximum number of administered split members.<br><br>For Communication Manager systems with EAS, 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/logout records stored by the system. Each time an agent logs in, the system creates a login/logout record. The subsequent logout of the agent also uses this same record. If, at a later time, the agent logs in again, another login/logout record is created.<br><br>The following equation demonstrates how this number is calculated:<br><br>(Number of agents) x (Number of times each agent logs in each day) = Number of agent login/logout records<br><br>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.<br><br>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 currently specified ACD. This number is not representative of all ACDs. |
| **Number of unmeasured trunk facilities** | The number of trunks not measured by the CMS system.<br><br>An unmeasured trunk facilities are used for:<br><br>• Internal calls (intraswitch) to a measured split or agent<br><br>• Internal calls to VDNs<br><br>• Calls made by agents to internal destinations or using a trunk group that is not measured<br><br>• Transfers and conferences until the transfer/conference is complete<br><br>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 forth. |
| **Number of call records** | The number of call records the system stores for a selected ACD.<br><br>If the Avaya CMS Call History Interface product has been purchased and 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. |

# Data summarizing

Data is automatically archived based on the entries in the Storage Intervals window. The Data Summarizing window is used to manually archive data in the daily, weekly, and monthly tables of the historical database.

## Before using 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.
- 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.

## Permissions for Data summarizing

Depending on the procedure that you want to perform, you need the following permissions:

- To view the Data Summarizing window, the user ID used to log in to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To use the Data Summarizing window to perform an archive of the system, the user ID used to log in to this Supervisor session requires “write” permission for the CMS System Setup feature.

## Archiving data

### About this task

This section provides the procedure for manually archiving data using the Data Summarizing window.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **Data Summarizing**.
3. Select **OK**.

   Supervisor displays the Data Summarizing window.
4. In the **ACD** field, select the ACD for which data will be archived.
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.

# 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.

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 contact 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 contact center data consolidation program - This third-party software is used to collect data from all contact 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, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **External Application Status**.
3. Select **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, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **External Application Status**.
3. Select **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, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.

2. In the **Operations** list, highlight **External Application Status**.
3. Select **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.

# Free Space Allocation

The Free Space Allocation window is used to view the current storage statistics and disk usage for the contact center data collected through CMS .

If, at any time, you modify the Data Storage Allocation configuration, Free Space Allocation will automatically adjust the amount of required space.

## Before using Free Space Allocation

The following items should be read and understood before working with the Free Space Allocation feature:

- When any of the CMS data storage parameters are altered, the change is reflected (for information purposes only) in the Free Space Allocation window. For example, if the number of splits/skills on your system is increased in the Data Storage Allocation window, the Free Space Allocation window will then display the new number as well as the approximate amount of disk space required to handle the data storage for splits/skills.
- The IDS dbspaces used in the Free Space Allocation window are created during installation.
- Be aware that creating custom tables causes CMS to use more disk space. If dbspace is used to store custom tables nears capacity, you are presented with a warning message during login.
- Values entered in the CMS System Setup features of Data Storage Allocation, Storage Intervals, and Call Work Codes directly affect usage of disk space. Check **Free Space Allocation** when any of these features are modified.
- Values entered in the Data Storage Allocation window of Forecast Administration also affect storage space.

## Permissions for Free Space Allocation

To view the Free Space Allocation window, the user ID used to log in to this Supervisor session requires “read” permission for the CMS System Setup features.

## Viewing Free Space Allocation

### About this task

This section provides the procedure for viewing the Informix Dynamic Server (IDS) storage information and allocations through the Free Space Allocation window.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.

2. In the **Operations** list, highlight **Free Space Allocation**.
3. Select **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 contents

### About this task

This section provides the procedure for viewing the allocations for each contact center entity within an ACD.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **Free Space Allocation**.
3. Select **OK**.

   Supervisor displays the Free Space Allocation input window.

   **Note:**

   The window make 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**.

   Supervisor displays a secondary window showing the amount of data currently in use by each contact center entity.

# Migrating CMS data

This section provides the procedures and information involved in migrating data from a backup device that was created using a previous version of CMS and into the database of the new CMS .

## Before migrating CMS data

The following items should be read and understood before working with the R3 Migrate Data window:

- Attempting to migrate Agent and Call Center Administration data more once may cause serious errors from which recovery is difficult. A re-migration of ACD administration data requires a second setup of the CMS software must be performed.
- To migrate 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 results in two separate sets of data. Only one set of data can be used and cannot be migrated into another set.

## Permissions for migrating CMS data

Depending on the procedure that you want to perform, you need the following permissions:

- To run the R3 Migrate Data process, the user ID used to log in to this Supervisor session requires “write” permission for CMS System Setup.

## Migrating R3 data

### About this task

This section provides the procedure for using the R3 Migrate Data to merge data created using a previous version of CMS to the database of the current version.

### Procedure

1. From the Controller window, select **Tools** > **CMS System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **R3 Migrate Data**.
3. Select **OK**.

   Supervisor displays the R3 Migrate Data window.
4. Enter a value in the **Device name** field.

   To list all devices on the system, select **Actions** > **List devices**.

   **Caution:**

   If you choose the **System Administration data** option in this step, note that this migration can only be performed once. Performing the migration of this data a second time can result in corruption of the password tables.

5. In the **Data type** group, select one of the following three options:
   - 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 will report the progress of the migration.

## R3 Migrate Data field descriptions

| Name | Description |
|---|---|
| **Device name** | The name of the backup device containing the data |
| **Data type**: **System Administration data (single-user required)** | Migrated data:<br>• Report GEM files (historical)<br>• Report GEM files (real-time)<br>• Shortcut settings for CMS<br>• CMS users<br>• Timetable settings<br>• Database items<br>• Hypothetical data for the Forecast product<br>• Feature access settings, timetables, schedules, and associated tasks from the User Permissions subsystem<br>• Historical and real-time custom reports<br>• Menu and interface settings for the CMS terminal interface<br>• Printer parameters for the CMS printer |
| **Data type**: **Agent/Call Center Admin data (single user required)** | Migrated data:<br>• ACD profiles - VDN profiles<br>• Agent trace - agents being traced, trace data<br>• Agents - shifts, groups |

*Table continues…*

| Name | Description |
|---|---|
| | • Dictionary - synonyms<br>• Exceptions - agent admin, link data, malicious call trace, split admin, splits, split profile, trunk group admin, VDN admin, vector admin<br>• User permissions - ACD access, split/skill access, trunk groups access, VDN access, vector access<br>• Forecast - current day report, current day configuration, call handling profiles, costs profiles, data storage allocation, special day admin, manager status, trunk group profiles |
| **Data type**: **Historical data** | Migrated data:<br>• Exceptions - agent data, split access, trunk groups, trunk group access, VDN data, vector data<br>• 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<br>• Forecast - daily split data, daily trunk group data, special day split data, interval split data, interval trunk group data |
| **Stop date** | The date through which you wish to record data for migration to the new CMS . The migration process does not migrate data collected after the date specified. |
| **Stop time** | The time through which you wish to record data for migration to the new CMS . The migration process does not migrate data collected after the stop date and time specified.<br>If this field is left blank, the stop time defaults to `23:59`. |
| **Specify ACD(s) to migrate**: **All ACDs** | Data is migrated from the backup device to the hard disk on an ACD-by-ACD basis. Data for ACD1 on the backup device will be used for ACD1 on the new CMS . |
| **Specify ACD(s) to migrate**: **Single ACD** | Historical data is migrated from the backup device to the hard disk for the ACDs specified in the **from** and **To** fields.<br>For example, to migrate data from ACD1 on the backup device to ACD4 on the new CMS , place `1` in the **from** field and `4` in the **To** field. |

# Pseudo-ACDs

A pseudo-ACD is an area created on the CMS server to store previously backed-up ACD data. A pseudo-ACD is not a real ACD and does not communicate with any Communication Manager system.

Pseudo-ACDs are used to store data which can then be viewed in reports. This could be useful in the following scenarios:

- Storing data from an off-site contact center for the purposes of reporting in conjunction with an on-site CMS .
- Storing data for archival purposes. This data can no longer be deleted by the Data Storage Allocation feature and can be used to generate reports on older data for comparison with more recent ACD data.

## Before using pseudo-ACDs

The following items should be read and understood 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.
- In order to load the pseudo-ACD data, the CMS server must have enough free space available. Use the Free Space Allocation window to see how much space is required for the existing ACDs and how much is available for the pseudo-ACD data.
- Use the Data Storage Allocation window to define how much historical data will be stored for the pseudo-ACD. Enter storage values equal to or greater than those used from the ACD which originally held the data.
- Use the Storage Intervals window to 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.
- The Data Collection feature can be running when modifications are made in the Data Storage Allocation or Storage Intervals windows for a pseudo-ACD, but CMS must be in single-user mode.
- If the pseudo-ACD has the separately purchased Forecast feature on it, Forecast Data Storage Allocation parameters can require changes in order to match those of the pseudo-ACD. This is not the same as the Data Storage Allocation window normally used in CMS .
- In order for users to access the pseudo-ACD, permissions must be given through the ACD Access window in the User Permissions subsystem.
- A pseudo-ACD can have a name assigned to it in the Dictionary even before the pseudo-ACD is created.
- Creation of a pseudo-ACD using Supervisor while users are logged in requires that the users log out and back in before they can see the new pseudo-ACD.
- 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 available when a pseudo-ACD is selected and the appropriate user permissions are assigned:

| | | |
|---|---|---|
| **Reports** | **CMS System Setup** | **Maintenance** |
| **Historical** | **CMS State** | **ACD Status** |
| **Dictionary** | **Data Collection** | **Archiving Status** |
| all submenu items | **Data Storage Allocation** | **Backup Data** |
| **Forecast** | **Data Summarizing** | **Backup/Restore Devices** |
| all submenu items | **Free Space Allocation** | **Connection Status** |
| **Custom Reports** | **Load Pseudo-ACD** | **Printer Administration** |
| all submenu items | **Pseudo-ACD Setup** | **Restore Data** |
| **User Permissions** | **R3 Migrate Data** | |
| all submenu items | **Storage Intervals** | |
| | **Switch Setup** | |

# Permissions for pseudo-ACDs

Depending on the procedure that you want to perform, you need the following permissions:

- To view the Pseudo-ACD Setup window, the user ID used to log in to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To add or delete pseudo-ACDs, the user ID used to log in to this Supervisor session requires “write” permission for the CMS System Setup feature.

# Creating a pseudo-ACD

## About this task

This section provides the procedure for creating a pseudo-ACD on a CMS server.

**Important:**

To create a pseudo-ACD, CMS must be operating in single user mode.

## Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **Pseudo-ACD Setup**.
3. Select **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. In the **Operations** list, highlight **Data Storage Allocation**.
13. In the **ACD** list, highlight the appropriate pseudo-acd.
14. Select **OK**.

    Supervisor displays the Data Storage Allocation window.
15. Enter storage values equal to or greater than the values used for the ACD which originally stored the data.
16. 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?
    ```
17. Select **YES**.
18. Close the Data Storage Allocation window.
19. In the **Operations** list, highlight **CMS State**.

    Supervisor displays the CMS State window.
20. Select the option **Multi-user mode**.
21. From the menu bar, select **Actions** > **Modify**.
22. Close the CMS State window.
23. In the **Operations** list, highlight **Storage Intervals**.
24. In the **ACD** list, highlight the appropriate pseudo-acd.
25. Select **OK**.

Supervisor displays the Storage Intervals window.

26. Enter storage values equal to the values used for the ACD which originally stored the data.
27. 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.
28. Close the Storage Intervals window.
    - If you want to create a Dictionary name for the pseudo-ACD just created, continue with Step 29 on page 292.
    - If you do not want to create a Dictionary name for the pseudo-ACD just created, continue with Viewing pseudo-ACDs on page 293.
29. 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.
30. In the **Operations** list, highlight **ACDs**.
31. Select **OK**.

    Supervisor displays the Dictionary ACDs window.
32. In the **ACD Name** field, enter the name for the pseudo-ACD.
33. In the **ACD Number** field, enter the number for the pseudo-ACD from Step 4.
34. In the **Description** field, a description for the pseudo-ACD. The origin of the data can be useful information in the description field.
35. 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.
36. Continue with Viewing pseudo-ACDs on page 293.

# Viewing pseudo-ACDs

## About this task

This section provides the procedure for listing the pseudo-ACDs on a CMS server.

## Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **Pseudo-ACD Setup**.
3. Select **OK**.

   Supervisor displays the Pseudo-ACD Setup window.
4. From the menu bar, select **Actions** > **List all**.

   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 this user ID has “read” permission are displayed.

# Deleting a pseudo-ACD

## About this task

This section provides the procedure for deleting a pseudo-ACD on a CMS server.

## Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
2. In the **Operations** list, highlight **Pseudo-ACD Setup**.
3. Select **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 for a pseudo-ACD

This section provides the procedure for backing up historical data, archived from an existing ACD, to be used for a pseudo-ACD.

## Before backing up data for a pseudo-ACD

The following items should be read and understood before backing up data for a pseudo-ACD:

- Data used for a pseudo-ACD must have been archived from an existing ACD on a CMS server.
- You must back up pseudo-ACD data to tape, a USB storage device, or a network mount point.
- A pseudo-ACD accepts any data on a backup volume. So the data from a full backup can be more than needed. Loading a pseudo-ACD with a full backup creates problems of disk space. To eliminate this problem, perform a backup of specific tables when creating a backup of ACD data to load into a pseudo-ACD.
- The pseudo-ACD entity, administration, must match or be greater than the ACD where the data was archived. Document the values in the Data Storage Allocation table 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, loading the data into the pseudo-ACD can fail.
- The pseudo-ACD entity, Storage Intervals, must match the ACD where the data was archived. Document the values in the Storage Intervals table for the ACD where the data was archived. Verify that the pseudo-ACD configuration matches the documented values. If these settings are incorrect, loading the data into the pseudo-ACD can fail.
- CMS R16.2 and later releases support CMS data backups to tape, NFS mount points, and USB storage devices. The backup path must be defined in **Maintenance** > **Backup/Restore Devices**. Refer to the *Avaya Call Management System Software Installation, Maintenance and Troubleshooting*, for the appropriate operating system, to administer a Backup/Restore Device for a network mount point or a USB storage device. Systems with CMS releases prior to R16.2 must back up to tape or use RTM to back up the data to an alternate backup device. Refer to the *Avaya Call Management System Software Installation, Maintenance and Troubleshooting*, for the appropriate operating system, to perform a tapeless migration.

  **Tip:**

  The CMS feature, Loading Pseudo-ACD Data, loads data from the latest CMS maintenance backup that exists in the Backup/Restore Device path. If the Backup/Restore Device is a network mount point or USB storage device, and the pseudo-acd data is only a set of specific tables, create a directory specifically for the pseudo-acd data. Next, create a Backup/Restore Device pointing to the specific directory for the pseudo-acd data. Perform a backup of the desired data for the pseudo-acd using the Backup/Restore Device just created. Then load the pseudo-acd data using the same Backup/Restore Device name in the Loading Pseudo-ACD Data form as used in the Backup Data form. This process ensures that correct data is loaded into the pseudo-acd since the only data that exists in

the directory of the Backup/Restore Device path is the data specifically backed up for the pseudo-acd.

## Permissions for backing up data for a pseudo-ACD

The user ID used to log in to this Supervisor session requires write permission for the Maintenance feature as well as the Back Up Data feature.

## Backing up data for a pseudo-ACD

### Procedure

1. Document the entries in the Data Storage Allocation form for the ACD that will be used to load data into the pseudo-acd.
2. Document the entries in the Storage Intervals form for the ACD that will be used to load data into the pseudo-acd.
3. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the CMS Maintenance window.
4. In the **Operations** list, highlight **Backup Data**.
5. In the **ACD** list, highlight the ACD that contains the data to be backed up for the pseudo-ACD.
6. Select **OK**.

   Supervisor displays the Backup Data window.
7. In the **Device name** field, enter the Backup/Restore device name to use to backup the ACD data.
8. If the backup device is not a tape storage device, clear the **Verify tape can be read after backup?** option.
9. From the**ACD(s) to back up** options, select **Current ACD**.
   - If all the tables from the current ACD are being backed up, continue with Step 15 on page 296.
   - If only specific tables from the current ACD are being backed up, continue with Step 10 on page 295.
10. From the menu bar, select **Actions** > **Select tables**.

    Supervisor displays the Backup Data - Select Tables window.
11. Click inside the box for selecting all the tables to be backed up.
12. From the menu bar, select **Actions** > **Modify**.

    Supervisor saves the tables selected for the back up.
13. From the menu bar, select **Actions** > **Exit**.

    Supervisor displays the Backup Data window and checks the **Specific tables** option under **Data to back up**.

14. From the **Data to back up** options, clear the **System**, **ACD-specific administration dataHistorical**, and **Non-CMS data** data options. When **Specific tables** is selected, no other type of data can be selected.
15. To start the backup, select **Actions** > **Run**.

    Supervisor displays the following message:

    ```
    The backup is estimated to be xxxxxx kbytes.
    ```

16. Select **OK**.

    Supervisor displays the following message if the backup device already contains CMS data:

    ```
    Mounted volume might belong to CMS data archive. Enter yes to
    overwrite it or no to mount another volume.
    ```

    - If you are not sure whether or not to overwrite the data, enter `No`.
      - If the backup device is a tape storage device, replace the tape and repeat Steps 1-14.
      - If the backup device is a network mount point or USB storage device, repeat Steps 1-14 but choose a different backup device in Step 7.
    - If you are sure it is safe to overwrite the CMS data, enter `Yes`.

    CMS begins backing up the data for the current ACD. The **Status** field at the top of the window displays events in the backup process. The **Error name** field displays any problems encountered during the backup process.

    Cancelling the backup process before it is finished causes the backup to be incomplete.

### Result

If the backup is to a network mount point or a USB storage device, the backup filename can be found under the path defined for the Backup/Restore Device name used for the backup.

An example of a CMS data backup filename is:

```
CMS-130417-04-XXXX-04-F-01-04-igor00000000000
```

**Important:**

The data backup filename must be in the format as shown in the example or CMS fails to detect the file as a data backup file.

The data backup file name identifies the following:

- Type of backup: CMS Data
- Date of the backup: 130417 (yymmdd)
- Number of CMS data backups completed for the day: 04
- Type of data backed up: XXXX (specific tables only)

  LSAC (System, ACD-specific, Historical and Non-CMS data)

  LSMC (System and ACD-specific data)
- ACD Number: 04

  ACD 4, this value is 00 if all ACDs are being backed up.

- Type of back up: F-01

  F (Full Maintenance backup)

  I (Incremental Maintenance backup)
- Number of characters in hostname: 04 (igor)
- CMS hostname: igor

  This field is 15 characters long. The number of trailing zeros in this example is 11 so that the total number of letters in the hostname is 15.

# About loading pseudo-ACD data

This section provides the procedure for loading historical data archived from an existing ACD into a pseudo-ACD. After the pseudo-ACD receives the data, historical reports can be run with this information.

## Before loading pseudo-ACD data

The following items should be read and understood before loading data into a pseudo-ACD:

- A pseudo-ACD must have been created in order for data to be loaded into it.
- Loading data into a pseudo-ACD requires data archived from an existing ACD on a CMS server.
- Set the pseudo-ACD as the current ACD before attempting to load data into it.
- Since the pseudo-ACD accepts any data on a backup volume, the data from a full backup may be more than needed. Loading a pseudo-ACD with a full backup creates the possibility of disk space problems. To eliminate this problem, perform a **Specific tables** backup when creating the ACD data to load into a pseudo-ACD.
- Loading a pseudo-ACD with data automatically overwrites any existing data currently used by the pseudo-ACD.
- The number of splits/skills, agents, and other contact center entities are set to 0 (zero) for the pseudo-ACD when it is created. Set these entities to match the ACD supplying the data. Change these settings through the Call Center Administration feature.
- When created, a new pseudo-ACD has historical data storage parameters set to 0 (zero). To load data into the pseudo-ACD, the historical data storage parameters must be set to those of the ACD from which the data was archived, if not greater. Change these settings through the Data Storage Allocation window.
- The **Storage Intervals** and **Data Collection** settings for the pseudo-ACD require configuration in order to match those of the ACD supplying the data. If these settings are incorrect, loading the data into the pseudo-ACD fails.

## Permissions for loading pseudo-ACD data

To load data into a pseudo-ACD, the user ID used to log in to this Supervisor session requires “write” permission for the CMS System Setup feature.

# Loading pseudo-ACD data

## About this task

Perform Steps 1 through 5 on the CMS server.

## Procedure

1. Verify that the data on the media is from the desired source. Enter:

   `/cms/bin/br_check`

   The system displays the following message:

   `Enter device type ['q' for qtape, 'f' for floppy, 'n' for nfs/usb]:`

2. Depending on the type of backup media containing the data, enter `q`, `f`, or `n`.

   The system displays the following message:

   `Enter device path:`

3. Enter the device path.

   The system displays the br_check information found on the device. The following example is for backup data on a tape:

```
Opening the volume...
Label: CMS-110421-01-LSAC-00-F-01
CMS Database Version: r16.2da.g.0
Machine name: igor
forecasting: y
global dictionary/ACD groups: y
ACD(s) backed up on the volume:
ACD     Switch  EAS     Vectoring
1       R6      y       y
2       R5.2    y       y
3       R4/R5   n       y
4       R4/R5   y       y
5       R6      y       y
Enter 'l' to list the tables or 'v' to also verify the volume:
```

4. Review the br_check output.
   - If the information is correct, continue with Step 5 on page 298.
   - If the information is not correct, replace the tape or path with the correct backup data information. Repeat Steps 1 on page 298 through 4 on page 298.
5. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS System Setup window.
6. In the **Operations** list, highlight **Load Pseudo-ACD**.
7. In the **ACD** field, select the pseudo-ACD that will receive the data.
8. Select **OK**.

   Supervisor displays the Load Pseudo-ACD Data window.

9. In the **From ACD** field, enter the number of the source ACD, which is the ACD used to make the data backup, or the number of the ACD to migrate data from the full maintenance backup tape.
10. In the **Device name** field, enter the name of the device that has the backup volume loaded.

    To list all the devices on the CMS server, select **Actions** > **List devices** from the menu bar.

    **Caution:**

    The Loading Pseudo-ACD Data feature loads data from the latest CMS maintenance backup that exists in the path defined in the Backup/Restore Device name entered. Ensure that the latest CMS data backup under the Backup/Restore Device name contains the data you want loaded into the pseudo-acd.
11. 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.
12. In the **Start time** field, enter the time of the **Start time** for which CMS will start loading data. The default is `12:00AM`.
13. In the **Stop date** field, enter the last date of historical data that CMS will load into the pseudo-ACD.
14. In the **Stop time** field, enter the time of the **Stop time** for which CMS will stop loading data from the data backup. The default is `12:00AM`.

    **Note:**

    To restore all the data, for the selected ACD, you can leave the **Start date** blank and enter a future date for the**Device name** in the backup file.
15. 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 **Error name** field displays any problems encountered during the loading process.

    Cancelling 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**.
16. When you select the **Stop** option in the Load Pseudo-ACD Data - Acknowledge window, Supervisor updates the **Status** field at the top of the Load Pseudo-ACD Data window with the timestamp during which the loading of the pseudo-acd data was completed.

# Storage intervals

The Storage Intervals window allows changes to be made to CMS which affect how and when data for the contact center is stored.

It is recommended that these settings are configured during installation and not changed because subsequent changes will affect data storage and report data coverage.

## Before using Storage intervals

The following items should be read and understood before working with the Storage Intervals window:

- CMS must be in single-user mode and the data collection must be off before modifications to these settings can be made.
- Do not open another Storage Intervals window if one is already being used to alter these settings. The loss of data tables can result if multiple Storage Intervals windows are used.
- Free space allocation, data storage allocation, and storage intervals closely tied. A change in storage intervals may require adjustment of data storage or storage times in the Data Storage Allocation window. The more frequently CMS archives data, the more storage space is required.

## Permissions for Storage intervals

Depending on the procedure that you want to perform, you need the following permissions:

- To view settings in the Storage Intervals window, the user ID used to log in to this Supervisor session requires “read” permission for the CMS System Setup feature.
- To modify settings in the Storage Intervals window, the user ID used to log in to this Supervisor session requires “write” permission for the CMS System Setup feature.

## Viewing storage interval settings

### About this task

This section provides the procedure for viewing the Storage Intervals settings for contact center data.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS 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. Select **OK**.

   Supervisor displays the Storage Intervals window.

# About changing the intrahour interval

This section provides the procedure for changing the rate at which CMS archives data within a one-hour time period.

## Before changing the intrahour interval

The following items should be read and understood before changing the intrahour interval setting:

- Changing the intrahour interval can result in a lengthy process as CMS must make modifications to all previously collected data.
- Increasing the frequency of the intrahour interval results in the contact center data taking more storage space. This can require changes to the length of time for which CMS stores contact center data. To change the length of time which data is stored, use the Data Storage Allocation window.
- Perform a full backup of historical data before making changes to the intrahour interval or data collection times or dates. After the changes are made, perform another full backup of historical data.
- Real-time reports use the intrahour interval when displaying data. Cumulative data is reset to zero at the beginning of each intrahour interval.

## Changing the intrahour interval

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS 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. Select **OK**.

   Supervisor displays the Storage Intervals window.

5. In the **Intrahour interval (select one)** group, select the option for the rate at which CMS archives contact 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 Changing the data collection state on page 273 for information on this procedure.

8. Return CMS to multi-user mode.

   See the Changing the CMS state on page 271 for information on this procedure.

# About changing switch time zone

This section provides the procedure on changing the time zone settings for an ACD so that it matches the time zone of the CMS server. Use this feature if you want the CMS title bar to show the time where the CMS is located instead of the master ACD time. If you do not use this feature, the CMS title bar will automatically display the master ACD time.

This procedure is only necessary for those configurations where an ACD resides in a different time zone than that of the CMS server, but you want the title bar to display the CMS time.

## Before changing switch time zone

The following items should be read and understood before changing the time zone for an ACD:

- CMS must be in single-user mode and the data collection must be off before modifications to these settings can be made.
- If an ACD is connected to a CMS server in the same time zone, the **Switch time zone offset** field should be set to **0**.
- This procedure does *not* effect the time stamps on the CMS reports, real time or historical.
- This procedure does *not* effect the timetable schedule for timetables set to run at local times for a specific ACD.

## Changing switch time zone

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS 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. Select **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 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 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 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 Unix 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 Changing the data collection state on page 273 for information on this procedure.

8. Return CMS to multi-user mode.

   See Changing the CMS state on page 271 for information on this procedure.

# About modifying data summarizing settings

This section provides the procedure for modifying the times and days for which contact center data is recorded and summarized.

## Before modifying data summarizing settings

The following items should be read and understood before modifying data summarizing settings:

- CMS must be in single-user mode and the data collection must be off before modifications to these settings can be made.
- Perform a full backup of historical data before making changes to the data collection times or dates. After the changes are made, perform another full backup of historical data.
- When a weekly report is requested, the date entered must correspond to the day of the week specified in the **Week start day** field.

  **Caution:**

  Do not open another Storage Intervals window and attempt to change other settings while modifying these settings. Doing so can result in the loss of database tables.

# Modifying data summarizing settings

## Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the CMS 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. Select **OK**.

   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 contact 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 contact 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 Changing the data collection state on page 273 for information on this procedure.
12. Return CMS to multi-user mode.

    See Changing the CMS state on page 271 for information on this procedure.

# Switch setup

Use the Switch Setup window to view the following information:

- Communication Manager setup information - ACD name, release, and activated features, such as Call Vectoring, Call Prompting, and Expert Agent Selection (EAS)
- CMS software information - release, version, and load
- Phantom abandon call timer values

## Before using Switch Setup

The following items should be read and understood before working with the Switch Setup window:

- The Switch Setup window can only display real ACDs. Pseudo-ACDs are not supported.
- This window can only be used to view information. No modifications to the ACD can be made through Supervisor.
- The phantom abandon call timer is used to determine which calls to count as abandoned calls rather than ACD call. If the call lasts less than the number of seconds specified, the Communication Manager system considers it an abandoned call. The feature is useful in areas where the central office does not provide disconnect supervision on trunks.
- To display an ACD name in the Switch Setup window, it must first have the name assigned in the Dictionary. See Adding an ACD name on page 46 for more information on this procedure.

## Permissions for Switch Setup

Depending on the procedure that you want to perform, you need the following permissions:

- To view ACDs in the Switch Setup window, the user ID used to log in to this Supervisor session requires “read” permission for the feature.

## Viewing switch setup data

### About this task

This section provides the procedure for viewing setup information for an ACD.

### Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the System Setup window.

2. In the **Operations** list, highlight **Switch Setup**.
3. Select **OK**.

   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**.

   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

## About this task

This section provides the procedure for viewing setup information for all ACDs.

## Procedure

1. From the Controller window, select **Tools** > **System Setup**.

   Supervisor displays the System Setup window.
2. In the **Operations** list, highlight **Switch Setup**.
3. Select **OK**.

   Supervisor displays the Switch Setup window.
4. From the menu bar, select **Actions** > **List all**.

   Supervisor displays a secondary window listing all ACDs and their associated settings.

# Chapter 12: Maintaining CMS

## Maintaining CMS

Maintaining a CMS server consists of routine tasks such as backing up data, checking the status of the CMS connection to the switch, and viewing the maintenance error log.

The **Maintenance** menu allows you to perform the following tasks:

- Initiate CMS backups and restores
- Assign a name and description to the full path name for a device used for data backups
- Assign printer names and options
- Monitor the data link between the CMS server and the switch
- View the measurement status of a particular ACD
- View the Maintenance Error Log
- View the archiving status

## Before using the Maintenance window

If an ACD Group is selected as the current ACD in the Maintenance window, only those operations that are valid for the ACD Group will appear in the **Operations** list.

## ACD status

The ACD Status window displays information about the current selected ACD, including the number of splits or skills, agents logged in, trunk groups, trunks, VDNs, vectors (if your company has purchased Call Vectoring), and measured splits. You can also use the ACD status window to request a complete set of translations from a specific ACD. The ACD status window will look different if your switch has Expert Agent Selection (EAS).

### Before using ACD status

You should read and understand the following items before viewing the status of an ACD through the Maintenance subsystem:

- The link must be up between the Communication Manager system and the CMS , if you want to view the status or request translations from a specific ACD.

- Data collection must be on for the specific ACD for the translations you request.
- The data will be lost during a translations pump-up. An acknowledgement window will ask if you want to proceed.

## Permissions for ACD status

Depending on the procedure you wish to perform, you will need the following permissions:

- To view the ACD Status window, you need to have “read” permission for the Maintenance subsystem.
- To request translations, you need to have “write” permission for the Maintenance subsystem.

## Viewing ACD status

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Highlight **ACD Status** in the **Operations** list.
4. Select **OK**.

   Supervisor displays the ACD Status window.

   For additional information on the fields in the ACD Status window, see Description of the ACD Status window - with EAS on page 310 and Description of the ACD Status window - without EAS on page 310.

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

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.

3. Highlight **ACD Status** in the **Operations** list.
4. Select **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.

## Description of the ACD Status window - with EAS

The following table provides the descriptions of the fields on the ACD Status window where Expert Agent Selection (EAS) is installed:

| Name | Description |
|---|---|
| **Skills** | The skills measured by CMS. |
| **Skill members in use** | The agent/skill pairs logged in at the time the ACD Status window was opened. |
| **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. |
| **Error name** | The errors encountered by the ACD. |

## Description of the ACD Status window - without EAS

The following table provides the descriptions of the fields on the **ACD Status** window where Expert Agent Selection (EAS) is not installed:

| Name | Description |
|---|---|
| **CMS is measuring** | The current value of each of the following items. |
| **Splits** | The splits measured by CMS . |
| **Total split members** | The agent/split pairs logged in at the time the **ACD Status** window was opened. |
| **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 ACD. |
| **Vectors** | The vectors available for use in the selected ACD. |
| **Measured splits** | The number of measured splits in a selected ACD. |
| **Error name** | Errors encountered by the ACD. |

### Requesting ACD translations

The ACD translation request was used to manually synchronize the measure contact center entities from an ACD to the CMS server.

**Important:**

This functionality was available for Generic 2 and System 85 switches and is no longer needed when your CMS server is connected to a Communication Manager system. The system downloads the ACD translations automatically when changes are made to measured contact center entities.

**Important:**

If you request an ACD translation, contact center data is interrupted on the Communication Manager system and can result in inaccurate reports.

# Archiving status

Use the Archiving Status window to display the status, date, and time of the last archive for interval, daily, weekly, and monthly data. This information can help you decide when to turn off data collection or change your archiving times to minimize data loss.

**Note:**

In CMS R18, 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.

## Before using Archiving Status

Read and understand the following items before working with the Archiving Status window:

- “Archive” indicates that CMS is storing interval, daily, weekly, and monthly data in the appropriate database tables.
- The three archive status indications are:
  - “Finished” - The last archive has been completed
  - “Running” - The archive is currently running
  - “Not run” - The archive has never run

## Permissions for Archiving Status

You need “read” permission for the Maintenance subsystem to view the Archiving Status window.

# Viewing the archiving status of a single ACD

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Archiving Status** in the **Operations** list.
4. Select **OK**.

   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**.

   Supervisor displays the Archiving Status - List All window.

   For more detailed information about the Archiving Status - List All window, see Description of the Archiving Status - List All window on page 313.

   **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 the archiving status of all ACDs

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Archiving Status** in the **Operations** list.
4. Select **OK**.

   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**.

   Supervisor displays the Archiving Status - List All window.

   For more detailed information about the Archiving Status - List All window, see Description of the Archiving Status - List All window on page 313.

## Description of the Archiving Status - List All window

The following table lists the fields and the associated descriptions for the Archiving Status - List All window:

| Name | Description |
|---|---|
| **Status** | The archiving status of the ACD. |
| **Date** | The date the last archive completed for the ACD. |
| **Time** | The time the last archive completed for the ACD. |
| **Next scheduled** | The date and time of the next-scheduled archive.<br>Dates and times will not appear for the Interval archiving. Interval archives occur at the end of each interval: 15, 30, or 60 minutes. |

# Backup/restore devices

Use the Backup/Restore Devices window to assign a name and description to a full path name for a device. The device name is used for data backup, data migration, data restore, and for loading a pseudo-ACD. The maintenance device menu now displays **Tape** and **Other** options for Device Type to the user to choose either **Tape** as a backup/restore device or **Other** which includes USB storage device and network mounted file system.

The LAN Backup feature of CMS is not available through the Supervisor interface. For more information regarding this feature, see the *Avaya Call Management System LAN Backup User Guide*.

## Permissions for Backup/Restore Devices

Depending on the procedure you wish to perform, you need the following permissions:

- You need “read” permission for the Maintenance subsystem to view the Backup/Restore Devices window.
- You need “write” permission for the Maintenance subsystem to add, delete or modify any backup/restore devices.

# Viewing a backup/restore device

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Select **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/restore devices

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Select **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/restore device

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.

4. Select **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**, it's 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/restore device

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Select **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/restore device

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Backup/Restore Devices** in the **Operations** list.
4. Select **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.

# Data Backup

There are two types of data backup available through CMS , CMSADM and Maintenance. Avaya CMS can backup and restore while the data collection remains on. This ability helps minimize data loss. However, once a CMSADM backup is started, new logins through the ASCII interface, through Avaya CMS Supervisor, and through Avaya Visual Vectors are blocked. A maintenance restore of CMS System Administration data or ACD Administration data requires Avaya CMS to be in single-user mode.

The LAN Backup feature of CMS is not available through the Supervisor interface. For more information regarding this feature, see the *Avaya Call Management System LAN Backup User Guide*.

## CMSADM backup

The CMSADM backup saves all of the system data on the computer onto a tape or other device such as USB or network.

The CMSADM backup includes the following data:

- Operating system files and programs
- CMS programs
- Non- CMS customer data placed on the computer

The CMSADM backup will not save CMS database tables. For complete data recovery, both CMSADM and maintenance backups are required.

This type of backup is only performed through the CMS ASCII interface. A Supervisor interface for this type of backup is not available.

## Maintenance backup

Maintenance backups are used to archive and restore CMS data. If you do not have a backup, data is lost and cannot be recovered in the event of system or disk failure. The frequency of your backups is determined by how much data your contact center is willing to lose.

Through Supervisor, you can use the Backup Data operation on the Maintenance window to perform full and incremental backups of CMS historical and administration data.

## Tape drives and cartridges

The following table lists the models of tape drives that are supported.

| Tape drive | Tape description |
|---|---|
| DAT 72 | DDS compliant 170 meter 36/<br>72-GB DAT cartridge 4 mm |
| LTO-4 | 820 meter 800 GB LTO cartridge 12.65 mm |

## USB/network backup/restore devices

The screen containing Backup/Restore Devices now displays **Tape** and **Other** options to the user under the **Device name** field. The **Other** option may be either a USB storage device or network device, and does not include any location on the CMS disk itself. If the device chosen for a CMS Maintenance Backup is of type **Other**, the backup file is named using the tape label convention. This file is a compressed file. The CMSADM backup can also be performed on the USB or network devices. The backup file generated by CMSADM backup is labeled with a unique label that includes date, time, and machine name, and is not compressed.

# Things to consider when backing up or restoring data

Avaya recommends that you back up your CMS system data on a monthly basis and you back up your CMS ACD data on a daily basis. If you are using tape, the backup tapes should be stored in a safe location, easily retrievable, correctly labeled, and replaced when worn out. Running system backups is no longer service affecting, but the backups will impact the performance of the CMS system. It is recommended that you run backups when CMS system activity is low.

**Note:**

The **Maintenance** > **Restore** Data option is only used 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 then the data needs to be migrated using the **System Setup** > **R3 Migrate Data** option.

For example, if the CMS version on the backup media is r17ab.g and the CMS version installed on the system is r17ab.g then the data can be restored. If the CMS version on the backup media is r17ab.c and the CMS version installed on the system is r17ab.g then the data must be migrated.

This section presents several factors that will impact the amount of time it takes to backup or restore your data and presents options to reduce backup and restore times.

## Factors that impact backup and restore times

The amount of time it takes to back up or restore data depends on the:

- Amount of data - An increase in the amount of data will cause an increase in the amount of time it takes to back up or restore the data. Some factors that will 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 that will have to be backed up or restored. When the CMS system reaches a predetermined threshold for data storage, the oldest record is deleted so that the newest record can be stored. Twice the amount of data is stored if you set your data storage for 62 days instead of 31 days.
  - Interval size - Shorter intervals generate more data. A 15 minute interval will generate significantly more data than a 60 minute interval.
- System load - Processes that require a large amount 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 will use a large amount of system resources.
  - Archiving data - Archiving a large amount of data will use a large amount of system resources.
- Necessity for manually changing backup tapes - If the amount of data exceeds the capacity of a single backup tape, someone must monitor the system and manually load additional tapes. A

data backup or restore does not finish unless someone is able to load tapes into the tape device as needed.

- The device you are backing up to. If you are backing up to a USB storage device or a network mounted directory, the backup times will be longer than the LTO tape device. You may want to consider a backup strategy of the following type:
  - Performing full backups only once a week
  - Performing incremental backups on three or four other days of the week

  For example, you might want to perform your full backup on Saturday nights, and your incremental backups on Mondays, Wednesdays, and Fridays.

## Reducing tape backup and restore times

If you do not take steps to optimize your CMS backup and restore times, you will begin to experience performance issues. Your CMS system performance will drop if the backup continues to run when contact center activity increases. With the increased CMS capacities that are now available, CMS backups and restores could take much longer to complete than they have in the past.

Due to the higher capacity limits and fewer database restrictions, the maintenance backup time can take longer with CMS R16 than previous releases. In some cases the extended amount of time may be unacceptable to customers. 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 will meet your data collection needs.
- Select the minimum data storage times that will meet 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 time that is different from data archiving.
- Schedule routine backups to occur when CMS system activity is low.
- Use the new binary backup that is provided with CMS R16.
- Reduce the amount of data being stored so only one backup tape is needed to store the data.
- Upgrade your CMS system to a more powerful hardware platform or add additional memory and CPUs.

## Alternate methods for backing up and restoring data

### LAN Backup

If you need a higher capacity process for backing up and restoring your data, you may want to use the Avaya CMS LAN Backup feature. The Avaya CMS LAN Backup feature provides an alternative to the traditional method of backing up and restoring data which requires you to manage your tape library, your USB storage device(s), or your network file space. LAN Backup allows you to back up CMS data and system information over a local area network (LAN) to a storage manager, which

manages the number of backups and their location. CMS supports the use of Tivoli Storage Manager and Symantec Netbackup storage managers.

The *Avaya Call Management System LAN Backup User Guide* provides information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

### Binary Backup

To speed up the time it takes to run a backup, you can use the new binary backup that is provided with CMS R16. The CMS R16 binary backup procedure can write data to a tape drive, a USB storage device or over the network. Similar to the LAN backup and restore processes, the binary backup does not support table level restore and data migration. A binary backup is a good alternative for disaster recovery. In general, a binary backup to a tape device or a USB storage device, of a fully loaded CMS system takes approximately 30 minutes. A binary backup over a network will vary depending upon the network bandwidth.

## Determining the duration of a standard CMS R16 full Maintenance Backup to tape

### About this task

To determine the duration to do a full maintenance backup to tape, you must determine the amount of used disc space on the system.

### Procedure

1. Log in to the CMS server as root user.
2. Run **cms** > **System Setup** > **Free Space Allocation**.
3. Refer to the Space Used to Date column for each ACD that appears on the screen.
4. Sum the total space used for all ACDs (shown in kilobytes).
5. Divide the total space used by 1000 (approximate speed of backup to tape), then by 3600 (seconds in an hour).

### Result

For example, if the total space used is 10,000,000 kilobytes (10 million), then run the calculation 10000000/1000/3600. This equals 2.77, which is the number of hours that a full maintenance backup to tape will take for all ACDs on the system. Note that you can use this calculation on each individual ACD to determine the time to back up a single ACD.

## Restoring or Migrating from a non-tape device

When your backup device is of type **Other**, it means that you have specified either a USB storage device or a network mount point as your chosen location for maintenance backups. It is your responsibility to manage this storage area. You must keep enough free space in your chosen “Other” device to allow for scheduled maintenance backups. This means that you must periodically check the network mount point or the USB storage device for available space, and remove older backup files to allow for more storage. If you do not wish to manage the non-tape storage area, you should consider the LAN Backup feature described above. If you are using a network directory, ensure that you include this directory in the system backups of your company's UNIX or non-CMS servers.

You should keep in mind the following recommendations for maintenance of your “Other” storage area:

- Do not store CMSADM backup files and Maintenance backup files on the same USB storage device or in the same network mount point . Keep a separate set of USB storage devices for your CMSADM backups (at least two), or create separate network directories for your CMSADM backups with adequate storage for at least two backups.
- Do not store more than one full Maintenance backup and 6 incremental backups on one USB storage device.
- Keep at least two full Maintenance backups and the accompanying week's worth of incremental backups on two separate USB storage devices. If you are using a network directory, allow 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.

When performing a Maintenance restore, if you check the **Restore from the latest backup?** box, the logic used to determine the latest backup is as follows:

- The backup file labeled with the latest full backup for the given server
- The backup file labeled with the next latest full backup if the latest cannot be found
- If no full backups can be located for the given server, the latest incremental backup is looked for

**Note:**

All the above steps are relative to the “Other” device location (USB storage device or network mount point).

You may wish to control which backup file is used for a restore or a migration. This is similar to mounting your chosen tape and performing the restore or migrate from that tape. If you wish to control which backup file is used for a restore, follow the steps below:

- On your “Other” storage device, create a UNIX file named `restore_list` which will contain the names of the files you wish to restore from. These files must be ordered in the restore list beginning with the first backup you wish to restore from, to the last backup. For example, if your CMS maintenance backups on server finch begin on October 4, 2010 with a full backup and are followed by an incremental backup on October 6, October 8, and October 10, you would see the following files in your backup storage area or on your USB storage device:

```
# ls -rt *finch*
CMS-101004-02-LSAC-00-F-01-05-finch0000000000
CMS-101006-02-LSAC-00-I-01-05-finch0000000000
CMS-101008-02-LSAC-00-I-01-05-finch0000000000
CMS-101010-02-LSAC-00-I-01-05-finch0000000000
```

- To create a list of these file names in a file named “ restore_list ”, run the following command:

```
# ls -rt *finch* > restore_list
```

- Once the restore list is created, you may begin your Maintenance restore. Do not check the **Restore from the latest backup?** box so that “restore_list” is used. As each of the backups is restored, it is removed from the list. When you have restored all backups, you may choose **Stop** to end the restore.

# About adding a Full Maintenance Backup Timetable for an ACD

## Before adding a Full Maintenance Backup Timetable for an ACD

The following items should be read and understood before performing maintenance backups:

- Maintenance backups to tape require that backup tapes be manually rotated. The frequency of the rotation depends on the dates and times of all scheduled backups. By creating individual ACD backups, the risk of data being overwritten is increased. Timetable backups must be scheduled such that the tape can be manually rotated before another scheduled backup runs. Failing to rotate the tape will cause the data to be overwritten by the next scheduled backup.
- If you are backing up to tape, a sufficient supply of tapes should be available so that tapes can be rotated. One common plan is to keep seven tapes in stock and recycle them daily. A new tape is used each day of the week, and each week the sequence is repeated.
- The maintenance backups do not back up the CMS software, operating system files, or non-CMS customer data on the system. For complete data recovery, both CMSADM and all maintenance backups are required.
- Running backups during archiving may cause performance problems. For best performance, run backups either before or after the archiving process.

**Note:**

When doing this procedure, use the arrow keys or type the first few unique letters of an item to highlight the item.

## Adding a Full Maintenance Backup Timetable for an ACD

### Procedure

1. Log in to CMS.
2. From the **Main Menu**, press `F4` to access the 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 “fullBackup timetable” to a unique name that will identify the ACD being backed up, such as “acd1fullBackup” for ACD 1.

10. Press `Enter`.
11. Enter the letter `a` to highlight the **Add** item.
12. Press `Enter`.

    Key strokes for building the new timetable will now be tracked. A message appears at the bottom of the Main Menu with the words `Keeping Entries`.
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 get out of the **Options** menu.
23. Enter the letter `m` to highlight the **Maintenance** item from the **Main Menu**.
24. Press `Enter`.
25. Do one of the following:
    - If the **Back Up Data** item is already be highlighted, press `Enter`.
    - If the **Back Up Data** item is not highlighted, enter the letters `back` to select **Back Up Data**, and press `Enter`.
26. Use the down arrow key to move to the **ACD(s) to back up** field.
27. Place an `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** options.
33. **Stop** should be highlighted, press `Enter`. If **Stop** is not highlighted, enter the letters `st` to highlight **Stop**.
34. Press `Enter`.
35. Enter `y` when prompted to save the changes.

36. Press `Enter`.

    The timetable has been created. The system returns to the Timetable screen for the timetable just created.

37. As needed, modify the dates and times you want the timetable to run. If changes are made:

    a. Press `Enter`.

    b. Enter the letter `m` to select the **Modify** item.

    c. Press `Enter`.

38. Press `Enter`.

39. Press `F5` to exit the **Timetable** menu.

40. From the **Main Menu**, press `F4` to access the CMS timetables.

41. Select **Timetable**.

42. Press `Ctrl+Z` to clear out the entries in the form.

43. Press `Enter`.

44. Enter the letter `l` to select the **List all** item.

    A list of all Timetables is displayed.

45. Use the arrow keys to locate the Timetable just created. If the timetable is not found repeat this procedure.

46. Press `F5` to exit the Timetable: **List all** menu.

47. Press `F5` to exit the **Timetable** menu.

# About performing a CMSADM backup

The CMSADM backup should be done at the following times:

- Once a month (This is always the customer's responsibility.)
- After the CMS is provisioned (If using tape, never use the original tapes made during provisioning.)
- Before and after the CMS software is upgraded
- After the system has been set up in the factory (performed by factory personnel).

  This backup contains the default factory configuration. These tapes should be saved if the system must be reinstalled in the field.

  **Note:**

  The factory will no longer provide a CMSADM backup as of R17.0.

**Important:**

If you are backing up to tape, use a new set of backup tapes for the monthly CMSADM backup. Do NOT use the original sets of factory backup tapes or provisioning backup tapes. Make sure that there are enough tapes for the new backup.

## Before performing a CMSADM backup

The following items should be read and understood before beginning to work with removable media on your Sun Microsystems, Inc. Solaris or Linux® system.

- Prior to running a cmsadm backup, you are recommended to restart the CMS server.
- If you choose tape as your backup device, verify that you are using the correct tape for the tape drive on your system.
- If you choose USB storage device as your backup device, verify that you are using a recommended USB device.
- Backup tapes and USB storage devices can wear out. Be sure to refresh your supply of backup devices at appropriate intervals.

## Permissions for performing a CMSADM backup

In order to perform a CMSADM backup you need “write” permission for the Unix (r) subsystem. Only employees with administrative responsibilities should be given the permissions and passwords.

## Performing a CMSADM backup

### Procedure

1. Log in to the CMS system as root and open a terminal window.

   See Logging in to CMS from the server console on page 373 for additional information.

2. Verify that the operating system of the computer is in a multi-user state (2 or 3). To check if you are in the multi-user state, enter `who -r`
3. Enter `cmsadm` and press the `Enter` key:

   The **Avaya Call Management System Administration Menu** is displayed.

4. Enter the number associated with the backup option.

   ```
   Choose a backup device:
   1) Tape
   2) Other
   Enter choice (1-2):
   ```

   Depending upon your preferences, choose your backup device. If you choose Tape, continue with step 5. If you choose Other, continue with step 9.

5. Press the `Enter` key.

   The backup process begins.

If more than one tape is required, the program displays the following message:

```
End of medium on "output".
Please remove the current tape, number it,
insert tape number x, and press Enter
```

If you receive the message displayed above, insert the next tape and allow it to rewind. When it is properly positioned, press the `Enter` key.

6. When the backup is completed, the system displays information according to the number of tapes that are required for the backup:
   - If the number of tapes required is one, the system displays the following message:

     ```
     xxxxxxx blocks
     Tape 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.  . . . .
     Please label the backup tape(s) with the date and the current CMS version
     (Rxxxxx.x)
     ```

   - If the number of tapes required is more than one, the system displays the following message:

     ```
     xxxxxxx blocks
     Tape Verification
     Insert the first tape
     Press Return to proceed :
     ```

   If you receive the message displayed above, insert the first tape used in the backup and press the `Enter` key. Wait for the tape drive light-emitting diode (LED) to stop blinking before you remove the tape. When prompted, repeat this process for any additional tapes generated by the backup process.

   When the final tape is verified, CMS displays the following message:

   ```
   xxxxxxx blocks
   Tape 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.  . . . .
   Please label the backup tape(s) with the date and the current CMS version
   (Rxxxxx.x)
   ```

7. Label all tapes with the following information:
   - Tape number
   - Date of backup
   - Current version of Avaya CMS
8. Set the tape write-protect switch to read-only and put the tapes in a safe location.

   If you have problems performing a CMSADM backup to tape, see the document, *Software Installation, Maintenance, and Troubleshooting*.

   The system displays the following message:

   ```
   Enter backup path (must not be located on CMS disk):
   ```

9. Enter the directory of the network mounted file system that you wish to use for your backup, or the mount point of your USB storage device, and press the `Enter` key.

If the directory is accessible for the backup, CMS displays the following message:

```
Using file /sss/CMSADM-<CMS load name>-<date-time>-<machine name>
```

After the backup has been written, it is verified, and CMS displays the following message:

```
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>
```

# About performing a maintenance backup

Since new data is written each day, you should frequently back up this data. Both the full and incremental backups can be scheduled to run automatically on a timetable.

## Before performing a maintenance backup

The following items should be read and understood before performing a maintenance backup:

- If you backup to tape, a sufficient supply of tapes should be available so that tapes can be rotated. One common plan is to keep seven tapes in stock and recycle them daily. A new tape is used each day of the week, and each week the sequence is repeated.
- Backups run in the background. You can exit the Backup Data window without affecting the backup.
- Running backups during archiving may cause performance problems. For best performance, run backups either before or after the archiving process.
- Currently supported tape drives can accommodate a full backup on one tape. Incremental backups may not need to be done. Full backups can be scheduled to run every day.

**Important:**

The maintenance backup does “not” back up the CMS software, operating system files or non- CMS customer data on the system. For complete data recovery, both CMSADM and maintenance backups are required. See About performing a CMSADM backup on page 324 for instructions on how to run a CMSADM backup.

## Permissions for performing a maintenance backup

To run a Maintenance backup you need “write” permission to the Maintenance subsystem.

## Performing a maintenance backup

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select 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. Select **OK**.

   Supervisor displays the Backup Data window.
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 being 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 error messages on page 330 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 will back up data from all real ACDs (not pseudo-ACDs).
   - The **Current ACD** option will back 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 the maximum amount of data, clear the types of data you do not want backed up.

   For an explanation of the **Data to back up** check box options, see The Backup Data window on page 328 .
10. From the **Actions** menu, select **Run**.

    The backup process begins. When the backup process is complete, Supervisor displays an acknowledgement window.

    If you have selected “Tape” as your backup device and your backup requires more than one tape, you will receive a message telling you to mount another volume to complete the backup.
11. When the backup completes, remove and label the tape(s) if your backup device is tape.

# Description of the Backup Data window

## The Backup Data window

Fields in the Backup Data window are described as follows.

| Name | Description |
|---|---|
| **Backups completed today** | Shows the number of backups completed for the current day. |
| **Status** | Shows the status of the current or most recent backup and what is currently being backed up. |
| **Errors** | Shows any errors found in the backup. |
| **Device name** | Displays the name of the backup device. |
| **Verify tape can be read after backup?** | Check box to request that the data be reread to ensure that the data has been backed up properly. This check box applies to tape backups only. |
| **ACD(s) to back up** | Options to perform a backup of all ACDs or a single ACD. |
| **Data to back up** | Series of check boxes where you can select the types of data you want to back up. See Data to back up descriptions on page 329 for additional information. |

## Data to back up descriptions

Descriptions of the types of data that may be backed up are described as follows.

| Name | Description |
|---|---|
| **Local System administration data** | Includes IP addresses, port numbers, and other data configured at installation. |
| **CMS System administration data** | Includes user permissions, feature access permissions, **Main Menu** additional data, timetable, printer administration, default values, color choices, and custom report definitions (not the data associated with custom reports). |
| **ACD-specific administration data** | Includes Forecast data (if the feature is active), call work code administration data, VDN administration data, data storage allocation data, exception administration data, agent trace data (historical list of agents traced), and ACD-specific Dictionary names. |
| **Historical data** | Includes the historical data stored in the CMS database. There are two options for backing up historical data, Full and Incremental<br>Full: includes data for all the time periods in the historical database. You must do a full backup before the first incremental backup. It is recommended that you periodically (for example, once a week) do a full backup of your system.<br>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** | Includes all data from Informix tables with names that start with “c_”. The table definitions for non- CMS Informix tables are not backed up, these would be captured by a CMSADM backup. |
| **Specific tables** | Allows you to back up data from specific data tables. |

*Table continues…*

| Name | Description |
|---|---|
| | To backup specific tables, select **Actions** > **Select tables**. Supervisor then displays the Backup Data - Select Tables window. The Table name column shows the name of the data table and the Description column shows the type of data in the table. Select the check boxes for the tables you want to back up. Close the window when finished. |

## Common backup error messages

Common error messages and their solutions are described as follows.

| Error | Solution |
|---|---|
| `CMS cannot access the specified device.` | Enter a new device name. |
| `The volume mounted is bad (corrupt).` | Mount a new volume. |
| `A volume tape is not mounted in the drive.` | Mount a volume. |
| `The volume mounted contains CMS data that you might not want to overwrite.` | 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.` | You have to mount a different volume. Unless you direct CMS to do so, it does not let you overwrite your last backup. |
| `The volume mounted has errors.` | Mount another volume. |
| `A table cannot be backed up.` | You must decide if you want to skip the table and continue or cancel the backup. |

## Labeling the backup volume

After a successful backup, CMS generates backup volume labels depending on the rules that apply to the particular backup device being used. This is “Tape” or “Other” in the new CMS systems.

Depending on the circumstances, CMS provides the following information:

- An acknowledgement window displays the final backup information. If the backup was scheduled on a timetable, the information is recorded in the Maintenance Error Log.
- An acknowledgement window displays a message indicating when a backup can write to a previously used tape.

### Example backup information format and interpretation

```
0001 CMS-NNNNNN-NN-LLLL-NN-L-NN
0002  |    |    |   |   |  | |
0003  1    2    3   4   5  6 7
```

The following table provides information on the labels of backup tapes.

| Part # | Code | Meaning |
|---|---|---|
| 1 | CMS | System name |
| 2 | NNNNNN | Year, month and day of the backup (yymmdd) |

*Table continues…*

| Part # | Code | Meaning |
|---|---|---|
| 3 | NN | Number of backups for this day |
| 4 | LLLL | Type of data backed up:<br>A - ACD-specific administration data and historical data<br>C - custom data<br>H - historical data<br>L - local system administration data<br>M - ACD-specific administration data<br>S - CMS system data<br>X - no backup |
| 5 | NN | Number of the ACD (`00` means **All ACDs** were selected on the Backup Data window) |
| 6 | L | Backup mode (`F` for Full, `I` for Incremental) |
| 7 | NN | The tape number if this tape was part of a multi-tape backup. |

If the device type is “Other”, the file name for Maintenance backup has the same format as the tape label. For example, if you have performed a full Maintenance backup on your CMS server named sapsucker for all ACDs and all data types on September 18, 2010, the file name will appear in the directory as `CMS-100918-01-LSAC-00-F-01`.

## Recovery kit

The recovery kit is composed of the backup media that the Avaya Technical Services Organization needs to restore service to your system if major problems occur. This kit should be stored in a secure location in order to minimize the time your system is out of service.

### Recovery kit contents

The Recovery Kit contains the most recent:

- CMSADM backup tape (if your chosen backup device is tape)
- Full Maintenance backup tape and any Incremental backup tapes since the latest full backup (if your chosen backup device is tape)
- CMS Load DVD
- Patching DVDs
- If your chosen backup device is USB storage device, then your Recovery Kit should contain the appropriate USB storage device containing your CMSADM backup, along with the USB storage device containing your Full Maintenance backup.
- If your chosen backup device is network, you must manage the location of the CMSADM and Maintenance backups yourself.

## Binary backup of database

The binary backup procedure will backup the entire database in binary form. Similar to the LAN backup and restore process, this procedure does not allow System data, Call Center Administration data or Historical data to be restored individually.

**Important:**

Unlike tape devices, USB storage devices and network mount points must be monitored to ensure they are accessible. Timetables and Backup/Restore devices using USB storage devices and network mount points must be able to access these media sources to function properly. Remember to remount all non-tape media sources used by CMS, after any reboot of the system.

- If the binary backup is to tape, continue with Binary backup of database to tape.
- If the binary backup is to a USB storage device, continue with Binary backup of database to a USB storage device.
- If the binary backup is to a network mount point, continue with Binary backup of database to a network mount point.

## Taking a binary backup of database to tape

### Procedure

1. Log in to the CMS server as root.
2. Insert a blank tape into the tape drive.
3. Enter:

   `/cms/install/bin/db_backup <tape_device>`

   If a *tape_device* is not entered, the default device will be `/dev/rmt/0c`.

   **Note:**

   You can set up a cron job to run this command on a regular basis.

## Taking a binary backup of database to a USB storage device

### About this task

**Important:**

USB storage device backups are considered permissive use. A new procedure is supplied to facilitate USB storage device backups. You should setup and verify as Avaya does not support debugging and setup of USB storage device backups.

As an option, the CMS server can be configured to utilize a USB storage device for the binary backup and restore. The binary backup can write backup data to a USB storage device. This procedure requires knowledge and experience with configuring and mounting USB storage devices.

**Important:**

Unlike a backup to a tape drive, the speed of a USB storage device is determined by the speed of the USB interfaces and the USB storage device.

### Procedure

1. Insert a USB storage device and create a mount point, then mount the USB storage device to the CMS server.

Refer to Configuring and Connecting a USB storage device in the *Avaya Software Installation, Maintenance, and Troubleshooting* document for more information.

2. Modify `/etc/vfstab` to make sure your USB storage device mount point can survive reboot.

   However, if the USB storage device is moved to a different USB location, the `/etc/vfstab` entry will fail to mount after a reboot.

   **Important:**

   Unlike tape devices, USB storage devices and network mount points must be monitored to make sure they are accessible. Timetables and Backup/Restore devices using the USB storage devices and network mount points must be able to access these media sources to function properly. Remember to remount all non-tape media sources used by CMS, after any reboot of the system.

3. Create an empty file using the touch command.

   Example: `touch /<USB_path>/<binary_backup_filename>`

4. Run the backup using the following command:

   `/cms/install/bin/db_backup /<USB_path>/<binary_backup_filename>`

   Avaya recommends that binary backup files written to USB storage devices be saved to another location for disaster recovery.

## Taking a binary backup of database to a network device

### About this task

**Important:**

Network backups are considered permissive use. A new procedure is supplied to facilitate network backups. You should setup and verify as Avaya does not support debugging and set up of network backups.

As an option, the CMS server can be configured to utilize a network device for the binary backup and restore. The binary backup can write backup data to a network device. This procedure requires knowledge and experience with network file system mounts.

**Important:**

Unlike a backup to a tape drive, the speed of a network backup is determined by your network bandwidth.

### Procedure

1. Create a mount point, then mount a network file system to the CMS server.
2. Modify `/etc/vfstab` to make sure your network file system can survive reboot.
3. Create an empty file using the **`touch`** command.

   Example: `touch /<mount_point_path>/<binary_backup_filename>`

4. Run the backup using the following command:

```
/cms/install/bin/db_backup /<mount_point_path>/
<binary_backup_filename>
```

**Example**

Example to mount nfs to a Linux® system:

```
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>
```

# Restoring data

Use the Restore Data window 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 have previously backed up. You can also select which ACDs and CMS data to restore.

The automatic restore will restore all CMS data files from your last backup. Most data is restored by the automatic restore procedure.

The manual restore will restore specific CMS data files. The manual restore is used only when a select number of database tables need to be restored. A manual restore gives you control over which data is restored.

## Before restoring data

The following items should be read and understood before attempting to restore data:

- The Data Collection and CMS states must be set as noted for the following backups:
  - Local system administration data - Data Collection off; CMS Single-user mode
  - CMS system administration data - Data Collection on or off; CMS Single-user mode
  - ACD system administration data - Data Collection on or off; CMS Single-user mode
  - Historical data, Non-CMS data, or specific tables - Data Collection on or off; CMS Single- or Multi-user mode.
- Data must be backed up before it can be restored. To ensure the safety of your data, you should frequently back up your system.
- The restore procedure is run in the background. The **Status** field on the Restore Data window allows you to monitor the status of the restore process as it is performed.
- You can turn CMS back to multi-user mode when the**Status** field displays `Restore is complete`.

# Permissions for restoring data

To restore data you need “write” permission for the Maintenance subsystem.

# Performing an automatic restore

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Select **Restore Data** in the **Operations** list.
4. Select **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 will show 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 will automatically be 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.

# Performing a manual restore

## 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. Cancelling 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 will receive an acknowledgment window asking if you are sure you want to cancel the restore.

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Select **Restore Data** in the **Operations** list.
4. Select **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 will show 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 will accept 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 back up** 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 337. 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 will corrupt 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**.

## Restore 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 *Avaya CMS Software, Installation, Maintenance, and Troubleshooting* document for instructions on how to perform a CMSADM restore and a binary restore.

# Recommendation to restart your CMS server

Avaya recommends that you restart your CMS server once every three months for preventative maintenance reasons. Rebooting your CMS server should not take longer than 10 minutes and should be performed when the CMS server load is low.

Although rebooting your CMS server is not a requirement, periodically rebooting your CMS server is a recommended procedure targeted at minimizing the risk of a system failure. Restarting your CMS server lessens the possibility of your system being adversely impacted by anomalies such as memory leaks, packet loss, un-released file locks, data inconsistency, data corruption, and storage space fragmentation. These types of problems are known to occur on any computer system.

Avaya offers a High Availability solution if data loss from a server restart is a concern. The Avaya CMS High Availability (HA) solution provides an uninterrupted data stream between the communication server and two HA CMS servers. If you use the HA solution, restart each CMS server at a different time to prevent data loss.

Avaya support personnel who are performing system maintenance work may require you to restart your CMS system. If Avaya support personnel require you to restart your CMS system, they will work with you to determine the best time to perform the restart. Avaya support personnel will make every attempt to determine the root cause of any problem that might require a restart.

# Connection status

You can use the Connection Status window to monitor the data link between the CMS processor and the Communication Manager system. You can also view the current status of the application, session, and connection layers of the link between the Communication Manager system and CMS .

## Permissions for Connection Status

You need “read” permission for the Maintenance subsystem to view the Connection Status window.

## Viewing the connection status of an ACD

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Connection Status** in the **Operations** list.
4. Select **OK**.

   Supervisor displays the Connection Status window.
5. In the **ACDs** field, enter the name or number of the ACD or ACD Group.

   See Description of the ACD Status window - with EAS on page 310 or Description of the ACD Status window - without EAS on page 310 for additional information about the fields present on the Connection Status window.
6. From the **Actions** menu, select **Find one**.

   Supervisor displays the Connection Status window for the selected ACD.

## Listing the connection status of all ACDs

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Select **Connection Status** in the **Operations** list.
4. Select **OK**.

   Supervisor displays the Connection Status window.

   See Description of the ACD Status window - with EAS on page 310 or Description of the ACD Status window - without EAS on page 310 for additional information about the Connection Status window fields.
5. If the **ACDs** field is not clear, select **Edit** > **Clear All**.
6. From the **Actions** menu select **List all**.

   Supervisor displays the Connection Status - List All window.

## Description of the Connection Status window

The Connection Status window contains the following fields.

| Field | Description | Status Messages |
|---|---|---|
| ACD(s) | Enter the number or name of the ACD(s) for which you would like to check the connection status. | - |
| Application | Displays status for the application layer of the link between the Communication Manager 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.<br>`translation pumpup` - CMS is receiving translations from the Communication Manager system. Translations are needed for CMS to correctly track the ACD calls coming from the switch.<br>`data transfer` - The application layer can receive and transmit data successfully.<br>`not collecting data` - Data collection has been turned off.<br>`CMS System Setup - The link has gone down.` To resume data collection, use the Data Collection window<br>`busied out (switch)` - The link between CMS and the Communication Manager system has been busied out from the switch side, usually to change switch translations. |
| Session | Displays status for the session layer of the link | `quiescent` - The session layer is inactive. This is the state of the session layer when the system is first powered on. |

*Table continues…*

| Field | Description | Status Messages |
|---|---|---|
| | between the Communication Manager system and CMS . | `waiting acceptance` - The session layer is waiting for the connection layer to become operational and for the remote session layer to accept the session.<br>`data transfer` - The session layer can now transmit and receive data from the Communication Manager system. |
| Connection | Displays status for the connection layer of the link between the Communication Manager system and CMS . | `quiescent` - Indicates that the connection is inactive. This is the state of the connection when the system is first powered on.<br>`out of order` - Something is wrong with the connection to the Communication Manager system. For example, the network connection between the Communication Manager system and CMS is currently unavailable.<br>`operational` - The connection can transmit information physically between the Communication Manager system and CMS .<br>`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. | |
| Errors | Displays any errors found. | |

# Administering a printer

Use the Printer Administration window to assign a name, description, and options to a printer that can be used by terminals connected to CMS . Users of Supervisor do not have access to printers assigned through this window but can use printers that are normally used through their Windows-based PC.

## Before administering a printer

- Before you can assign a printer in the Printer Administration window, the printer must already be administered in the operating system. See the *Avaya CMS Terminals, Printers, and Modems* document for additional information about the Port Administration Tool.
- The printer set up as the default printer will receive all terminal requested print jobs, unless otherwise specified by the user.

- 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 in the Printer Administration window can be used by terminal users as the default destination when printing historical reports.

## Permissions for administering a printer

Depending on the procedure you want to perform, you will need the following permissions:

- To view the Printer Administration window, you will need “read” permission for the Maintenance subsystem.
- To add, delete, or modify the Printer Administration window, you will need “write” permission for the Maintenance subsystem.

## Adding a new printer

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Printer Administration** in the **Operations** list.
4. Select **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**.

# Listing all printers

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Select **Printer Administration** in the **Operations** list.
4. Select **OK**.

   Supervisor displays the Printer Administration window.

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

   Supervisor displays the Printer Administration - List All window.

# Modifying printer options

## Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Operations** tab.
3. Select **Printer Administration** in the **Operations** list.
4. Select **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 on page 343, and Adding a new printer on page 341 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

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.
2. Select the **Operations** tab.
3. Select **Printer Administration** in the **Operations** list.
4. Select **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.

# Maintenance reports

This section provides information to help you set up and run the reports. Avaya CMS administrators and users with read permission for the Maintenance tool can display the Maintenance reports.

The Reports section of the Maintenance system helps you:

- Identify problems and facilitate the work necessary
- Aid Services personnel in clearing problems in your system

- Track changes made to the ACD by users

There are two reports available from the Maintenance subsystem:

- Maintenance Error Log on page 344
- ACD Administration Log on page 367

# Maintenance Error Log

Use the Maintenance Error Log Report to aid you in working on system problems and to aid Services personnel in clearing problems from your system. The Maintenance Error Log displays a chronological list of warnings, information, and errors detected by CMS .

## Before using Maintenance Error Log

The following items should be read and understood before working with the Maintenance Error Log:

- The Maintenance Error Log 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 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 Avaya CMS Forecast, the results of the Forecast Manager are written to the Maintenance Error Log.

## Running a Maintenance Error Log

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   Supervisor displays the Maintenance window.

2. Select the **Reports** tab.
3. Select **Error Log Report** in the **Reports** list.
4. Select **OK**.

   Supervisor displays the Maintenance Error Log window.

5. In the **ACD** drop down list, enter the ACD on which you want to see an error log or select **All** to include all ACDs. Selecting an ACD Group shows the error logs for only the member ACDs of that group.
6. If the **Error codes** field is blank, all error codes are displayed in the error log report. If you only want the report to include specific error codes, enter the necessary codes in the **Error codes** field.
7. In the **Severities** drop down list, enter the severity of errors you want to see the report or select **All Severities** to include errors of any severity.

See Severity of errors on page 345 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**.
10. Select **OK**.

    Supervisor displays the Maintenance Error Log report.

    See Maintenance Error Log messages on page 345 for additional definitions for the possible 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. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 505 | The following two errors are found together:<br>`UNIX error on WRITE, file: SIGPIPE signal caught during printing, print request is incomplete or failed`<br>`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.<br>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.<br>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 Additions** 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.<br>Call Services. |
| 557 | `UNIX call error: UNIX process limit exceeded. System is too busy` | This error could occur for multiple reasons.<br>Call services for assistance. |
| 557 | `UNIX call error: uucp failed` | The uucp file transfer mechanism for the External Call Records feature has failed.<br>The system will automatically retry the transfer. If it fails repeatedly, call Services. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 1001 | UNIX error on NEW<br>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.<br>Delete unneeded exceptions or allocate more space in **Data Storage Allocation** > **System Setup**. |
| 1001 | UNIX error on NEW<br>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.<br>Delete unneeded exceptions or allocate more space in **Data Storage Allocation** > **System Setup**. |
| 1001 | UNIX error on NEW<br>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.<br>Delete unneeded exceptions or allocate more space in **Data Storage Allocation** > **System Setup**. |
| 1001 | UNIX error on NEW<br>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.<br>Delete unneeded exceptions or allocate more space in **Data Storage Allocation** > **System Setup**. |
| 1001 | UNIX error on NEW<br>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.<br>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 |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | corrected there. For CMS , this is usually a software problem which may need reporting.<br>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.<br>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.<br>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. |
| 1302 | PROCESS COMMUNICATIONS (PO) library error, function:<br>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.<br>Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered. |
| 1302 | PROCESS COMMUNICATIONS (PO) library error, function:<br>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.<br>Reduce the number of active exceptions or change thresholds so that fewer exceptions are triggered. |
| 1302 | PROCESS COMMUNICATIONS (PO) library error, function: | Exceptions are being generated faster than the switch interface process can handle |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | 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. | them. This is the result of having too many exceptions activated, or having thresholds set to produce too many exceptions.<br>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.<br>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. |
| 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.<br>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.<br>Call Services. |
| 1350 | GENERAL error internal to process: Failure in trunk group exception database table. Trunk | 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 |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | group exception data not being stored. Call Services. | partition holding the trunk group exception table becomes full. No more trunk group exceptions can be recorded until the problem is corrected.<br>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.<br>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.<br>Call Services. |
| 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.<br>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 Additions**, try rewriting the **Main Menu Additions** 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.<br>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.<br>Clean up unnecessary files from disk. |
| 1350 | GENERAL error internal to process: Failure in removing data from database table: ag_actv. | An internal error occurred that prevents data from being deleted from the ag_actv database table.<br>Call Services. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | Agent Trace data not being stored. Call Services. | |
| 1351 | GENERAL error in process interface: Invalid action request. | Something is corrupted with the window interface.<br>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.<br>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. |
| 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.<br>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.<br>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/ |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | 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.<br>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.<br>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. |
| 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.<br>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.<br>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. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | 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.<br>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. |
| 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.<br>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.<br>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.<br>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 | Protocol error as explained in the message.<br>Ask the agent to log off and log in again with a single login ID. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | login ID. Ask the agent to log off and log in again with a single login ID. | |
| 1404 | One of the following messages will be displayed depending on the switch configuration:<br>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.<br>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.<br>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:<br>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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>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:<br>`SPI ACD administration error: switch unable to move ext <ext> from split <num> to <num>`<br>`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.<br>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.<br>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.<br>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.<br>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.<br>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.<br>Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur. |
| 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. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | 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.<br>Verify the following:<br>• The backup device is administered properly (name corresponds with the operating system administered device)<br>• The tape compatibility is correct (320 meg tape for 320 meg drive, etc.).<br>• 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.<br>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 `br_check`). |
| 1705 | `BACKUP Volume verification failed. Retry Backup.` | A problem reading the tape exists.<br>Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur. |
| 1706 | `BACKUP Table backup failed. Retry Backup. Table=` | A problem was encountered either reading the indicated table or writing that table to tape.<br>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.<br>Re-execute the backup process. Verify that the problem does not re-occur. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 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.<br>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.<br>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.<br>Respond to the backup acknowledgement window. |
| 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.<br>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.<br>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.<br>No action required |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 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.<br>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.<br>Exit the current instance of the backup screen and re-initiate the backup. Verify that the problem does not re-occur. |
| 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.<br>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.<br>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. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | 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).<br>Verify the following:<br>• The backup/restore device is administered properly (name corresponds with the operating system administered device).<br>• The tape compatibility is correct (320 meg tape for 320 meg drive, etc.).<br>• The tape drive is clean. |
| 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.<br>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.<br>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.<br>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 |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | is necessary to determine the source of the problem.<br>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.<br>Exit the current instance of the restore screen and re-initiate the restore. Verify that the problem does not re-occur. |
| 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.<br>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.<br>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.<br>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.<br>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.<br>Use **Data Storage Allocation** to adjust the amount<br>of space available to the ACD. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 1901 | `FULL DISK ERROR:` | There is no more disk space to load the data for this pseudo-ACD. The `load ACD` process cannot continue.<br>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. |
| 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.<br>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.<br>No immediate action is necessary. |
| 1901 | `FULL DISK ERROR: Storage Interval Migration failed migrating` | The disk or ACD dbspace is out of space.<br>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.<br>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.<br>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.<br>Call Services. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 1902 | `CALL RECORD ERROR: Call Records not being stored. Call Services.` | An error was encountered in writing call records to a disk file.<br><br>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.<br><br>No action necessary. |
| 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.<br><br>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.<br><br>Call Services. |
| 2000 | `Could not run timetable: - Aborting Timetable. <timetable name>` | Something is wrong with the timetable which is not allowing properly functionality.<br><br>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.<br><br>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.<br><br>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. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 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.<br>Try rescheduling the timetable. |
| 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.<br>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.<br>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.<br>This problem can usually be repaired by stopping CMS and restarting it.<br>Call Services. |
| 2200 | `Sometimes the problem can be repaired by stopping CMS and restarting it. <table>` | An error was encountered during migration.<br>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.<br>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.<br>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.<br>Contact services. |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| 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.<br>Verify that the new days are correct. |
| 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.<br>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`.<br>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`.<br>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.<br>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.<br>Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not re-occur. |
| 2702 | `MIGRATE DATA Process startup failed. Contact Services` | Any number of startup activities could cause this problem. If the problem re-occurs, there |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | is an error in the environment of the migrate process and further investigation is necessary to determine the source of the problem.<br><br>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:<br><br>• Invalid migration device<br>• Tape drive needs cleaning<br>• Table header format problem (internal error).<br><br>Verify the following:<br><br>• The backup/restore device is administered properly (name corresponds with the operating system administered device)<br>• The tape compatibility is correct (320 meg tape for 320 meg drive, etc.).<br>• 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.<br><br>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.<br><br>Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not re-occur. |
| 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 |

*Table continues…*

| Error Code | Message | Reason/Action |
|---|---|---|
| | | 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.<br><br>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.<br><br>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.<br><br>Exit the current instance of the R3 Migrate Data screen and re-initiate the migration. Verify that the problem does not reoccur. |

# ACD Administration Log

The ACD Administration Log provides an audit trail for administrative changes made to an ACD by CMS users. The ACD Administration Log records real-time administrative changes made by a user through the CMS ASCII interface, Supervisor, or Visual Vectors. The log also records the administrative changes made by a user through a scheduled timetable or Supervisor script.

## Before using ACD Administration Log

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 Supervisor script.
- The historical database items of the CMS ACD Administration Log is not available for use with the Avaya CMS Supervisor Report Designer tool. The Supervisor **File** menu option for this report will not display the Designer option. It will, however, behave in the same manner as drill-down reports.

## Permissions for ACD Administration Log

To view the ACD Administration Log report, the user ID used to log in to this Supervisor session requires “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

### Procedure

1. From the Controller window, select **Tools** > **Maintenance**.

   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. Select **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 window field descriptions on page 368 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** - 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 window field descriptions

The following table provides descriptions for the fields on the ACD Administration Log window.

| Name | Description |
|---|---|
| **CMS User IDs** | The login(s) of the user(s) to display in the report. If changes were made to the ACD with the specified IDs, those user IDs and the associated changes will be 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 ACD(s) to include in the report. |
| **VDNs(n)** | The VDN(s) to include in the report. |
| **Vectors(n)** | The Vector(s) to include in the report. |
| **Agents(n)** | The login ID(s) to include in the report. |

# Administering Report Properties

You can use the Report Administration window to impose a system wide limit on report queries. The system wide limit on report queries is implemented using the following two properties:

- You may impose a specific time limit, in 1 second increments, on historical report queries. That is, if a report query takes more than X seconds to return data from the Informix database, it times out. The range of allowed values is 3 to 999 seconds, or you may allow all historical report queries to run for an unlimited amount of time.

  If the time limit for all historical reports is set to any value other than never (unlimited), a historical report whose query takes longer than the limit times out, and the user receives an error message.

- You may also limit the size of an agent group which is part of either a real time or historical query. The limit choices for agent group are groups of 99 members or less, or unlimited.

  If the agent group limit is set to 99 members or less, a real time or historical agent group report which uses an agent group of 100 members or more does not run. The user receives an error message.

The system defaults for both of these properties are the unlimited value, and it changes only if you modify these properties with this window. The changes to this window take effect upon the next running report, and are imposed on all users. This window is only available from the ASCII interface and cannot be used from Supervisor.

Report limits apply to standard reports, custom reports, designer reports, and reports run from 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 elog.

This window may be placed in a timetable. Therefore, if you wish to limit the properties of report queries only during certain times of the day, you can create two timetables. The first timetable should run at the beginning of your system's busiest time, and modifies the report properties to impose time limits. The second timetable should run at the beginning of your system's quiet time, and modifies the report properties back to unlimited.

## Before administering report properties

- Examine the query log to determine if you have any reports which are adversely affecting your system performance due to the time spent on their Informix database query.

  **Note:**

  The report should be historical or real time, and it should use agent groups.

- Decide if you want to limit your historical report queries and what that limit, in number of seconds, should be
- Decide if you want to limit the size of agent groups used in agent group reports

## Permissions for administering report properties

Depending on the procedure you want to perform, you need the following permissions:

- To view the Report Administration window, you need “read” permission for the Maintenance subsystem.
- To modify the Report Administration window, you need “write” permission for the Maintenance subsystem.

## Modifying the Report Properties

### About this task

The Report Administration window is only available from the ASCII interface of CMS.

### Procedure

1. From the Main Menu, choose **Maintenance** and press `Enter`.
2. Choose **Report Administration** and press `Enter`.
3. Enter `n` in the first field if you wish to limit Agent Group reports to groups of 99 members or less. If you wish to allow all sizes of Agent Groups in queries, enter `y`.
4. Enter the number of seconds (3 to 999) in the second field if you wish to limit historical report queries to a specific time length. If you do not want a time limit to be enforced by the system, enter never.
5. From the **Actions** menu, select **Modify**.

# Advanced Debugging window

Always call Avaya Support before you use this window. For more information, see http://support.avaya.com

# Chapter 13: Using the Operating System

## Using the operating system

Avaya CMS uses the operating system to communicate with terminals and printers, to log errors, and to perform operations. This section addresses how to perform several procedures using operating system commands.

## Before using the operating system

Be cautious when accessing the operating system and running operating system commands. Damage can result to your CMS system if you use the operating system commands incorrectly. Before you run any operating system command, be sure you know what effect it can have.

## Logging in to CMS

This section contains procedures for logging in to CMS through methods other than using Supervisor. Some administrators will need to do this in order to access capabilities not available through the Supervisor interface.

### Logging in to CMS from the remote console

#### About this task

This procedure describes how to log in to CMS from a remote console. Most users log in to CMS remotely.

**Important:**

Do not allow users to share the same login ID as this action will use up operating system processes.

#### Procedure

1. At the `Login:` prompt, enter your login ID.

   The `Password:` prompt is displayed.

2. Enter your password.

   A prompt for the terminal type is displayed.

3. Enter your terminal type.

   If you use a login other than “cms”, CMS will automatically open to the CMS **Main Menu**.

   If “cms” is used as the login, you will have to enter `cms` a second time at the `$` prompt before the **Main Menu** will be displayed

## Logging in to CMS from the server console

### About this task

This procedure describes how to log in to CMS from the CMS server console. Logging in to CMS at the server is occasionally necessary in order to perform certain functions, such as a CMSADM backup or other administration functions that require you to switch to single-user mode.

**Important:**

Users who use a `/usr/bin/cms` shell will not be able to log in to CMS through the Common Desktop Environment (CDE).

To remedy this problem, you can either use the `/usr/bin/ksh` shell or use a command line login. The command line login will not use the CDE.

### Procedure

1. If the server has just been rebooted or inactive for an extended period of time, the console may be password-protected. If this is the case, unlock the console by entering your authorized username (if necessary) and password in the appropriate login console fields.

   Solaris displays the CDE interface.

2. Right-click the cursor in an empty area within the desktop space.

   The **Workspace Menu** is displayed.

3. Depending on how CMS was installed, choose one of the following alternatives:

   - If the `CMS XTERM` option is displayed in the **Workspace Menu**, you can open an xterm window directly by selecting that option.
   - If the `CMS XTERM` option is not displayed, choose **Tools** > **Terminal** from the **Workspace Menu** to open a terminal window. At the command prompt, enter `xterm` to open an xterm window.

   An xterm window is displayed with a `#` prompt.

# 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 system can replace a forgotten password.

## Before administering passwords

The following items should be read and understood before attempting to administer passwords:

- Password administration should only be done by an administrator with the password for the root user.
- Forcing a password change and administering the Password Aging feature can only be done through the CMS ASCII interface. The ASCII interface is available through the following methods:
  - A Terminal Emulator connection to the CMS server
  - A telnet session to the CMS server
  - Direct interaction with the CMS server
- Users should choose a password with no less than six characters. The password must have at least one character as a number or special character and have 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.

See Chapter 10: Administering user permissions on page 216 for more information on special characters.

## Changing a user's password

### About this task

When a user's password expires or it is forcibly made to expire by an administrator, the user is presented with a prompt or window during the CMS login process that allows the entry of a new password. The following procedure allows an administrator to cause a user's password to expire so that the user must enter a new password upon their next login attempt.

If a user forgets their password, perform the following procedure.

### Procedure

1. From the CMS **Main Menu**, highlight the **Commands** Screen-Labeled Key (SLK).

   CMS displays the **Commands** menu.

2. Select **UNIX (r) system**.

   The screen clears and a `$` prompt is displayed.

3. Enter the `su` command.

4. At the `Password:` prompt, enter the root password.

   The `#` prompt is displayed.

5. Enter the following command:

`passwd <userid>`

Where *userid* is the ID of the user who needs a new password.

The operating system displays a prompt for the new password.

6. Enter a new password for the user.
7. Re-enter the password when prompted for the confirmation password.

   The operating system displays the `command line` prompt.

   - If the operating system is Solaris, continue with Step 8 on page 375.
   - If the operating system is Linux®, continue with Step 10 on page 375.
8. Enter the following command:

   **passwd** `-f` *userid*

   Where *userid* is the ID of the user with a new password.

   The operating system displays the `command line` prompt.

   The `passwd -f` command will force the user to change their password the next time they log in to CMS .
9. Continue with step 11 on page 375.
10. Enter the following command:

    `chage -d 0 <userid>`

    where <*userid*> is the ID of the user with a new password.

    The operating system displays the command line prompt.

    The `chage -d 0` command forces the user to change their password the next time they log in to CMS.
11. Enter `exit` and press the `Enter`.

    The system displays the `$` prompt.
12. Enter `exit` and press the `Enter`.

    CMS displays the **Main Menu**.

# Administering password aging

## About this task

This section provides introductory and prerequisite information regarding the password aging feature of CMS .

Password aging is a feature that forces CMS users to change their password after a specified number of weeks have passed. Once this feature is activated, all users are required to change their passwords when the expiration period is reached.

### Before you begin

**Important:**

If you have a custom configuration from the Avaya Professional Services Organization (PSO) or use third-party applications on your CMS server, you must contact the PSO before enabling the password aging feature so that customizations are not affected. The PSO can be contacted through the technical support telephone number.

The following items should be read and understood before attempting to change the password aging feature:

- The number of weeks that pass before a password change is required can range from 1 to 52 weeks. The default value for this feature is 9 weeks.
- The password aging feature is only available through the `cmsadm` menu in the ASCII interface of CMS . This feature is not accessible through Avaya CMS Supervisor .

### Procedure

For more information and procedures for administering the password aging feature, see the appropriate *Avaya Call Management System Software Installation, Maintenance, and Troubleshooting Guide*.

# Chapter 14: Using Timetables And Shortcuts

## Using timetables and shortcuts

This section provides information on timetables and shortcuts and how to create and administer them. Timetables and shortcuts are used to run multiple administrative tasks and are only available through the CMS ASCII interface.

Access to the CMS ASCII interface can be done through the following methods:

- Terminal Emulator
- Telnet session to the CMS
- Direct interaction with the CMS server 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

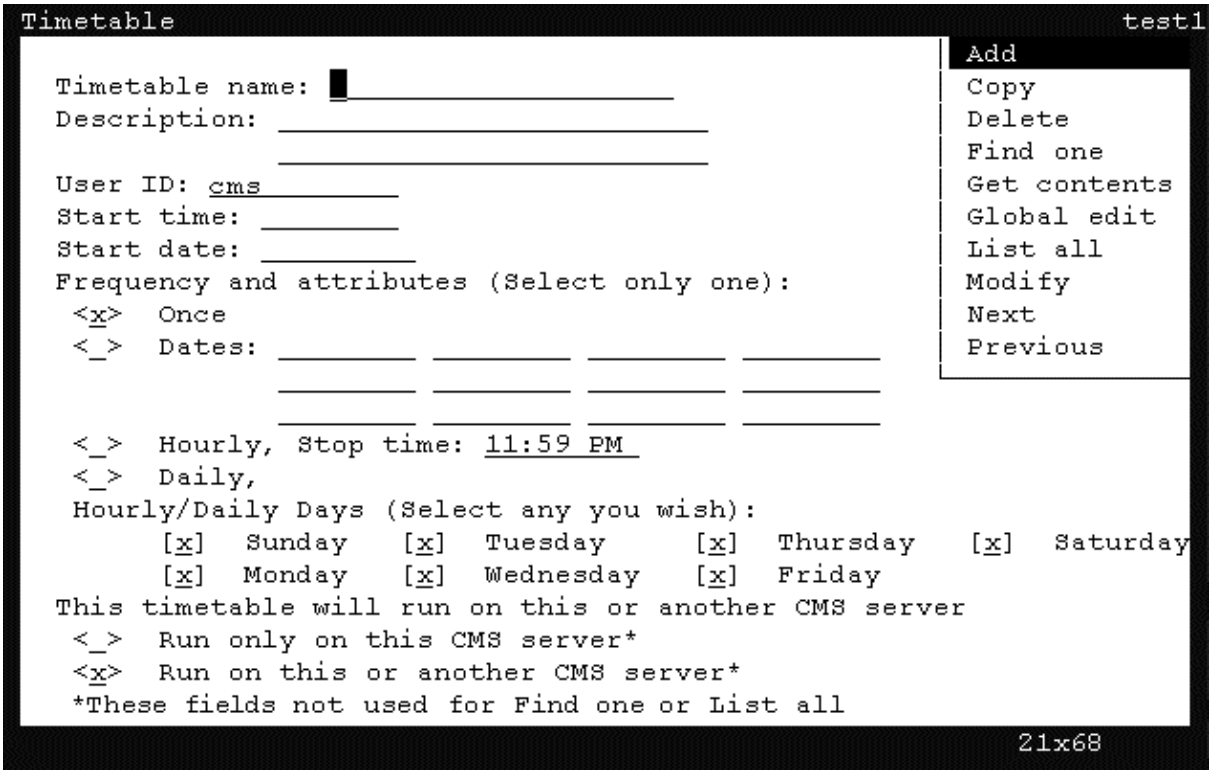
### About this task

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.




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 381.

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 381. 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

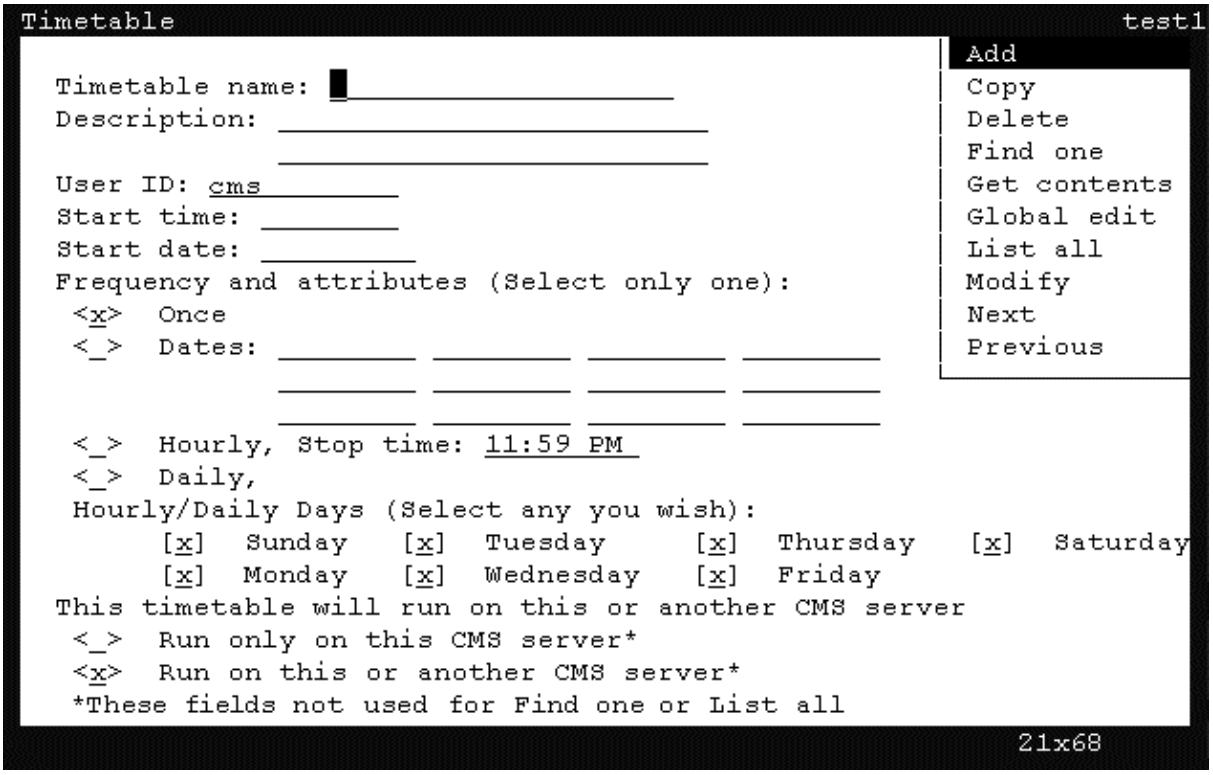
### About this task

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**, select the **Keep** Screen-Labeled Key (SLK).
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.

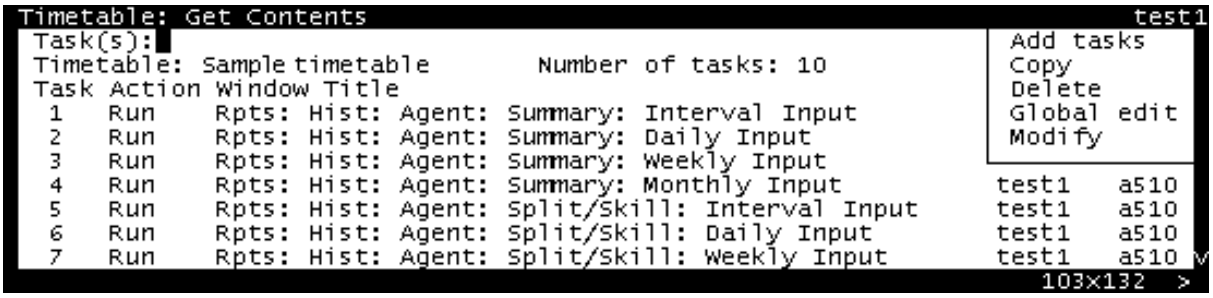
4. In the **Timetable name** field, enter the name of the timetable to which you want to add a task.

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.




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 379 in Creating and scheduling a timetable on page 379.

    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**, select the **Keep** Screen-Labeled Key (SLK).
2. On the **Keep** SLK menu, select **Keep Timetable**.

   CMS displays the Timetable window.

3. Press `Ctrl+Z`.

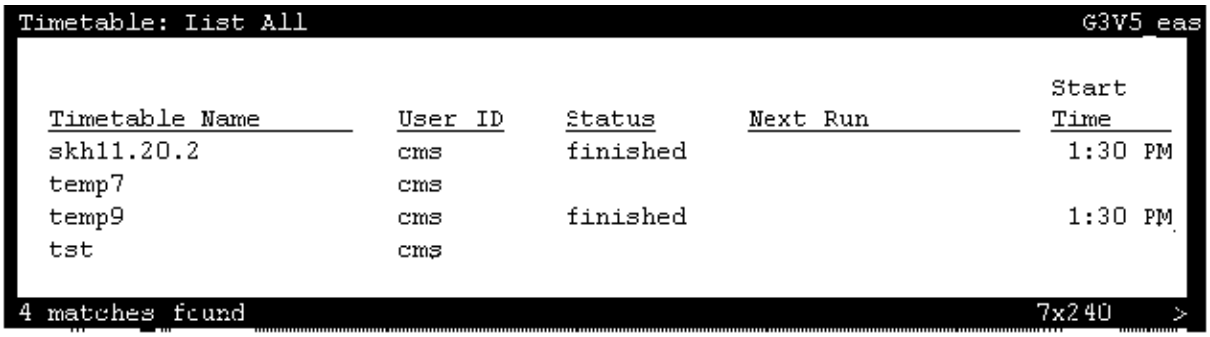
   CMS clears the default information from all fields in the Timetable window.

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.




   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

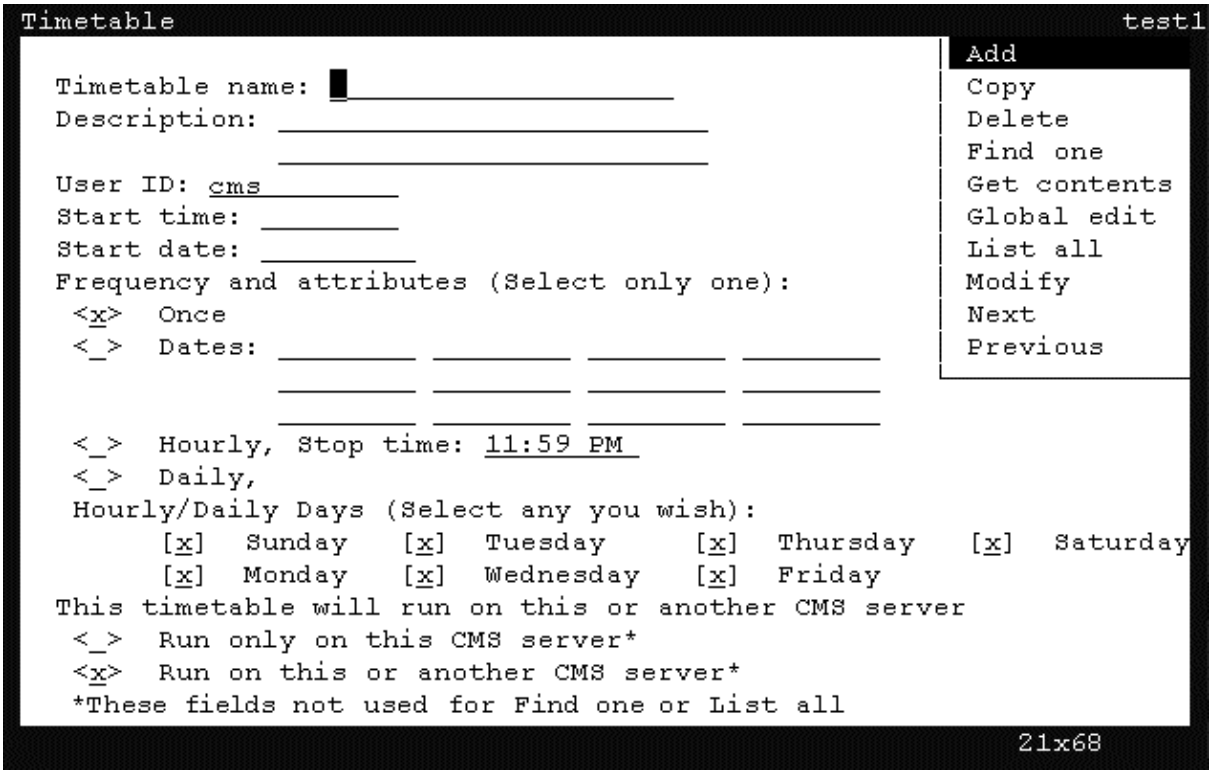
### About this task

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

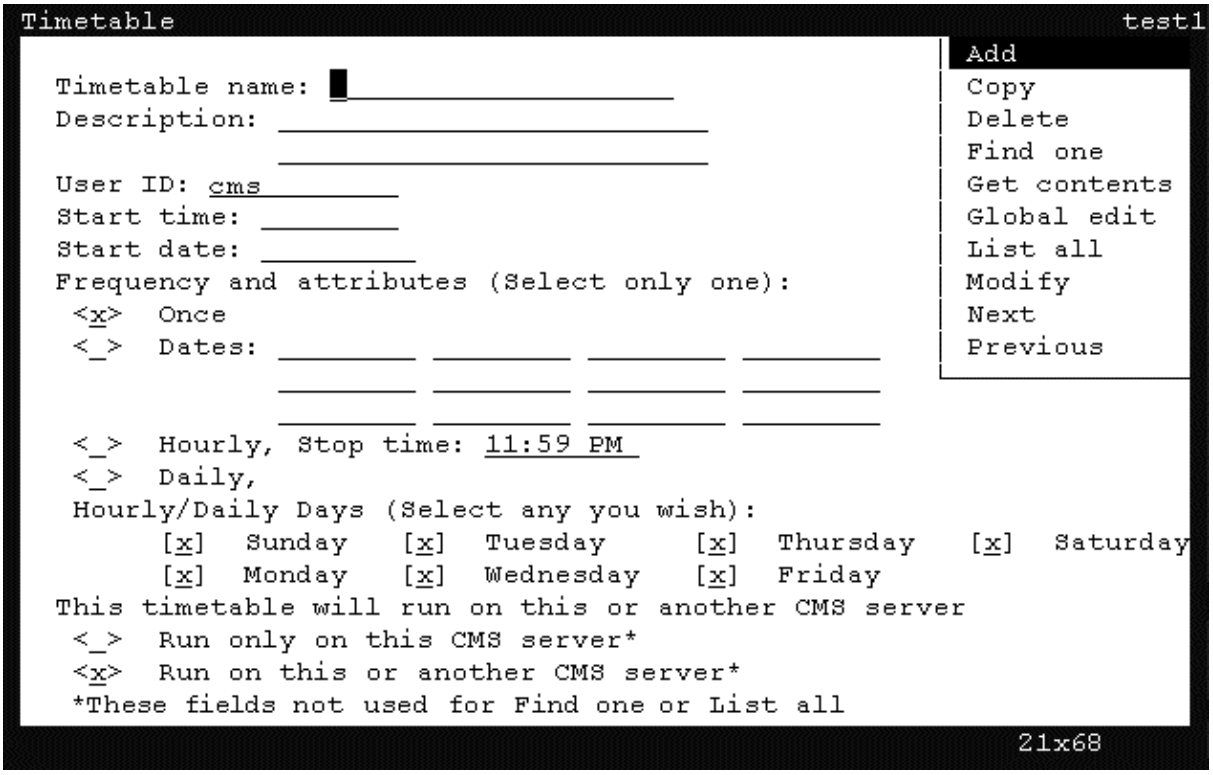
The following items should be read and understood before copying timetable tasks:

- 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**, select the **Keep** Screen-Labeled Key (SLK).
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 copy.
5. In the **User ID** field, enter the user ID that created the timetable.

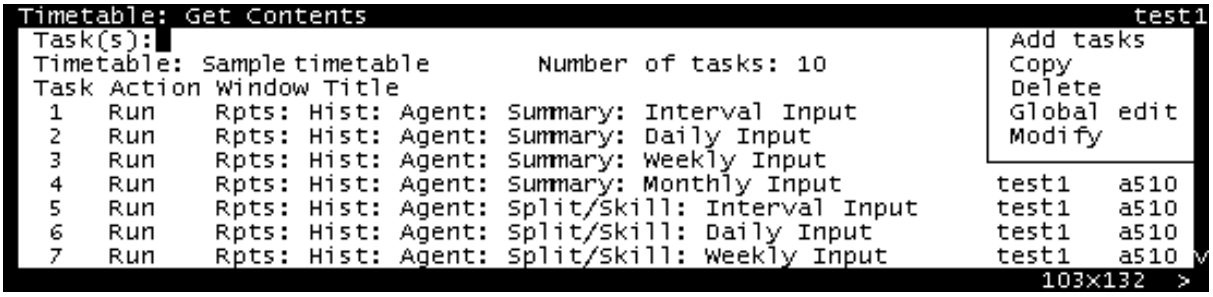
   If you are not the owner or an administrator, you will not be able to copy tasks in the timetable.

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.

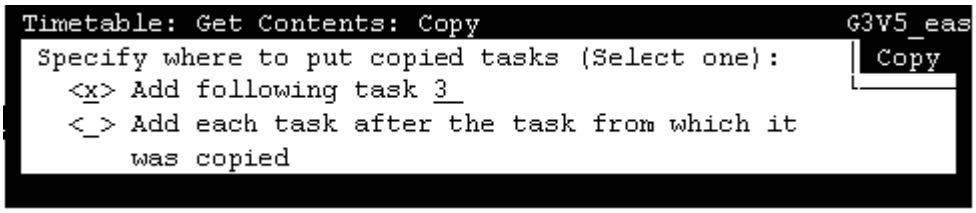



8. In the **Task(s)** field, enter the task number to copy and press the `Enter` key.

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

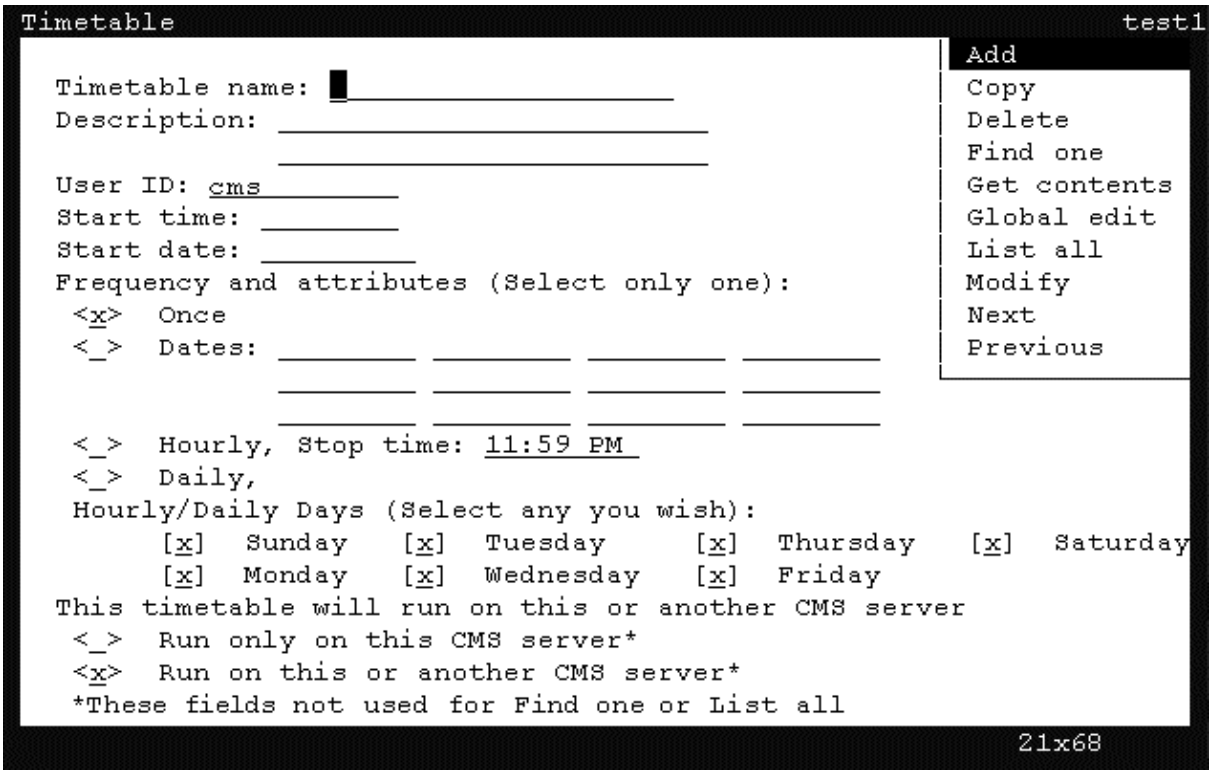
The following items should be read and understood before modifying timetable tasks:

- 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**, select the **Keep** Screen-Labeled Key (SLK).
2. Select **Timetable** and press the `Enter` key.

   CMS displays the Timetable window.



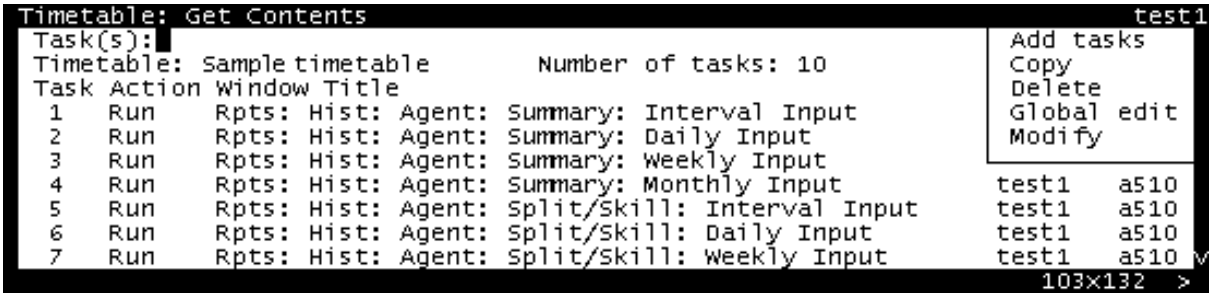

3. Press `Ctrl+Z`.

   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.



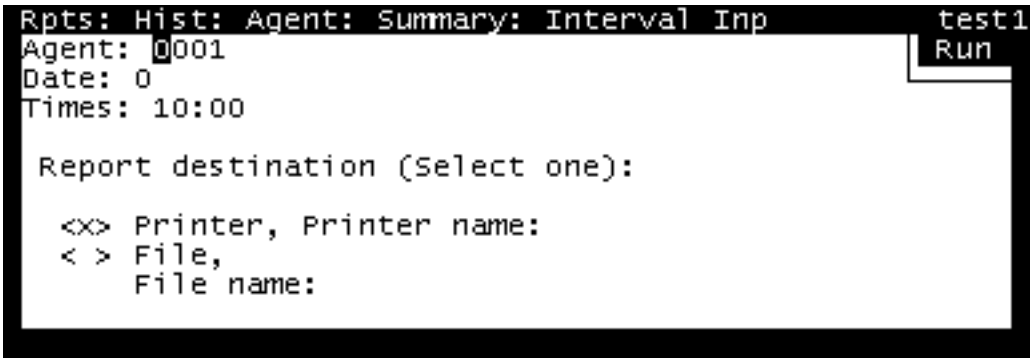

8. In the **Task(s)** field, enter the number of the task to modify and press the `Enter` key.

   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:




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

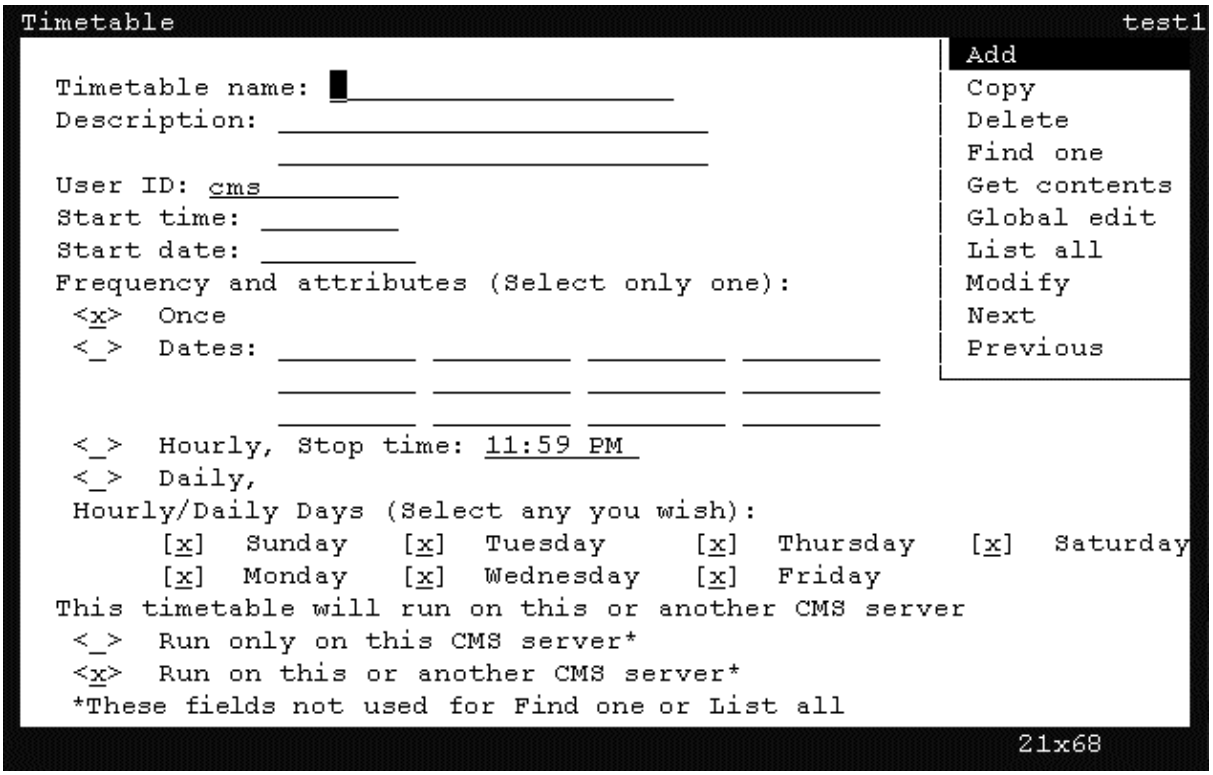
The following items should be read and understood before making global edits to timetable tasks:

- 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**, select the **Keep** Screen-Labeled Key (SLK).
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.

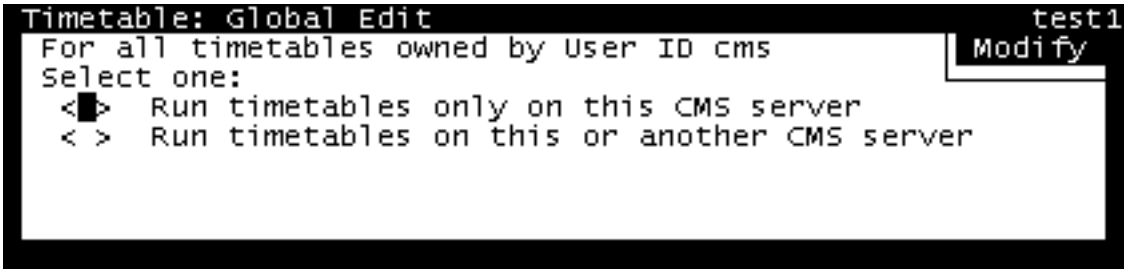
4. In the **Timetable name** field, enter the name of the timetable containing the tasks to modify globally.
5. Press the `Enter` key.

   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 **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

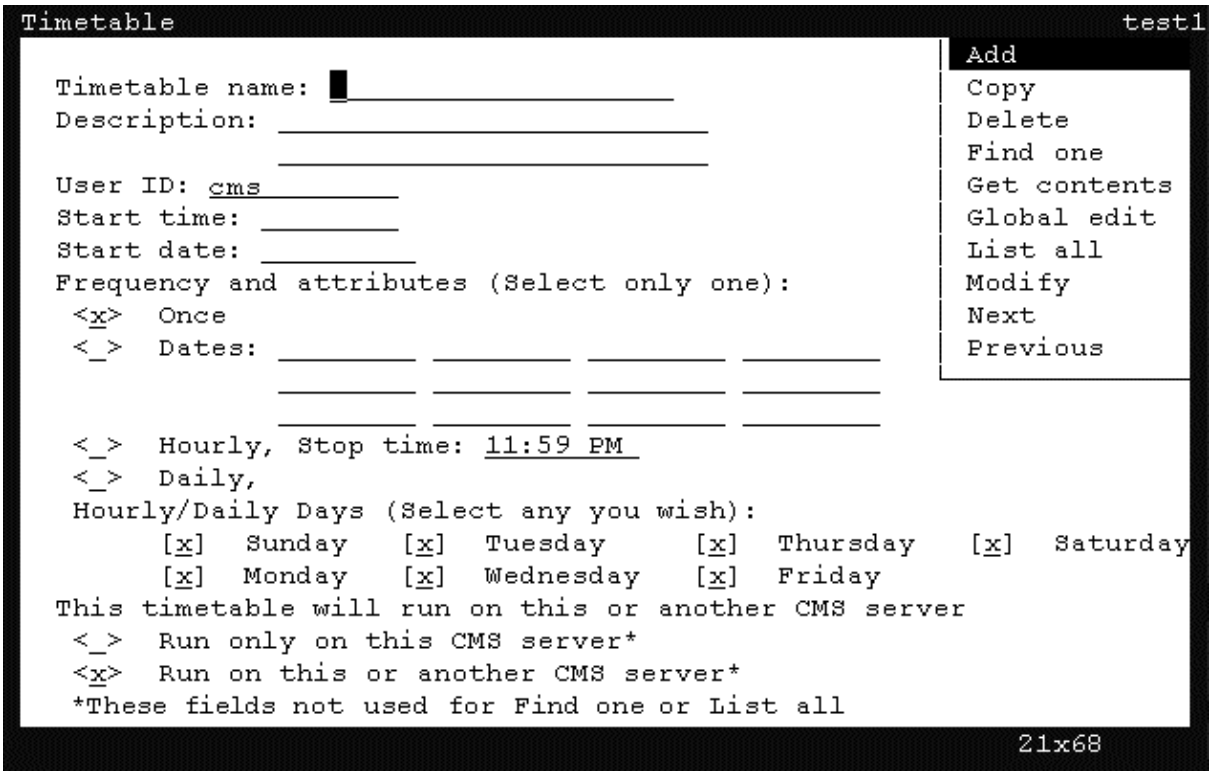
The following items should be read and understood before making global edits to timetable tasks:

- 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**, select the **Keep** Screen-Labeled Key (SLK).
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.

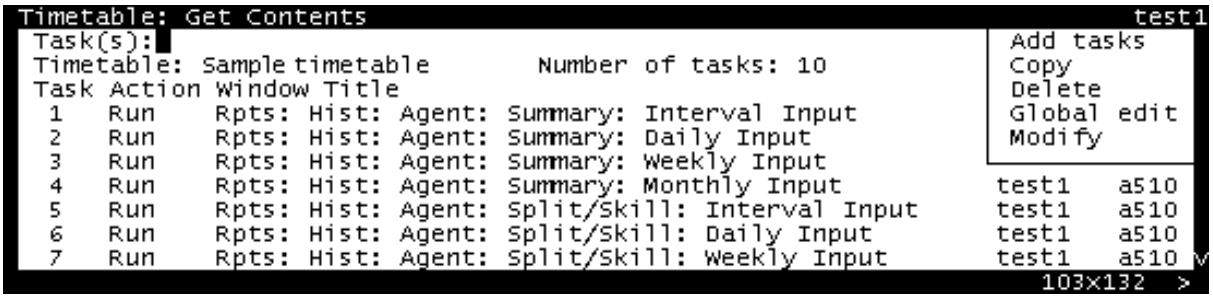
4. In the **Timetable name** field, enter the name of the timetable containing the tasks to modify globally.
5. Press the `Enter` key.

   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.




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.

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 contact 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.

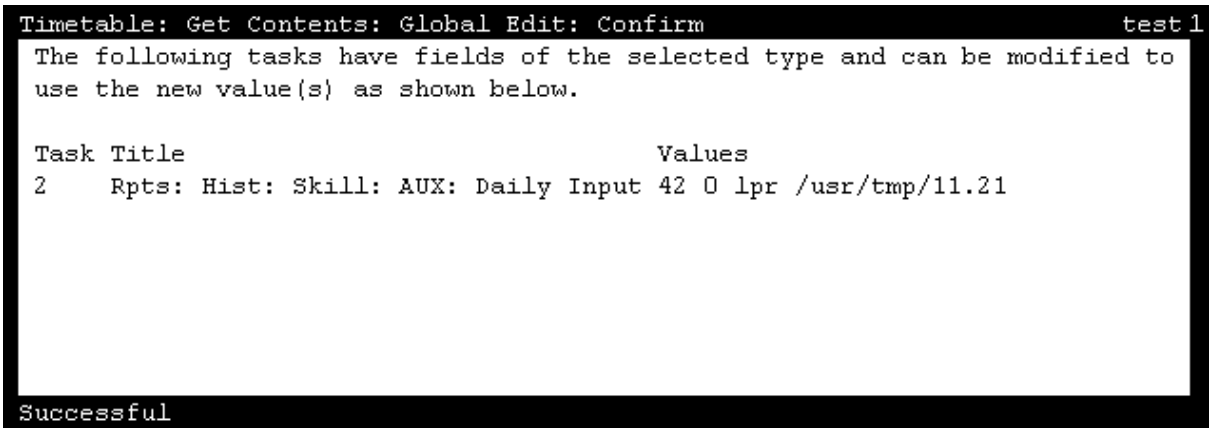
For the **Date/Dates** option, enter dates in either MM/DD/YY format or the relative format based on today (`0` for today, `-1` for yesterday). You can separate individual data entry items with semicolons (;) and value ranges with hyphens (-) between entries.

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.




    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

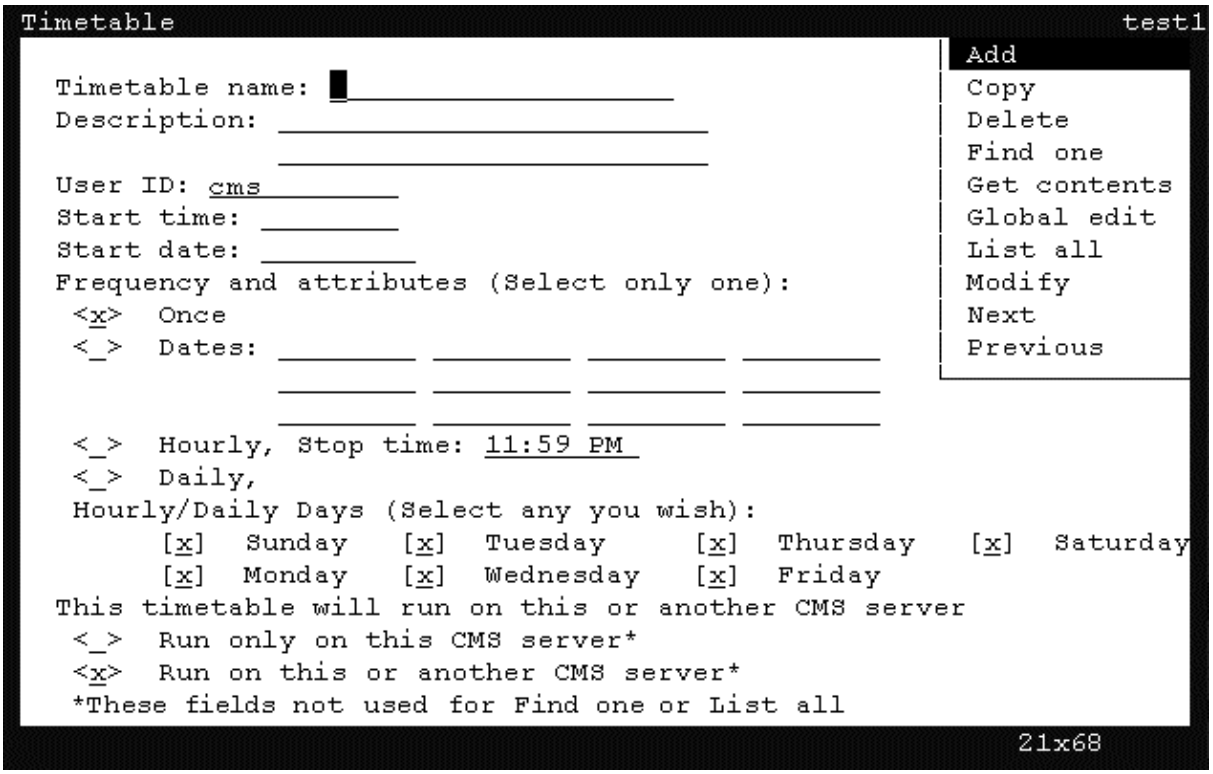
The following items should be read and understood before deleting tasks from a timetable:

- 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**, select the **Keep** Screen-Labeled Key (SLK).
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.

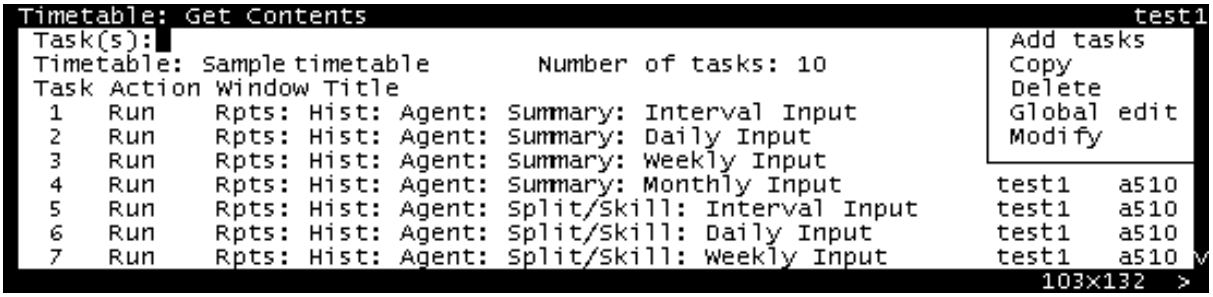
CMS locates the timetable and populates the remaining fields with the information from the timetable.

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.




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

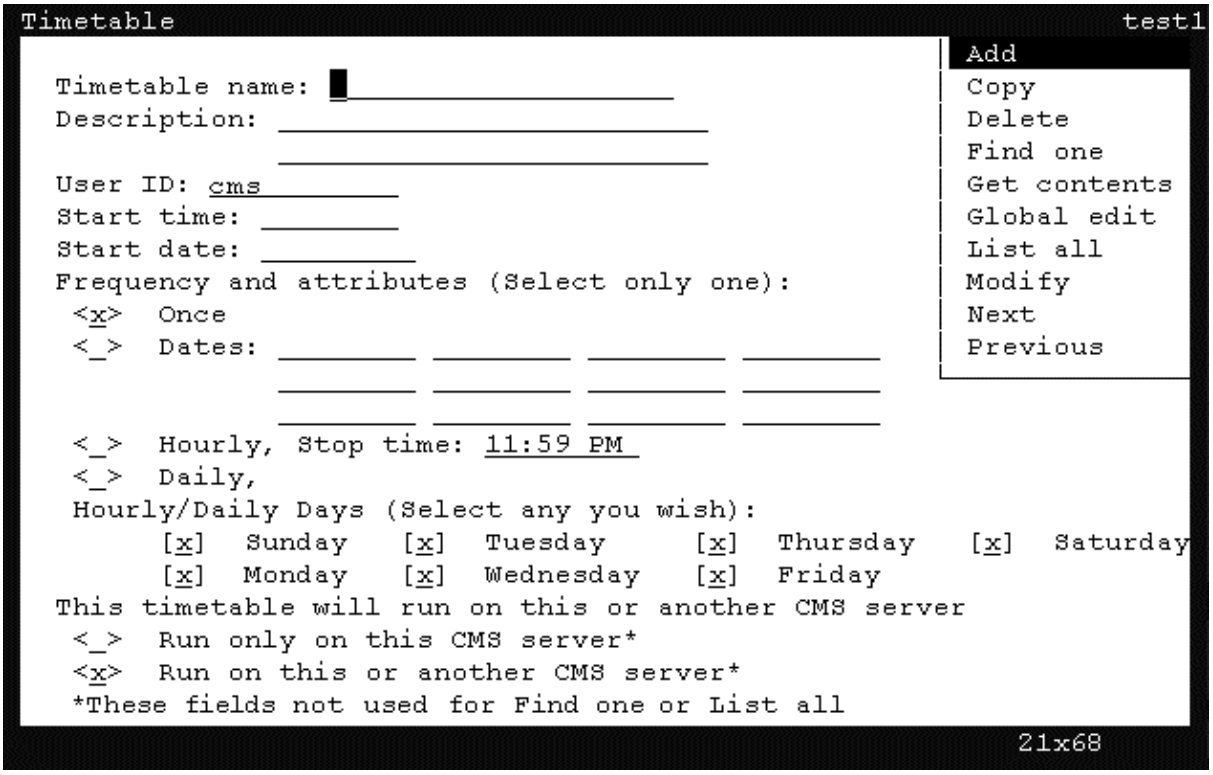
### About this task

Only the owner of the timetable or an administrator can delete timetables.

### Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
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 **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

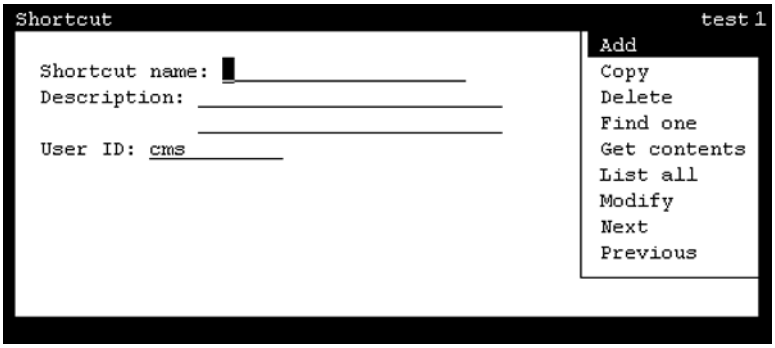
## About this task

This topic provides the procedure for creating a shortcut and adding tasks for it to perform.

## Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
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

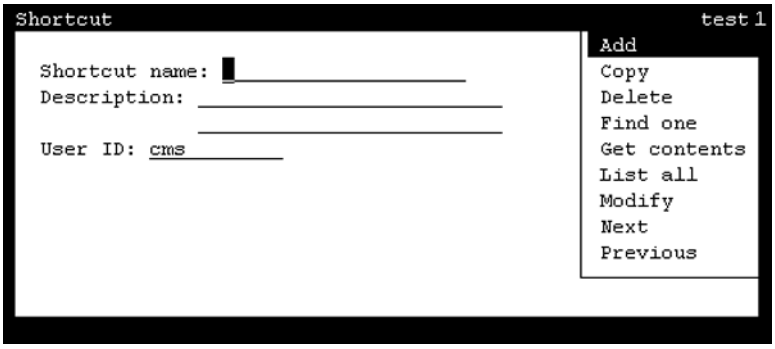
### About this task

This topic provides the procedure for adding tasks to an existing shortcut.

### Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
2. Select **Shortcut** and press the `Enter` key.

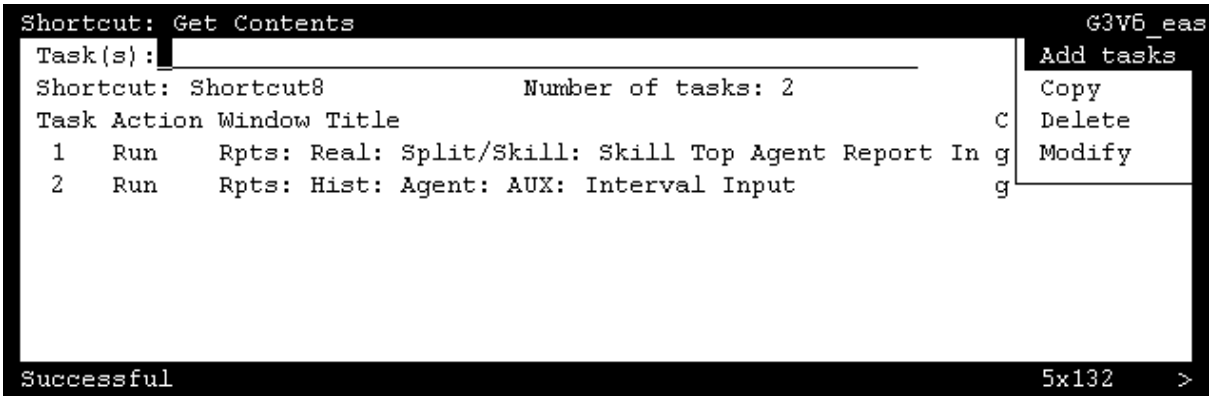
   CMS displays the Shortcut window.




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.




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

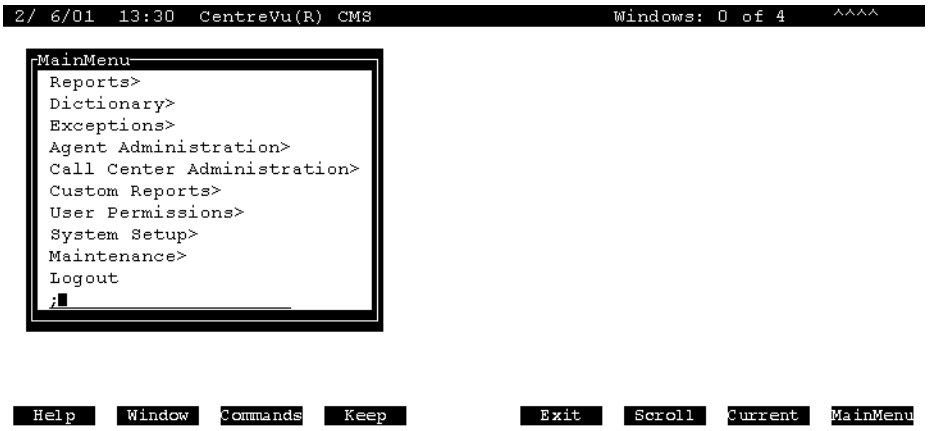
### About this task

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

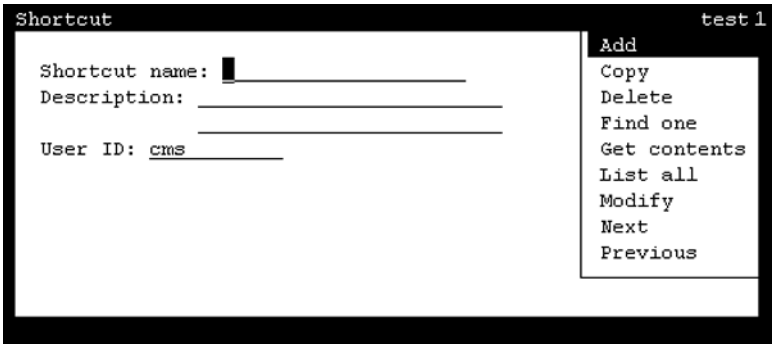
## About this task

This topic provides the procedure for editing the name or description of a shortcut.

## Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
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 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

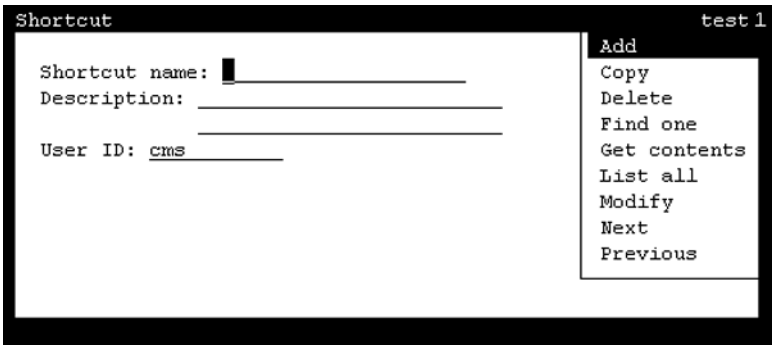
## About this task

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**, select the **Keep** Screen-Labeled Key (SLK).
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

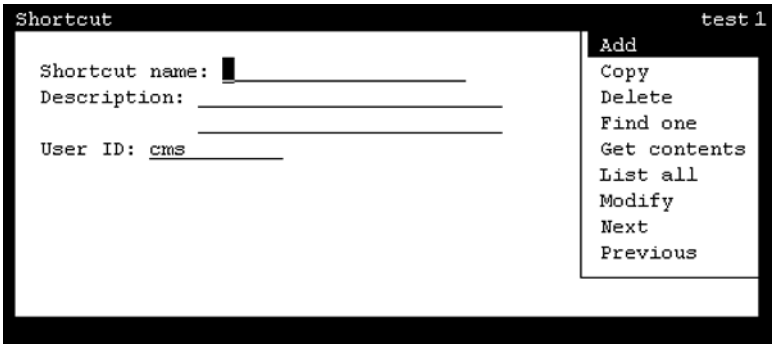
## About this task

This topic provides the procedure for copying tasks within a shortcut.

## Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
2. Select **Shortcut** and press the `Enter` key.

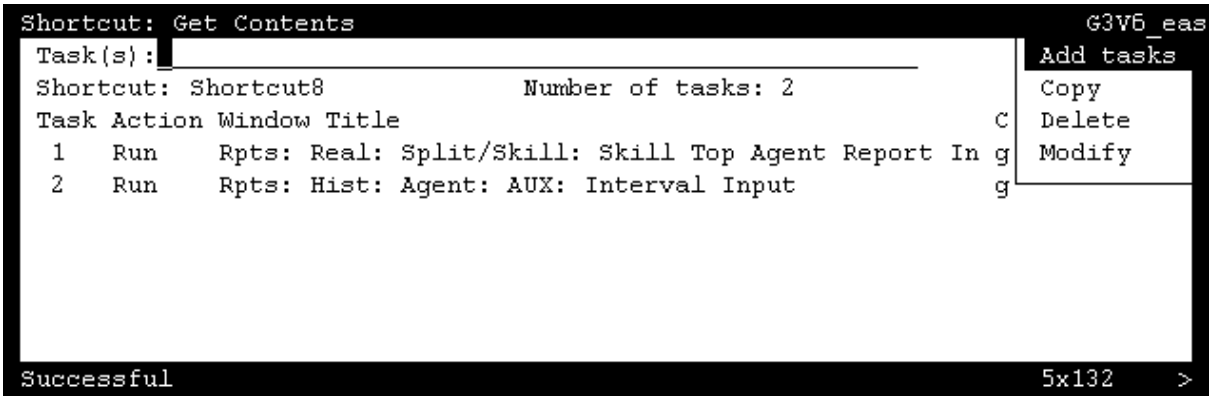
   CMS displays the Shortcut window.




3. In the **Shortcut name** field, enter the name of the shortcut 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.

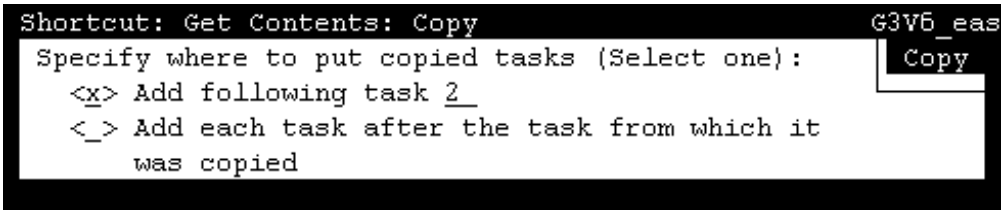
   CMS displays the Shortcut: Get Contents window.




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

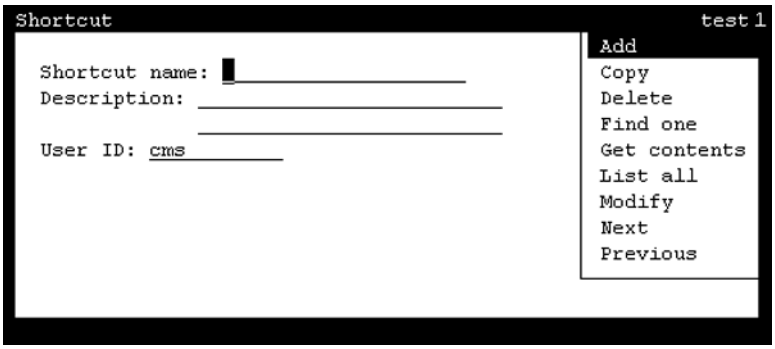
### About this task

This topic provides the procedure for editing tasks within a shortcut.

### Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
2. Select **Shortcut** and press the `Enter` key.

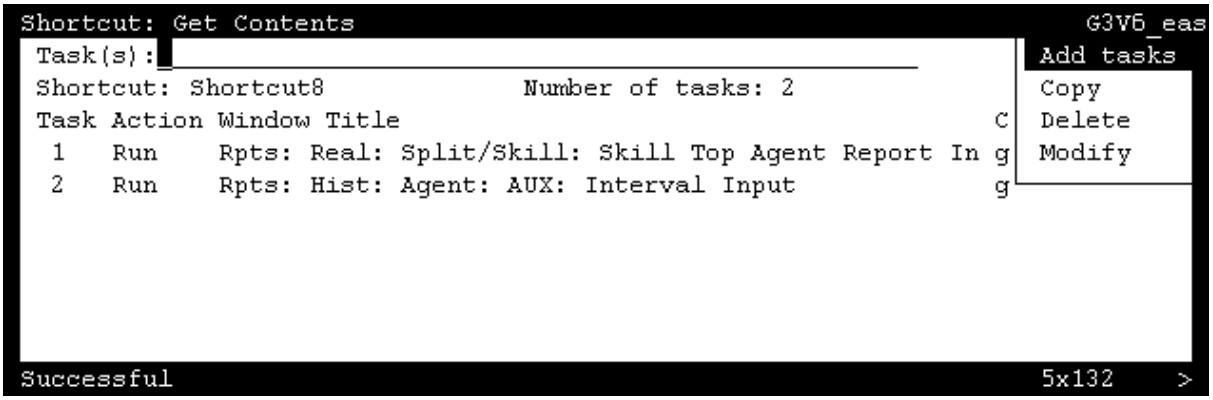
   CMS displays the Shortcut window.



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.




6. 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.
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

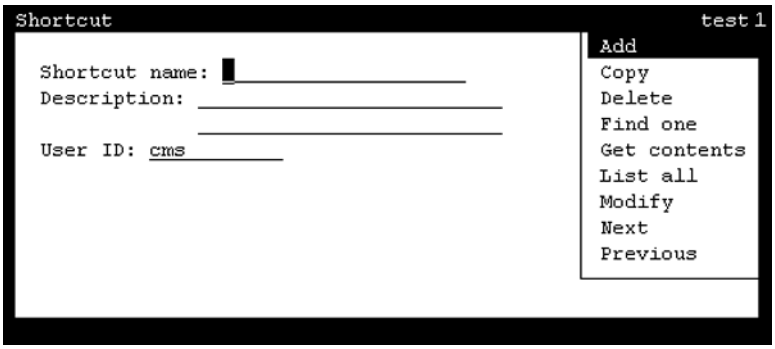
### About this task

This topic provides the procedure for deleting a task from a shortcut.

## Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
2. Select **Shortcut** and press the `Enter` key.

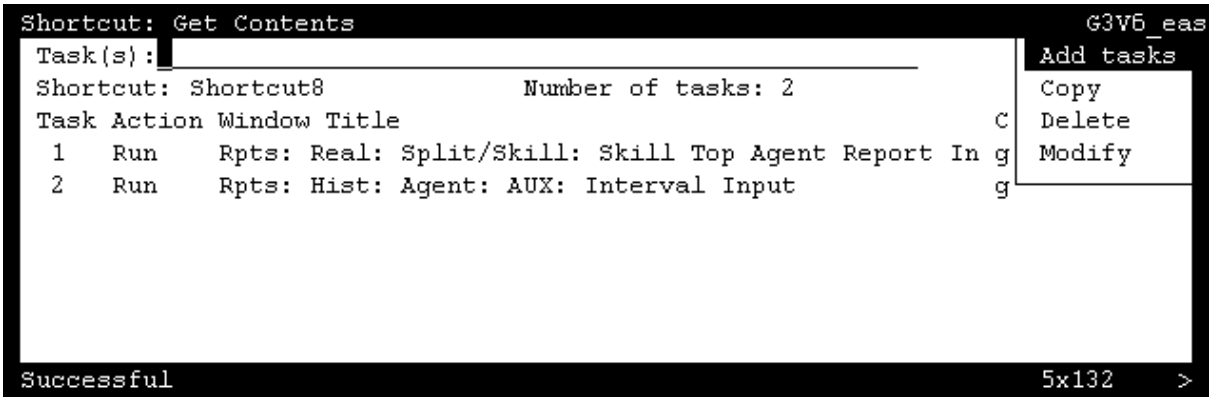
   CMS displays the Shortcut window.




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

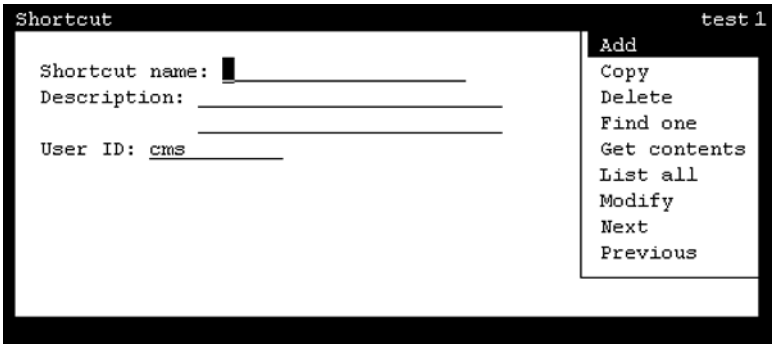
### About this task

This topic provides the procedure for deleting a shortcut from the CMS server.

### Procedure

1. From the CMS **Main Menu**, select the **Keep** Screen-Labeled Key (SLK).
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.

# Appendix A: Updating time zones

## Updating time zones displayed to users

### About this task

In CMS R18, a time zone list stored on the CMS server is used by the R18 Supervisor and the R18 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 your R18 Supervisor is connecting to an R17 CMS server, follow the instructions in the *Avaya CMS Supervisor Clients Installation and Getting Started*, Appendix B, for setting time zones for interval reports.

### 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 423, write permission on page 426.

**ACD** — See Automatic Call Distribution (ACD) on page 415

**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.

**ACW** — See after call work (ACW) on page 413

**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.<br><br>See also primary skill on page 422 , secondary skill on page 424 , and skill level on page 424 |
| **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 contact 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 415. |
| **ANI** | See Automatic Number Identification (ANI) on page 415. |
| **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 416.

**ASAI** See Adjunct/Switch Applications Interface (ASAI) on page 413.

**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 or 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 415.

**AUX reason codes** Codes that enable a contact 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 415.

**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 contact center entities in the Dictionary. Calculations generate the date for fields in a report. |
| **Call Management System (CMS)** | A software product used to connect to a switch that monitors and records data for large volumes of telephone calls that are processed through the ACD feature of the switch. |
| **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. |
| **CMSADM backup** | A backup that saves all the file systems on the CMS server including the Solaris operating system, CMS programs, and CMS administration data. |

**CONN** See connected (CONN) on page 417.

**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 415.

**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.

**CWC** See Call Work Code (CWC) on page 416.

**DABN** See dequeued and abandoned (DABN) on page 418.

**DACD** See direct agent ACD (DACD) on page 418.

**DACW** See direct agent ACW (DACW) on page 418.

**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 418. |
| **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 contact center entities such as login IDs, splits/skills, trunk groups, VDNs, and vectors. |
| **DID** | See direct inward dialing (DID) on page 418. |
| **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 contact 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 418. |
| **EAS** | See Expert Agent Selection (EAS) on page 419. |
| **entity** | A generic term for an agent, split/skill, trunk, trunk group, VDN, or vector. |
| **EWT** | See expected wait time (EWT) on page 419. |
| **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, contact 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. |
| **FBUSY** | See forced busy (FBUSY) on page 419. |
| **FDISC** | See forced disconnect (FDISC) on page 419. |
| **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. |
| **Forecast, Avaya CMS** | An Avaya product used to generate reports displaying expected call traffic and agent/trunk group requirements for the contact center for a particular day or period in the future. |

**historical database** A CMS database consisting of intrahour records for up to 62 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.

**HOLD** A trunk state in which an agent has put a call on this trunk on hold.

**IDLE** A trunk state in which this trunk is not in use and is waiting for a call.

**II** See Information Indicator (II) on page 420.

**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.

**INFORMIX SQL** An interactive interface typically used to view the INFORMIX database.

**Integrated Services Digital Network (ISDN)** A digital standard for telephony that enables analog and digital signals on the same line.

**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 416 and rolling ASA on page 423.

**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.

**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.

**ISDN** See Integrated Services Digital Network (ISDN) on page 420.

**LAN** See local area network (LAN) on page 420.

**local area network (LAN)** A private interactive communication network that allows computers and compatible devices to communicate over short distances, usually less than one mile, at high data transfer rates.

**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.

**LOGOFF** An agent trace work mode in which an agent is logged out and not available to take ACD calls.

**LOGON** An agent trace work mode in which an agent is logged in and available to take ACD calls.

**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 contact centers. LAI works with Call Vectoring and ISDN PRI trunks to intelligently route calls between contact centers. This allows multiple contact centers to share workloads, expand hours of coverage, and allows calls to be transparently handled by contact 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.

**MBUSY** See maintenance busy (MBUSY) on page 421.

**MCH** See Multiple Call Handling (MCH) on page 422.

**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 421.

**MIA** See Most Idle Agent (MIA) on page 421.

**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. |
| **OTHER** | An agent work mode in which the agent is on a direct agent call, on a call for another split or skill, or has put a call on hold and has not chosen another work mode. |
| **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.<br>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 414. |
| **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<br>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.

**UNKNOWN** 1) An agent state in which CMS does not recognize the state of the agent.

2) A trunk state in which CMS does not recognize the state of the trunk.

**UNSTAF** An agent state in which the agent is not logged in and, therefore, is not tracked by CMS.

**VDN** See Vector Directory Number (VDN) on page 425.

**VDN calls-counted** See active VDN calls on page 413.

**VDN or 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 contact 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 command** A step in a vector that describes the action to be executed for a call.

**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.

**VOA** See VDN or Origin Announcement (VOA) on page 425.

**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


about backing up data for a pseudo-ACD ..... 294
accessing script options ..... 117
accessing scripts ..... 116
ACD
  Administration Log ..... 367
  administrative interface ..... 21
  listing connection status ..... 338
  listing status ..... 309
  master, selecting ..... 272
  name, deleting ..... 47
  settings, listing all ..... 307
  settings, viewing ..... 306
  setup ..... 305
  translations, requesting ..... 311
  user permissions ..... 224
  user permissions, adding ..... 225
  user permissions, deleting ..... 228
  user permissions, listing all ..... 227
  user permissions, modifying ..... 227
  user permissions, viewing ..... 226
  viewing archiving status of all ..... 312
  viewing archiving status of one ..... 312
  viewing connection status ..... 338
  viewing status ..... 309
ACD administration ..... 27
ACD Administration Log report, running ..... 368
ACD Administration Log window field descriptions ..... 368
ACD-for-migration description ..... 289
ACD Group capabilities ..... 147
ACD groups
  before using ..... 44
  permissions ..... 44
ACD Groups ..... 43, 146
  Adding ..... 148
  Adding an ACD ..... 149
  Call Center Administration ..... 146
  deleting ..... 152
  deleting an ACD ..... 151
  Dictionary
    view contents ..... 45
  List all
    Dictionary ..... 44
  listing all
    Call Center Admin ..... 149
  modifying ..... 152
  renaming ..... 152
  view contents ..... 45
  viewing contents ..... 150
ACD Groups feature interfaces ..... 148
ACDs ..... 45
  permissions ..... 46
ACD status ..... 33, 308
actions not associated with reports ..... 121
adding
  CMS users ..... 218
  split/skill user permissions ..... 238
  trunk group user permissions ..... 244
  vector user permissions ..... 250
Adding ..... 91
adding a Full Maintenance Backup Timetable for an ACD 322
adding agents to an existing agent group ..... 50
adding an ACD name ..... 46
adding an agent group ..... 48
adding an AUX reason code name ..... 58
administering ..... 262
  tenancy at a high level ..... 30
  tenants ..... 262
  user permissions ..... 216
administering printers ..... 340
Advanced Debugging window ..... 371
agent
  changing skills ..... 130
  copying agent groups ..... 49
  exceptions ..... 180
  exceptions, adding ..... 181
  exceptions, definitions ..... 184
  exceptions, deleting ..... 183
  exceptions, modifying ..... 182
  exceptions, report ..... 206
  templates, changing skills for ..... 129
  trace, starting and stopping ..... 125
agent group
  deleting ..... 51
  listing agents ..... 49
agent group members
  running a report ..... 108
agent groups ..... 47
agents
  adding to an existing group ..... 50
  administrating ..... 125
  deleting from an existing group ..... 50
  multiple, adding to another skill ..... 136
  multiple, moving from skill to skill ..... 136
agent skills
  adding ..... 134
  deleting ..... 135
  for changing ..... 134
agent string value field descriptions ..... 52
agent string values ..... 51
  permissions ..... 51
agent trace
  stopping ..... 125
allocating
  disk space ..... 275

Already exists status message ..... 33
ANI/SID
see automatic number identification/station number identification ..... 208
announcement name
adding ..... 54
deleting ..... 56
listing all ..... 55
modifying ..... 56
viewing ..... 55
announcement names ..... 54
before using ..... 54
archiving data
Data Summarizing ..... 280
archiving status ..... 311
automatic number identification/station number identification ..... 208
AUX reason code names ..... 57
adding ..... 58
before using ..... 57
deleting ..... 60
listing all ..... 59
modifying ..... 59
viewing ..... 58

## B

backing up
pseudo-ACDs ..... 295
backup
adding a full maintenance backup timetable for an ACD ..... 322
before adding a full maintenance backup timetable for an ACD ..... 322
binary backup of database ..... 331
CMSADM ..... 324
CSMADM ..... 316
data ..... 316
duration of standard full Maintenance Backup to tape ..... 320
maintenance ..... 317, 327
performing a CMSADM backup ..... 325
performing a maintenance backup ..... 327
recovery kit ..... 331
USB/network backup restore devices ..... 317
backup/restore devices
adding ..... 314
deleting ..... 316
listing all ..... 314
modifying ..... 315
viewing ..... 314
backup and restore
alternative methods ..... 319
considerations ..... 318
factors ..... 318
reducing times ..... 319
Backup Data window ..... 328
backup error messages, common ..... 330
backup information
how to interpret ..... 330
backup volume
labeling ..... 330
before adding a Full Maintenance Backup Timetable for an ACD ..... 322
before adding split/skill user permissions ..... 238
before adding trunk group user permissions ..... 244
before adding VDN user permissions ..... 256
before adding vector user permissions ..... 250
before administering a printer ..... 340
before administering passwords ..... 374
before administering report properties ..... 370
before administering the contact center ..... 146
before backing up data for a pseudo-ACD ..... 294
before changing agent skills ..... 129
before changing extension split assignments ..... 141
before changing skills for multiple agents ..... 136
before changing switch time zone ..... 302
before changing the intrahour interval ..... 301
before configuring CMS system settings ..... 270
Before deleting CMS users ..... 223
before listing agents traced ..... 127
before listing all trunk group user permissions ..... 246
before listing all VDN user permissions ..... 258
before loading pseudo-ACD data ..... 297
before migrating CMS data ..... 286
before modifying data storage allocation ..... 276
before modifying data summarizing settings ..... 303
before modifying split/skill user permissions ..... 241
before modifying trunk group user permissions ..... 247
before modifying VDN user permissions ..... 259
before modifying vector user permissions ..... 253
before moving extensions between splits ..... 142
before performing a CMSADM backup ..... 325
before performing a maintenance backup ..... 327
before restoring data ..... 334
before using
ACD groups ..... 44
before using ACD Administration Log ..... 367
before using ACD groups ..... 146
before using ACD status ..... 308
before using agent exceptions ..... 180
before using Archiving Status ..... 311
before using calculations ..... 61
before using call work codes ..... 64
before using CMS State ..... 271
before using custom database items ..... 70
before using Data collection ..... 272
before using Data Storage Allocation ..... 274
before using exceptions ..... 178
before using External Application Status ..... 281
before using Free Space Allocation ..... 284
before using login ID names ..... 77
before using logout reason code names ..... 80
before using Main Menu Addition Access ..... 233

before using Maintenance Error Log ..... 344
before using pseudo-ACDs ..... 289
before using real-time exceptions log ..... 204
before using shortcuts ..... 400
before using split/skill access ..... 237
before using split/skill exceptions ..... 187
before using split/skill names ..... 86
before using split/skill string values ..... 83
before using Storage intervals ..... 300
before using Switch Setup ..... 306
before using the ACD access window ..... 224
before using the Feature Access window ..... 230
before using the Maintenance window ..... 308
before using the operating system ..... 372
before using the Trunk Group Access window ..... 243
before using the User Permissions subsystem ..... 216
before using trunk group assignments ..... 163
before using trunk group exceptions ..... 191
before using trunk group members report ..... 166
before using trunk group names ..... 93
before using VDN access ..... 255
before using VDN call profiles ..... 169
before using VDN exceptions ..... 195
before using VDN names ..... 99
before using VDN skill preferences ..... 157
before using VDN-to-vector assignments ..... 167
before using vector access ..... 249
before using vector configuration report ..... 173
before using vector exceptions ..... 200
before using vector names ..... 102
before viewing CMS users ..... 220
before viewing split/skill user permissions ..... 239
before viewing trunk group user permissions ..... 245
before viewing VDN user permissions ..... 257
before viewing vector user permissions ..... 251
Before you begin scripting CMS operations ..... 115
bfore using split/skill call profiles ..... 159
binary backup
  to a network device ..... 333
  to a USB storage device ..... 332
binary backup of database ..... 331

## C

calculations ..... 60
  adding ..... 62
  deleting ..... 63
  listing all ..... 62
  modifying ..... 63
  viewing ..... 61
call center
  configuration ..... 146
Call Center Administration
  ACD Groups ..... 146
Call Vectoring ..... 125
  capabilities of ..... 21
call work code 0 ..... 153
call work code names
  adding ..... 65
  deleting ..... 67
  listing all ..... 66
  modifying ..... 66
  viewing ..... 65
call work codes ..... 64, 153
  adding ..... 154
  configuring ..... 153
  deleting ..... 156
  listing all ..... 155
  unassigned ..... 153
  viewing ..... 155
Cancelled status message ..... 33
Change agent skills in CMS Supervisor Web ..... 133
changing agent string value descriptions ..... 51
changing skills for multiple agents ..... 137
changing switch time zone ..... 302
changing the intrahour interval ..... 301
Choosing a report ..... 112
chunks ..... 26
CMSADM backup ..... 316, 324
CMS state ..... 270
colors, reports ..... 36
colors threshold ..... 37
Communications Tab ..... 36, 38
configuring CMS system settings ..... 270
connection status ..... 338
considerations when backing up or restoring ..... 318
considerations when sizing and reporting on agent groups .48
constants ..... 67
  adding ..... 68
  deleting ..... 69
  listing all ..... 68
  modifying ..... 69
  viewing ..... 68
copying an existing agent group to a new name ..... 49
creating
  new report color scheme ..... 36
custom database items ..... 70
  adding ..... 70
  deleting ..... 72
  listing all ..... 71
  modifying ..... 72
  viewing ..... 71

## D

data
  historical, migrating ..... 286
  migrating ..... 286
  migrating, R3 ..... 286
  storage, allocating ..... 275
data backup ..... 316
Database constants ..... 67
database items
  custom ..... 70

database items *(continued)*
custom, adding ... 70
custom, deleting ... 72
custom, listing all ... 71
custom, modifying ... 72
custom, viewing ... 71
standard ... 89
data collection ... 272
disabling ... 273
enabling ... 273
report ... 207
state, changing ... 273
data restore ... 344
Data Storage Allocation ... 274, 275
Data Storage Allocation fields ... 276
Data summarization time zone ... 174
Data summarization time zone fields ... 174
data summarizing ... 22, 300
settings, modifying ... 303
Data summarizing ... 279
Data Summarizing ... 280
data to back up descriptions ... 329
date and time on status indicator ... 33
dbspace ... 26
dbspaces
contents, viewing ... 285
Default ACD ... 34
defining entity formats ... 39
deleting
CMS users ... 223
deleting a custom calculation ... 63
deleting agents in an existing agent group ... 50
deleting an agent group ... 51
deleting an announcement name or synonym ... 56
deleting an AUX reason code ... 60
description of the ACD Status window
with EAS ... 310
without EAS ... 310
description of the Archiving Status - List All window ... 313
Description of the Connection Status Window ... 339
devices
backup/restore ... 313
dictionary
before using ... 41
global search results ... 43
searching ... 42
Dictionary
ACD Groups ... 43
List all ... 44
view contents ... 45
ACD name, deleting ... 47
agent group members report, running ... 108
announcement name, adding ... 54
announcement name, viewing ... 55
calculations, adding ... 62
calculations, listing all ... 62
calculations, viewing ... 61
ACD Groups *(continued)*
call work code names, adding ... 65
call work code names, deleting ... 67
call work code names, listing all ... 66
call work code names, modifying ... 66
call work code names, viewing ... 65
call work codes ... 64
constant, deleting ... 69
constants ... 67
constants, adding ... 68
constants, listing all ... 68
constants, modifying ... 69
constants, viewing ... 68
custom database item, viewing ... 71
custom database items ... 70
custom database items, adding ... 70
custom database items, deleting ... 72
custom database items, listing all ... 71
custom database items, modifying ... 72
location ID, adding ... 74
location ID, deleting ... 76
location ID, listing all ... 75
location ID, modifying ... 75
location ID, viewing ... 74
location IDs ... 74
login ID name, adding ... 77
login ID name, deleting ... 79
login ID name, listing all ... 78
login ID name, modifying ... 79
login ID name, viewing ... 78
login ID names ... 76
logout reason code name, adding ... 80
logout reason code name, deleting ... 82
logout reason code name, listing all ... 81
logout reason code name, modifying ... 82
logout reason code name, viewing ... 81
logout reason code names ... 80
reports, printing ... 107
searching ... 42
split/skill name, adding ... 86
split/skill name, deleting ... 88
split/skill name, listing all ... 87
split/skill name, modifying ... 87
split/skill name, viewing ... 87
split/skill names ... 85
split/skill string value, field descriptions ... 84
split/skill string values ... 83
split/skill string values, modifying ... 84
split/skill string values, viewing ... 83
standard CMS item, viewing ... 89
standard database item, viewing ... 89
standard database items ... 89
standard database items, viewing alphabetically ... 90
trunk group name, adding ... 94
trunk group name, deleting ... 95
trunk group name, listing all ... 94
trunk group name, modifying ... 95

ACD Groups *(continued)*
trunk group names ....93
trunk group names, listing all ....95
trunk string value, viewing and modifying ....96
trunk string values ....96
trunk string values, field descriptions ....97
VDN Name, adding ....99
VDN name, deleting ....101
VDN name, listing all ....100
VDN name, modifying ....101
VDN name, viewing ....100
VDN names ....98
vector name, adding ....103
vector name, deleting ....104
vector name, listing all ....104
vector name, modifying ....104
vector name, viewing ....103
vector names ....102
dictionary, overview ....40
Dictionary ACDs Report ....105
Dictionary Login Identifications Report ....106
Dictionary rules ....41
Dictionary Standard CMS Items Report ....106
Dictionary tenant report ....106
Dictionary Trunk Groups Report ....106
Dictionary VDNs Report ....106
Dictionary Vectors Report ....107
disk space
allocating ....275
Does not exist status message ....33
duration of standard full maintenance backup to tape ....320

## E

EAS (see Expert Agent Selection), Expert Agent Selection 21
EAS (See Expert Agent Selection), Expert Agent Selection ....125
entity formats, defining ....39
error and warning messages ....123
error log messages
maintenance ....345
Error status message ....33
events that start or stop data collection ....28
exceptiona ....176
exception capacities ....178
exception counter ....33
Exception reports ....205
exceptions
agent ....180
agent, adding ....181
agent, definitions ....184
agent, deleting ....183
agent, modifying ....182
agent, report ....206
data collection ....207
definition ....176
malicious call trace report ....208
notification ....179
notification, changing ....180
Real-time exceptions log ....204
split/skill ....187
split/skill, adding ....187
split/skill, definitions ....190
split/skill, deleting ....189
split/skill, modifying ....188
split/skill, report ....209
trunk group ....191
trunk group, adding ....192
trunk group, deleting ....194
trunk group, modifying ....193
trunk group, report ....211
VDN, adding ....196
VDN, deleting ....198
VDN, modifying ....197
VDN, report ....212
vector ....200
vector, adding ....201
vector, deleting ....203
vector, modifying ....202
vector, report ....214
Expert Agent Selection (EAS)
agent trace ....125
export
report output ....119
Export All Data window ....119
Export Chart Data window ....119
extensions
split assignments, changing ....140
splits, moving between ....142
external applications
starting or stopping ....283
states, viewing ....282
External Application Status feature ....281
disabling ....282
enabling ....282

## F

Failed status message ....33
feature access ....229
Feature Access
user permissions, listing all ....231
user permissions, modifying ....232
user permissions, viewing ....231
First Day of Week ....34
for changing
agent skills ....130
Free Space Allocation ....284
contents, viewing ....285
viewing ....284

## G

generic string values synonyms ....73

global search results ..... 43

## H

historical data
archiving ..... 280
historical databases ..... 22
how Avaya CMS stores ACD data ..... 22
how CMS tracks a call ..... 27
how CMS tracks ACD data ..... 27

## I

Informix Dynamic Server (IDS) ..... 284
Informix Software, Inc.INFORMIX
interface to historical database ..... 21
input window
scripting ..... 121
interactive and automatic scripts ..... 116
interactive report script
creating ..... 118
interfaces for reports ..... 110
interval
intrahour ..... 300
intrahour, changing ..... 301
intervals
storage ..... 300
storage, viewing ..... 300
intrahour interval ..... 300
changing ..... 301

## L

listing agents in an agent group ..... 49
listing agents traced ..... 128
listing all
trunk group user permissions ..... 246, 258
vector user permissions ..... 252
listing all announcements on an ACD ..... 55
listing all AUX reason code names ..... 59
loading
pseudo-ACDs ..... 298
location IDs ..... 74
logging in to CMS ..... 372
login ID name
adding ..... 77
deleting ..... 79
listing ..... 78
modifying ..... 79
viewing ..... 78
login ID names ..... 76
login status ..... 33
logout reason code name
adding ..... 80
deleting ..... 82
listing all ..... 81
modifying ..... 82
viewing ..... 81
logout reason code names ..... 80

## M

Main Menu
Addition Access, assigning/modifying ..... 234
Addition Access, listing all ..... 234
Addition Access, viewing ..... 233
Main Menu Addition Access ..... 232
maintenance backup ..... 317, 327
Maintenance Error Log
running ..... 344
Maintenance Error Log, running ..... 344
Maintenance Error Log messages ..... 345
maintenance reports ..... 343
Maintenance tool ..... 308
malicious call trace
report ..... 208
master ACD
see ACD ..... 272
methods for backup and restore, alternative ..... 319
migrating
from a non-tape device ..... 320
migrating CMS data ..... 285, 286
modifying
CMS users ..... 222
split/skill user permissions ..... 241
trunk group user permissions ..... 247
vector user permissions ..... 253
modifying a custom calculation ..... 63
modifying an ACD name ..... 46
modifying an announcement name ..... 56
modifying an AUX reason code name ..... 59
modifying Data Storage Allocation ..... 275
modifying data summarizing settings ..... 304
modifying generic string values ..... 73
Multi-Agent Skill Change in CMS Supervisor Web ..... 138
multi-user mode
setting ..... 271

## N

Name Format Tab ..... 38
new report color scheme, creating ..... 36
N matches found ..... 33
No matches found status message ..... 33
No permission status message ..... 33
notification ..... 177

## O

operating system ..... 21
operating system, using ..... 372
Options

Options *(continued)*
Communications Tab ..... 38
Default ACD ..... 34
First Day of Week ..... 34
general ..... 34
Name Format Tab ..... 38
report colors ..... 36
threshold colors ..... 37
time synchronization ..... 34
Options...
Communications Tab ..... 36
Options window, before using ..... 32

## P

password
aging ..... 375
passwords
choosing ..... 373
pemissions
for split/skill call profiles ..... 159
permission
for Data Storage Allocation ..... 275
permissions
ACD ..... 224
ACD groups ..... 44
ACDs ..... 46
announcement names ..... 54
AUX reason code names ..... 57
for ACD Administration Log ..... 367
for ACD groups ..... 148
for ACD status ..... 309
for adding a CMS user ..... 217
for administering a printer ..... 341
for administering report properties ..... 370
for agent exceptions ..... 181
for agent groups ..... 48
for agent string values ..... 51
for Archiving Status ..... 311
for backing up data for a pseudo-ACD ..... 295
for Backup/Restore Devices ..... 313
for calculations ..... 60
for call work codes ..... 64, 154
for changing agent skills ..... 130
for changing extension split assignments ..... 141
for changing skills for multiple agents ..... 137
for CMS State ..... 271
for Connection Status ..... 338
for constants ..... 67
for custom database items ..... 70
for Data collection ..... 273
for Data summarizing ..... 280
for dictionary reports ..... 105
for External Application Status ..... 281
for Free Space Allocation ..... 284
for Generic string values synonyms ..... 73
for listing agents traced ..... 127
permissions *(continued)*
for loading pseudo-ACD data ..... 297
for location IDs ..... 74
for login IDs ..... 77
for logout reason code names ..... 80
for Main Menu Addition Access ..... 233
for migrating CMS data ..... 286
for modifying CMS users ..... 222
for moving extensions between splits ..... 143
for performing a CMSADM backup ..... 325
for performing a maintenance backup ..... 327
for pseudo-ACDs ..... 290
for restoring data ..... 335
for running a split members report ..... 144
for shortcuts ..... 400
for split/skill access ..... 238
for split/skill exceptions ..... 187
for Split/Skill names ..... 86
for split/skill string values ..... 83
for standard database items ..... 89
for starting or stopping an agent trace ..... 126
for Storage intervals ..... 300
for Switch Setup ..... 306
for the ACD access window ..... 225
for the Feature Access window ..... 230
for the Trunk Group Access window ..... 244
for timetables ..... 378
for trunk group assignments ..... 163
for trunk group exceptions ..... 192
for trunk group members report ..... 166
for trunk group names ..... 93
for trunk string values ..... 96
for VDN call profiles ..... 169
for VDN exceptions ..... 196
for VDN names ..... 99
for VDN skill preferences ..... 157
for VDN-to-vector assignments ..... 167
for vector access ..... 250
for vector configuration report ..... 173
for vector exceptions ..... 201
for viewing CMS users ..... 220
Main Menu Addition Access, assigning/modifying ..... 234
Main Menu Addition Access, listing all ..... 234
Main Menu Addition Access, viewing ..... 233
split/skill, adding user ..... 238
split/skill, deleting user ..... 242
split/skill, listing all ..... 240
split/skill, listing all user ..... 240
split/skill, modifying user ..... 241
split/skill, viewing user ..... 239
trunk group, adding user ..... 244
trunk group, deleting user ..... 248
trunk group, listing all user ..... 246
trunk group, modifying user ..... 247
trunk group, viewing user ..... 245
user, adding ACD ..... 225
user, deleting ACD ..... 228

permissions *(continued)*
user, listing all ACD ... 227
user, listing all Feature Access ... 231
user, modifying ACD ... 227
user, modifying Feature Access ... 232
user, viewing ACD ... 226
user, viewing Feature Access ... 231
VDN, adding user ... 256
VDN, deleting user ... 260
VDN, listing all user ... 258
VDN, modifying user ... 258, 259
VDN, viewing user ... 257
VDN access ... 256
vector, adding user ... 250
vector, deleting user ... 254
vector, listing all user ... 252
vector, modifying user ... 253
vector, viewing user ... 251
permitted ones displayed ... 33
phantom abandon call timer ... 305
print
setup ... 114
printer
adding ... 341
deleting ... 343
listing all ... 342
modifying options ... 342
printing a Historial report ... 113
printing a report ... 113
print window ... 113
pseudo-ACD
data, loading ... 297
pseudo-ACDs
backing up ... 295
creating ... 290
deleting ... 293
loading ... 298
viewing ... 293
Pseudo-ACDs ... 289

## R

R3 Migrate Data field descriptions ... 287
recommendation to restart your CMS server ... 337
recovery kit ... 331
reducing tape backup and restore times ... 319
related documentation ... 19
report colors ... 36
Report Designer ... 110
report properties, administering ... 369
report properties, modifying ... 370
reports
ACD Administration Log ... 367
choosing ... 111
colors ... 37
configuring ... 110
custom ... 110
data collection ... 207
Dictionary ... 105
Dictionary, printing ... 107
exceptions, agent ... 206
exceptions, trunk group ... 211
generating ... 112
interfaces ... 110
malicious call trace ... 208
members, trunk group ... 165
printing ... 113
print setup, changing ... 114
restarting ... 114
split/skill, exceptions ... 209
split members, running ... 144
to summarize ... 111
types of ... 110
VDN, exceptions ... 212
vector, exceptions ... 214
Reports input window ... 113
reports saved as HTML ... 120
restarting a report ... 114
Restarting a report in CMS Supervisor Web ... 114
restore
automatic ... 335
manual ... 335
restore database from a binary backup ... 337
restoring
from a non-tape device ... 320
restoring data ... 334, 344
running
real-time exceptions log ... 205
running a split members report ... 144

## S

Save As HTML window ... 120
Save as Script - Action window ... 122
script
creating automatic ... 119
creating to run reports ... 116
exporting report output ... 119
to export report data as HTML ... 120
Script descriptions ... 117
scripting
non-report actions ... 121
scripting an action ... 122
scripting an input window ... 121
Scripting tab ... 35
scripts
accessing ... 116
organizing ... 123
searching the dictionary ... 42
See status window message ... 33
server ... 21
service level
increment ... 160
increments ... 168

settings
ACD, listing all 307
ACD, viewing 306
setting user ID and password 118
setting users 118
setup
ACD/switch 305
severity of errors 345
shortcuts 377
copying 404
copying tasks in 406
creating 401
deleting 410
description, modifying 404
overview 400
running 403
tasks, adding 402
tasks, deleting 408
tasks, modifying 407
single-user mode
setting 271
skills
multiple agents, changing 136
VDN, configuring preferences 156
Skills for multiple agents
Adding 139
Deleting 140
Moving 139
Solaris 372
changing user passwords 374
local login 373
printer commands 375
remote login 372
split
extension assignments, changing 140
extensions, moving 142
members report, running 144
split/skill
call profile, deleting 162
call profile, modifying 162
call profile, viewing 161
call profiles 159
call profiles, adding 160
exceptions 187
exceptions, adding 187
exceptions, defintion 190
exceptions, deleting 189
exceptions, modifying 188
exceptions, report 209
string values 83
user permissions, adding 238
user permissions, deleting 242
user permissions, listing all 240
user permissions, modifying 241
user permissions, viewing 239
Split/Skill access 237
split/skill name
adding 86
deleting 88
modifying 87
viewing 87
split/skill names 85
listing all 87
split/skill string value
field descriptions 84
split/skill string values
modifying 84
viewing 83
split/skill user permissions
adding 238
viewing 239
standard database item
viewing 89
standard database items 89
viewing alphabetically 90
state
changing 271
changing, CMS 271
status indicators on controller window 33
status messages on Controller window 33
storage intervals 300
viewing 300
string values
generic, modifying 73
generic, viewing 73
Successful status message 33
summarizing
data, modifying 303
Summary
Tenancy 29
Sun Microsystems, Inc.Solaris
interface to CMS 21
Supervisor Tenant Administration sub menu 262
support 20
switch
settings, listing all 307
settings, viewing 306
setup 305
synchronize
time zone 302

## T

tape drives and cartridges 317
tasks
timetable, adding 377, 382
timetable, modifying 389
tasks scripts can automate 115
tenancy, administering at a high level 30
Tenant Access 235
Tenant Access window 236
Tenant administration reports 268
tenant administration tenant agent group members report 269
Tenant administration tenant agent groups report 269

Tenant agent assignment ..... 263
Tenant agent groups assignment ..... 267
Tenant Call Work Code assignment ..... 267
Tenant name ..... 91
Adding ..... 91
Deleting ..... 92
Modifying ..... 92
Viewing ..... 91
Tenant names ..... 90
Before using ..... 91
Listing all ..... 92
tenants ..... 262
Tenant split/skill assignment ..... 263
Tenant trunk group assignment ..... 264
Tenant user restricted access ..... 261
Tenant VDN assignment ..... 265
Tenant vector assignment ..... 266
threshold colors ..... 37
time
synchronization, master ACD ..... 272
time synchronization ..... 34
timetable
deleting ..... 398
tasks, adding ..... 377
timetables ..... 377
backups ..... 377
changing ..... 377
copying ..... 385
creating ..... 377, 379
global edits ..... 391
listing all ..... 384
overview ..... 377
prerequisites ..... 377
scheduling ..... 379
tasks, adding ..... 382
tasks, copying ..... 387
tasks, modifying ..... 389
timezone
adjustment, ACD ..... 300
time zone
offset, ACD ..... 302
time zones
updating ..... 411
trace
agent, listing all records ..... 127
trunk group
assignment, viewing a single ..... 164
assignment, viewing by VDN/split ..... 165
assignments ..... 163
exceptions ..... 191
exceptions, adding ..... 192
exceptions, deleting ..... 194
exceptions, modifying ..... 193
exceptions, report ..... 211
members report ..... 165
members report, running ..... 166
user permissions, adding ..... 244
user permissions, deleting ..... 248
user permissions, listing all ..... 246
user permissions, modifying ..... 247
user permissions, viewing ..... 245
Trunk group access ..... 243
trunk group assignments
viewing all ..... 164
Trunk group exception definitions ..... 194
trunk group name
adding ..... 94
deleting ..... 95
listing all ..... 94
modifying ..... 95
trunk group names ..... 93
listing all ..... 95
trunk group user permissions
adding ..... 244
listing all ..... 246, 258
modifying ..... 247
viewing ..... 245
trunk string values ..... 96
field descriptions ..... 97
modifying ..... 96
viewing ..... 96
types of exceptions ..... 176

## U

USB/network backup restore devices ..... 317
user data ..... 217
user permissions
administering ..... 216
user permissions example ..... 216
users
adding ..... 218
deleting ..... 223
Main Menu Addition Access, assigning/modifying ..... 234
Main Menu Addition Access, listing all ..... 234
Main Menu Addition Access, viewing ..... 233
modifying ..... 222
permissions, ACD ..... 224
permissions, adding ACD ..... 225
permissions, adding split/skill ..... 238
permissions, adding trunk group ..... 244
permissions, adding VDN ..... 256
permissions, adding vector ..... 250
permissions, deleting ACD ..... 228
permissions, deleting split/skill ..... 242
permissions, deleting trunk group ..... 248
permissions, deleting VDN ..... 260
permissions, deleting vector ..... 254
permissions, list all split/skill ..... 240
permissions, listing all ACD ..... 227
permissions, listing all Feature Access ..... 231
permissions, listing all split/skill ..... 240
permissions, listing all trunk group ..... 246
permissions, listing all VDN ..... 258

users *(continued)*
permissions, listing all vector ..... 252
permissions, modifying ACD ..... 227
permissions, modifying Feature Access ..... 232
permissions, modifying split/skill ..... 241
permissions, modifying trunk group ..... 247
permissions, modifying VDN ..... 258, 259
permissions, modifying vector ..... 253
permissions, viewing ACD ..... 226
permissions, viewing Feature Access ..... 231
permissions, viewing split/skill ..... 239
permissions, viewing trunk group ..... 245
permissions, viewing VDN ..... 257
permissions, viewing vector ..... 251
viewing ..... 220

## V

VDN
call profile, adding ..... 169
call profile, deleting ..... 172
call profile, modifying ..... 171
call profile, viewing ..... 170
call profiles ..... 168
exceptions, adding ..... 196
exceptions, deleting ..... 198
exceptions, modifying ..... 197
exceptions, report ..... 212
skill preferences ..... 156
skill preferences, changing ..... 157
skill preferences, configuring ..... 156
skill preferences, listing all ..... 158
skill preferences, viewing ..... 158
user permissions, adding ..... 256
user permissions, deleting ..... 260
user permissions, listing all ..... 258
user permissions, modifying ..... 258, 259
user permissions, viewing ..... 257
VDN access ..... 255
VDN exceptions ..... 195
VDN name
adding ..... 99
deleting ..... 101
listing all ..... 100
modifying ..... 101
viewing ..... 100
VDN names ..... 98
VDN-to-vector assignments ..... 167
modifying ..... 168
viewing all ..... 167
viewing by vector ..... 168
vector
configuration report ..... 172
configuration report, running ..... 173
exceptions ..... 200
exceptions, adding ..... 201
exceptions, deleting ..... 203
exceptions, modifying ..... 202
exceptions, report ..... 214
user permissions, adding ..... 250
user permissions, deleting ..... 254
user permissions, listing all ..... 252
user permissions, modifying ..... 253
user permissions, viewing ..... 251
Vector access ..... 249
vector exception definitions ..... 203
vector name
adding ..... 103
deleting ..... 104
listing all ..... 104
modifying ..... 104
viewing ..... 103
vector names ..... 102
vector user permissions
adding ..... 250
listing all ..... 252
modifying ..... 253
viewing ..... 251
videos ..... 19
viewing
CMS users ..... 220
split/skill user permissions ..... 239
trunk group user permissions ..... 245
vector user permissions ..... 251
viewing an AUX reason code name ..... 58
viewing generic string values ..... 73

## W

week
beginning of ..... 303
end of ..... 303
work day
start time ..... 303
stop time ..... 303
working status message, successful status message, error status message, failed status message ..... 33