CONTROL-M
Administrator Guide

Supporting

CONTROL-M/Enterprise Manager version 6.4.01
CONTROL-M/Server version 6.4.01
CONTROL-M/Agent version 6.4.01

September 2008
Contacting BMC Software

You can access the BMC Software website at http://www.bmc.com. From this website, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

**United States and Canada**

<table>
<thead>
<tr>
<th>Address</th>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC SOFTWARE INC</td>
<td>713 918 8800</td>
<td>713 918 8000</td>
</tr>
<tr>
<td>2101 CITYWEST BLVD</td>
<td>or 800 841 2031</td>
<td></td>
</tr>
<tr>
<td>HOUSTON TX 77042-2827</td>
<td></td>
<td></td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Outside United States and Canada**

<table>
<thead>
<tr>
<th>Telephone</th>
<th>Fax</th>
</tr>
</thead>
<tbody>
<tr>
<td>(01) 713 918 8800</td>
<td>(01) 713 918 8000</td>
</tr>
</tbody>
</table>

© Copyright 2008 BMC Software, Inc.

BMC, BMC Software, and the BMC Software logo are the exclusive properties of BMC Software, Inc., are registered with the U.S. Patent and Trademark Office, and may be registered or pending registration in other countries. All other BMC trademarks, service marks, and logos may be registered or pending registration in the U.S. or in other countries. All other trademarks or registered trademarks are the property of their respective owners.

DB2 is a registered trademark of International Business Machines Corporation.

Linux is the registered trademark of Linus Torvalds.

UNIX is the registered trademark of The Open Group in the US and other countries.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

**Restricted rights legend**

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC SOFTWARE INC, 2101 CITYWEST BLVD, HOUSTON TX 77042-2827, USA. Any contract notices should be sent to this address.
Customer support

You can obtain technical support by using the BMC Software Customer Support website or by contacting Customer Support by telephone or e-mail. To expedite your inquiry, see “Before contacting BMC.”

Support website

You can obtain technical support from BMC 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this website, you can

■ read overviews about support services and programs that BMC offers
■ find the most current information about BMC products
■ search a database for issues similar to yours and possible solutions
■ order or download product documentation
■ download products and maintenance
■ report an issue or ask a question
■ subscribe to receive proactive e-mail alerts when new product notices are released
■ find worldwide BMC support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

Support by telephone or e-mail

In the United States and Canada, if you need technical support and do not have access to the web, call 800 537 1813 or send an e-mail message to customer_support@bmc.com. (In the subject line, enter SupID:<yourSupportContractID>, such as SupID:12345). Outside the United States and Canada, contact your local support center for assistance.

Before contacting BMC

Have the following information available so that Customer Support can begin working on your issue immediately:

■ product information
  — product name
  — product version (release number)
  — license number and password (trial or permanent)
■ operating system and environment information
  — machine type
  — operating system type, version, and service pack or other maintenance level such as PUT or PTF
  — system hardware configuration
  — serial numbers
  — related software (database, application, and communication) including type, version, and service pack or maintenance level
■ sequence of events leading to the issue
■ commands and options that you used
■ messages received (and the time and date that you received them)
  — product error messages
  — messages from the operating system, such as file system full
  — messages from related software
License key and password information

If you have questions about your license key or password, contact BMC as follows:

- **(USA or Canada)** Contact the Order Services Password Team at 800 841 2031, or send an e-mail message to ContractsPasswordAdministration@bmc.com.
- **(Europe, the Middle East, and Africa)** Fax your questions to EMEA Contracts Administration at +31 20 354 8702, or send an e-mail message to password@bmc.com.
- **(Asia-Pacific)** Contact your BMC sales representative or your local BMC office.
## Contents

### About this book

- Conventions ................................................................. 21
- Syntax statements ...................................................... 22

### Part 1  Getting started and setting up  

#### Chapter 1  Essentials

- CONTROL-M architecture ............................................. 27
- CONTROL-M/EM components ......................................... 28
- CONTROL-M/Server and Agent components ....................... 30
- CONTROL-M/EM, CONTROL-M/Server, and CONTROL-M Agent
  Infrastructure processes ........................................... 32
- Who is a CONTROL-M Administrator? ............................. 33
- Key terms—user, owner, author .................................. 35
- Starting and stopping infrastructure processes ................. 35
  - Starting and stopping infrastructure processes in Windows 36
  - Starting and stopping infrastructure processes in UNIX and Linux 36
- Using CONTROL-M Configuration Manager ...................... 39
  - Starting CONTROL-M Configuration Manager ................. 39
  - Understanding the display ..................................... 40
  - Adjusting the display ............................................ 42
  - Filtering the display ............................................. 43
  - Viewing a component’s properties ............................. 44
  - Changing your password ......................................... 44
  - Setting your CONTROL-M Configuration Manager preferences .... 44
- Using interactive menus .............................................. 45
- Using the CONTROL-M/EM Root Menu ............................ 46
- Using the CONTROL-M/Server Main Menu ....................... 47
- Using the CONTROL-M System Maintenance Utility Main Menu 47

#### Chapter 2  Connecting components

- Conceptual overview .................................................. 50
- CONTROL-M/Server definition and management ................ 51
- CONTROL-M/Agents and remote hosts ............................ 52
- CONTROL-M/EM Web Launch ...................................... 52
- Recommended task summary ....................................... 54
- Defining CONTROL-M/EM components .......................... 54
Chapter 3 Setting up and managing the scheduling environment

Conceptual overview .................................................. 80
Methods for automating daily job scheduling .................... 81
Automatic prerequisite condition cleanup ......................... 86
Job version management .............................................. 87
Global condition distribution time limits ......................... 88
Alert processing ........................................................ 88
Time zone support ..................................................... 89
Daylight Saving Time support ....................................... 90
Load balancing .......................................................... 90
Shout facility and Shout Destination tables ....................... 91
CONTROL-M/EM periodic job statistics ........................ 92
Job statistics generated by CONTROL-M/Server ............... 93
Group scheduling table displays in ViewPoints ................. 93
CONTROL-M/Agent FileWatcher (ctmfw) ......................... 94
User exits ............................................................... 95
Shell scripts ............................................................ 95
Recommended task summary ....................................... 96
Automating job scheduling ......................................... 97
Preparing for automation ........................................... 98
Customizing the New Day procedure ............................ 98
Setting up User Daily jobs ......................................... 101
Defining jobs that use ctmorder to schedule other jobs ..... 103
Handling interruptions in User Daily job processing ......... 103
Collecting and viewing application server information .... 104
Implementing job version management ......................... 105
Defining quantitative resources, control resources, and global conditions ........................................ 107
Modifying the time limit on Global conditions distribution ........................................................................ 107
Activating scripts with alert data ................................ 108
Implementing time zone support (optional) ....................... 110
Setting up time zone support for jobs ........................... 110
<table>
<thead>
<tr>
<th>Contents 7</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring correct time zones for jobs in the Active Jobs file</td>
</tr>
<tr>
<td>Implementing Daylight Saving Time support</td>
</tr>
<tr>
<td>Editing definitions to support Daylight Saving Time</td>
</tr>
<tr>
<td>Implementing load balancing (node groups)</td>
</tr>
<tr>
<td>Defining and maintaining a node group</td>
</tr>
<tr>
<td>Identifying jobs that can be load balanced</td>
</tr>
<tr>
<td>Setting up Shout Destination Tables</td>
</tr>
<tr>
<td>Defining and maintaining Shout Destination tables</td>
</tr>
<tr>
<td>Making a Shout Destination table the currently active table</td>
</tr>
<tr>
<td>Modifying CONTROL-M/EM periodic statistic retention and cleanup defaults</td>
</tr>
<tr>
<td>Implementing job statistics generated by CONTROL-M/Server</td>
</tr>
<tr>
<td>Setting whether CONTROL-M/Server collects job statistics</td>
</tr>
<tr>
<td>Defining the CONTROL-M/Server statistics collection mode</td>
</tr>
<tr>
<td>Ensuring that the ctmjsa utility runs daily to collect CONTROL-M/Server statistics</td>
</tr>
<tr>
<td>Displaying (or deleting) CONTROL-M/Server statistics as needed</td>
</tr>
<tr>
<td>Displaying empty Group scheduling tables in ViewPoints</td>
</tr>
<tr>
<td>Ensuring that Collection data is retrieved at startup</td>
</tr>
<tr>
<td>Detecting file activity with FileWatcher (ctmfw)</td>
</tr>
<tr>
<td>Implementing user exits</td>
</tr>
<tr>
<td>Writing scripts <em>(UNIX only)</em></td>
</tr>
<tr>
<td>Specifying the shell type</td>
</tr>
<tr>
<td>Factoring in the run-time environment</td>
</tr>
<tr>
<td>Using the On Statement/Code parameter to interpret script lines</td>
</tr>
<tr>
<td>Writing scripts <em>(Windows only)</em></td>
</tr>
<tr>
<td>Implementing basic guidelines</td>
</tr>
<tr>
<td>Using On Statement/Code parameters correctly</td>
</tr>
<tr>
<td>Enabling CONTROL-M/Server to distinguish between exit codes</td>
</tr>
<tr>
<td>Using script utilities</td>
</tr>
<tr>
<td>Translating DOS files and REXX scripts to UNC</td>
</tr>
</tbody>
</table>

**Part 2**

**Implementing security and high availability**

<table>
<thead>
<tr>
<th>Chapter 4</th>
<th>Introduction to implementing CONTROL-M security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic CONTROL-M security concepts</td>
<td>147</td>
</tr>
<tr>
<td>Security flow</td>
<td>148</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Chapter 5</th>
<th>Setting up CONTROL-M authentication security</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conceptual overview</td>
<td>150</td>
</tr>
<tr>
<td>Authentication methods</td>
<td>151</td>
</tr>
<tr>
<td>Password requirements and expiration warnings</td>
<td>152</td>
</tr>
<tr>
<td>Administrator passwords</td>
<td>153</td>
</tr>
<tr>
<td>Recommended task summary</td>
<td>153</td>
</tr>
<tr>
<td>Setting the authentication method</td>
<td>154</td>
</tr>
<tr>
<td>Authenticating CONTROL-M/EM users against an LDAP or Active Directory server</td>
<td>155</td>
</tr>
<tr>
<td>Implementing external plug-in authentication</td>
<td>158</td>
</tr>
</tbody>
</table>
Defining password requirements ........................................... 160
Refreshing password-related system parameters ....................... 160
Setting allowable password lengths ..................................... 161
Setting password complexity rules (required character types) ........ 161
Setting password reuse limits ............................................. 162
Implementing password expiration policy .............................. 163
Implementing password policy for all users using the set_pwd_def_lifetime script ............................................. 164
Setting automatic account locking after consecutive failed logon attempts .................................................... 165
Unlocking multiple accounts with the unlock_user script ............ 166
Defining users and their authentication criteria to CONTROL-M/EM .................................................. 166
Manually modifying a user’s password criteria ......................... 169
Changing the DBO password ............................................... 170
Defining a CONTROL-M/Agent account (Windows only) ............ 170
Defining job owner and authentication settings for CONTROL-M/Agents and remote hosts ........................................ 173

Chapter 6  Setting up CONTROL-M authorization security 177

Conceptual overview ....................................................... 177
CONTROL-M/EM authorization security ................................. 179
CONTROL-M/Server authorization security ............................. 180
CONTROL-M/Agent security ............................................... 182
Recommended task summary ............................................... 184
Implementing CONTROL-M/EM authorization security ................ 184
  Creating and deleting group security definitions .................... 185
  Defining which group profiles apply to a user ....................... 186
  Defining or modifying user or group authorization details .......... 186
  Ensuring owner verification during New Day processing job ordering .................................................. 197
  Authorizing non-administrators to manage application accounts .................................................. 200
Enabling passage of global conditions from GCS to CONTROL-M/Servers .................................................. 202
Changing the default Global Conditions Server user name .......... 202
Implementing CONTROL-M/Server authorization security .......... 202
  Adding, deleting and modifying users and groups ................ 204
  Assigning authorizations to users and groups ..................... 205
  Activating CONTROL-M/Server security ............................ 206
Implementing CONTROL-M/Agent and remote host authorization security .................................................. 207
  Implementing CONTROL-M/Agent job owner security (Windows only) .................................................. 207
  Implementing CONTROL-M/Agent remote host security .......... 208
  Authorizing which CONTROL-M/Server utilities a CONTROL-M/Agent can request ........................................ 209

Chapter 7  Implementing CONTROL-M security auditing 211

Conceptual overview ....................................................... 211
Servers for auditing ....................................................... 212
Audit records ............................................................... 212
Recommended task summary ............................................... 213
Setting up auditing ........................................................ 213
Enabling auditing .......................................................... 213
Setting which activities will be audited ......................................................... 214
Refreshing the list of activities handled by each server ............................... 215
Setting up or stopping automatic deletion of old audit records ................... 215
Viewing audit records ................................................................. 216

Chapter 8  Setting up CONTROL-M firewall security  217

Conceptual overview ................................................................................. 217
Communication between CONTROL-M/EM clients and servers ............... 218
Communication between CONTROL-M/Server and CONTROL-M/EM ....... 219
Communication between agents and CONTROL-M/Server ....................... 219
Recommended task summary ............................................................... 221
Enabling communication between CONTROL-M/EM clients and servers ... 222
Enabling communication between CONTROL-M/Server and CONTROL-M/EM 223
Enabling communication between agents and CONTROL-M/Server ......... 224

Chapter 9  Configuring CONTROL-M for high availability  227

Conceptual overview ................................................................................. 228
Methods of ensuring high availability ........................................................ 228
Mirroring and failover .............................................................................. 229
Recommended task summary ............................................................... 230
Preparing to implement mirroring or failover ............................................ 231
Reviewing prerequisites .......................................................................... 231
Gathering worksheet data ....................................................................... 232
Performing additional preparations .......................................................... 241
Preparing the failover CONTROL-M/Server ........................................... 245
Implementing database mirroring ............................................................. 247
Building and initializing a new CONTROL-M mirror database ................. 247
Changing over to the mirror database following primary database failure ... 249
Changing back to the primary database after fixing the problem .............. 250
Disabling mirroring ................................................................................. 250
Implementing Failover ............................................................................ 251
Initializing the failover system ................................................................. 252
Changing over to the failover CONTROL-M/Server in an emergency ....... 254
Changing back to the primary CONTROL-M/Server after fixing the problem 255
Disabling the failover system ................................................................. 256
Periodically synchronizing the primary and mirror database .................... 257

Part 3  Maintaining and managing CONTROL-M  261

Chapter 10  Maintaining the CONTROL-M environment  263

Conceptual overview ................................................................................. 264
CONTROL-M/EM server and CONTROL-M/Server component states ....... 265
CONTROL-M/Server management .............................................................. 265
Heartbeat monitor and Watchdog facility ................................................ 266
Remote host network disconnections ....................................................... 267
Recommended task summary ............................................................... 267
Starting and stopping CONTROL-M/EM server components and
CONTROL-M/Server ................................................................. 268
Starting and stopping CONTROL-M/Agent .................................. 269
For UNIX ................................................................................. 269
For Windows ............................................................................ 270
Recycling CONTROL-M/Agent .................................................... 271
Manually testing CONTROL-M/Server communication with Agents and remote hosts .............................................................. 272
Viewing CONTROL-M/EM component activation history ................ 272
Sending Control Shell commands ................................................ 273
Managing CONTROL-M/Servers .................................................. 274
Setting whether a CONTROL-M/Server is managed or unmanaged from
CONTROL-M/EM .................................................................... 274
Disabling and enabling a CONTROL-M/Server ......................... 275
Deleting a CONTROL-M/Server definition from CONTROL-M/EM ... 275
Implementing Heartbeat Monitors and the Watchdog facility ....... 275
Managing CONTROL-M/Agents .................................................. 276
Disabling a CONTROL-M/Agent ............................................... 276
Setting debug on CONTROL-M/Agent ...................................... 276
Setting CONTROL-M/Agent system parameters ......................... 278

Chapter 11 Maintaining databases and CONTROL-M data 281

Conceptual overview ............................................................... 282
CONTROL-M databases ............................................................. 284
Database maintenance menus .................................................... 284
CONTROL-M/EM database backup, archive, and restore ............ 284
CONTROL-M/Server database backup, archive, rebuild, and restore 284
Automatic and manual database cleanup .................................. 286
Recommended task summary ..................................................... 286
Maintaining Databases ............................................................... 287
Implementing CONTROL-M/Server database archiving, backup, and restore ................................................................. 291
Enabling archiving of a CONTROL-M/Server database (Oracle and PostgreSQL only) ................................................................. 291
Backing up a CONTROL-M/Server database .............................. 292
Adding a new CONTROL-M/Server backup device .................... 294
Restoring a CONTROL-M/Server database from a backup ......... 295
Rebuilding a CONTROL-M/Server database ............................... 297
Managing the CONTROL-M/EM database ................................. 299
Exporting and importing CONTROL-M/EM data ....................... 299
Exporting and importing audit records ...................................... 301
Exporting and importing CONTROL-M/Server security definitions 301
Performing periodic CONTROL-M/EM database maintenance and cleanup ................................................................. 302
Checking available space in the CONTROL-M/EM database ....... 302
Extending the CONTROL-M/EM database ................................. 303
Cleaning up CONTROL-M/EM database error log files ............. 304
Removing old archived networks .............................................. 304
Removing old alerts ............................................................... 305
Removing old job versions ...................................................... 306
Removing exception alerts ...................................................... 306
### Part 4 Diagnostics and troubleshooting

#### Chapter 12 Diagnostics: conceptual information
- Basic diagnostic mechanisms ................................................................. 320
  - Source Level Debugging ................................................................. 320
  - Communication Traces ................................................................. 321
  - Exception Alerts ........................................................................... 321
- Basic diagnostic capability in CONTROL-M ........................................... 322
- Common symptoms, causes and best practices .................................... 322

#### Chapter 13 Activating diagnostics
- Activating CONTROL-M/EM diagnostics ............................................. 329
  - Activating source level debugging diagnostics .................................... 330
  - Activating Communication Trace Diagnostics ..................................... 337
- Activating diagnostics for CONTROL-M/Server .................................... 339
- Activating diagnostics for CONTROL-M/Agent ..................................... 340

#### Chapter 14 Collecting diagnostic data
- CONTROL-M data for BMC support (Health Check utility) ....................... 343

#### Chapter 15 Processes of elimination and analysis
- Troubleshooting by process of elimination ........................................... 346
  - Checking communication status between CONTROL-M/EM and CONTROL-M/Server .................................................. 346
  - Checking CONTROL-M/EM communication ..................................... 347
  - GUI Server: Processes of elimination .............................................. 349
  - Global Conditions Server: processes of elimination ......................... 352
  - Naming Service and Firewall functionality ..................................... 353
- Analyzing diagnostic data for CONTROL-M/Server ................................ 367
  - Troubleshooting menu analyzing options ......................................... 367
  - Process of elimination ................................................................. 369
- Log files: Analyzing ........................................................................... 371
- Working with Exception Alerts ......................................................... 375
Part 5  Appendixes  379

Appendix A  Configuring CORBA components  381

Concepts
  CORBA overview
  Naming Service
  What is an Interoperable Object Reference (IOR)?
  Advanced communication policies
  Assigning ports when using a firewall
  XML configuration file scopes
Recommended task summary
Configuring CORBA components
  Specifying domain settings
  Specifying Naming Service settings
  Assigning ports
  Specifying Advanced parameters

Appendix B  System parameters  403

Concepts
  Parameter modification
  Component refresh
Tasks
  Modifying CONTROL-M/EM system parameters
  Modifying CONTROL-M/Server system parameters
  Modifying CONTROL-M/Agent system parameters
  Modifying CONTROL-M for z/OS system parameters
  Refreshing CONTROL-M/EM components
  Refreshing CONTROL-M/Server components
  Refreshing CONTROL-M/Agent components
System parameter reference
  CONTROL-M/EM parameters
  CONTROL-M/Server parameters
  CONTROL-M/Agent parameters

Appendix C  Exits  523

User Exits
  Job Order Exit (CTMUE101)
  Job Submission Exit (CTMUE102)
  Before New Day Procedure Exit (CTMUE103)
  After New Day Procedure Exit (CTMUE104)
  Before User Daily Exit (CTMUE105)
  After User Daily Exit (CTMUE106)
Watchdog facility exits
  Enabling the Watchdog facility to run the ctdiskspace or ctmdbspace utilities, or other scripts
  Enabling the Watchdog facility to run the user-defined scripts or
  CONTROL-M/Server utilities
Defining the error handler criteria for the Watchdog facility . . . . . . . . . . . . . . . . 531

**Appendix D**  **SNMP interface**  533

Overview ........................................................................................................ 533
CONTROL-M/EM and SNMP traps .............................................................. 534
  SNMP trap format ....................................................................................... 534
  Customization ............................................................................................. 535

**Appendix E**  **Mass conversion of agents and remote hosts**  537

Converting multiple CONTROL-M/Agents to remote hosts .................... 537

**Appendix F**  **Working with Remedy**  539

Configuring the connection to the Remedy server ................................... 539
Refining Remedy incident information ......................................................... 540

**Index**  543
## Figures

CONTROL-M/EM architectural structure .......................................................... 28  
CONTROL-M/Server and Agent architectural structure ...................................... 31  
CONTROL-M Configuration Manager ................................................................. 40  
Options dialog box for CONTROL-M Configuration Manager ............................. 45  
CONTROL-M/EM Root Menu ............................................................................. 46  
CONTROL-M Main Menu .................................................................................. 47  
CONTROL-M System Maintenance Utility Main Menu ......................................... 48  
Recommended workflow for connecting CONTROL-M components .................... 50  
CONTROL-M/Agent Properties dialog box ......................................................... 64  
Recommended workflow for setting up the scheduling environment .................. 81  
Using the Active Shout Destination Table to direct shouts ............................... 91  
Sample Rull.dat file ......................................................................................... 128  
Sample Trace File Output ................................................................................ 129  
Recommended workflow for setting up authentication security ......................... 150  
Recommended workflow for setting up authorization security ........................... 179  
CONTROL-M/Server Security dialog box ......................................................... 203  
Recommended workflow for implementing auditing .......................................... 212  
Recommended workflow for setting up firewall security ................................... 218  
Transient connection model ............................................................................. 220  
Persistent connection model ............................................................................ 221  
Recommended workflow for configuring CONTROL-M for high availability ...... 229  
CONTROL-M/Server Mirroring ......................................................................... 230  
Recommended workflow for maintaining the CONTROL-M environment .......... 264  
Recommended workflow for maintaining and managing databases .................. 283  
CONTROL-M/Server Debug window ................................................................ 339  
CONTROL-M/Agent Debug window ................................................................. 340  
Excerpt from a GCS_LOG File ......................................................................... 373  
Exception Alerts window .................................................................................. 376  
Recommended workflow for connecting CONTROL-M/Enterprise Manager components .......................................................... 382  
Naming Service directory illustration ............................................................... 385  
Domain Settings panel—Domain Configuration (orbconfigure) wizard .............. 394  
Naming Service panel—Domain Configuration (orbconfigure) wizard .............. 396  
Show local settings—Naming Service panel (orbconfigure) wizard ................... 397  
Ports panel—Domain Configuration (orbconfigure) wizard ............................... 398  
Summary panel—Domain Configuration (orbconfigure) wizard ......................... 400  
Advanced settings—Summary panel (orbconfigure) wizard .............................. 400  
CONTROL-M Main Menu ................................................................................. 406
## Tables

Component icons ................................................. 41
Task summary: connecting components ........................ 54
CONTROL-M Definition dialog box ............................. 58
Parameters for manually defining a CONTROL-M/Server and its Gateway .......................... 59
Task summary: setting up the scheduling environment .......................... 96
Parameters for the Global Conditions distribution facility ......................... 108
Fields and values of the Shout Destination table .......................... 117
CONTROL-M General User Exits ................................ 129
Shell paths ......................................................... 131
Shell parameters .................................................. 132
CTMBAT2UNC Utility Parameters .................................. 142
Scripts before and after running CTMBAT2UNC .............. 142
Task summary: setting up the scheduling environment ......................... 154
Application security levels for CONTROL-M/Server .......................... 182
Task summary: setting up authorization security ......................... 184
Privileges tab access levels ......................................... 189
Privileges and features ............................................. 190
Scheduling table authorization ........................................ 191
Scheduling table access levels ...................................... 192
Access levels for conditions and resources .......................... 195
Calendar access levels .............................................. 196
Terms ............................................................. 198
Task summary: implementing auditing .............................. 213
Parameter values for activities to be audited ......................... 214
Task summary: configuring CONTROL-M for high availability ......................... 231
Relevant worksheet tables by database server type ......................... 232
Worksheet for database parameter values—Sybase ......................... 233
Worksheet for mirroring parameters (when *copying*)—Sybase ......................... 233
Worksheet for mirroring parameters (when *building*)—Sybase ......................... 234
Worksheet for environment variables and alternative names—Sybase ......................... 235
Worksheet for database parameter values—Oracle ......................... 236
Worksheet for mirroring parameters—Oracle ......................... 236
Worksheet for environment variables—Oracle ......................... 237
Worksheet for database parameter values—MSSQL ......................... 237
Worksheet for MSSQL Server mirroring parameters ......................... 238
Worksheet for MSSQL environment variables—MSSQL ......................... 238
Worksheet for database parameter values—PostgreSQL ......................... 239
Worksheet for mirroring parameters—PostgreSQL ......................... 239
Worksheet for environment variables and alternative names—PostgreSQL ......................... 240
Additional required details—Sybase ................................ 241
About this book

The *CONTROL-M Administrator Guide* is a single, inclusive guide that replaces the:

- **CONTROL-M/Enterprise Manager Administrator Guide**
- **CONTROL-M/Server Administrator Guide**
- **CONTROL-M/Agent Administrator Guide**

However, most of the utility descriptions from those earlier guides have been moved to the *CONTROL-M Utility Guide*.

The *CONTROL-M Administrator Guide* contains concepts and procedures CONTROL-M administrators and database administrators (DBAs) need to administer and maintain the following products:

- **CONTROL-M/Enterprise manager version 6.4.01**
- **CONTROL-M/Server version 6.4.01**
- **CONTROL-M/Agent version 6.4.01**

The examples provided in this guide assume the use of cshell. If your site uses a different shell type, it is your responsibility to adjust the instructions to fit your site’s needs.

**NOTE**

- BMC Software recommends that before you use this book, you become familiar with the concepts presented in the *CONTROL-M Concepts Guide*.
- This book assumes that CONTROL-M is already installed and initially configured. The installation and configuration tasks are described in the *CONTROL-M Installation Guide*.
- This book does not discuss end-user tasks (for example, defining job processing definitions or monitoring jobs in the production environment). Those tasks are described in the *CONTROL-M User Guide*.

This guide is divided into parts, each covering a major CONTROL-M administration area. Each part contains relevant chapters.

Most chapters in this book have the following format features:

- Conceptual information is separated from task procedures.
Conventions

- Conceptual information is provided at the beginning of the chapter; tasks are provided after all conceptual information in the chapter has been provided.

- At the beginning of the conceptual information is a workflow chart that identifies top level tasks the administrator performs and page numbers where those tasks begin.

- At the end of the conceptual information, immediately before the task descriptions is a task summary table that identifies the top level tasks, the lower level tasks that comprise the top level task, and the page numbers where those lower level tasks begin.

Like most BMC documentation, this book is available in printed and online formats. To request printed books or to view online books and notices (such as release notes and technical bulletins), see the Customer Support website at http://www.bmc.com/support_home. Most product shipments also include the books on a documentation CD.

**NOTE**

Online books are formatted as PDF or HTML files. To view, print, or copy PDF books, use the free Adobe Reader from Adobe Systems. If your product installation does not install the reader, you can obtain the reader at http://www.adobe.com.

The software also offers online Help. To access Help, press F1 within any product or click the Help button in graphical user interfaces (GUIs).

Conventions

This book uses the following special conventions:

- All syntax, operating system terms, and literal examples are presented in this typeface.

- Variable text in path names, system messages, or syntax is displayed in italic text:
  
  `testsys/instance/fileName`

- The symbol => connects items in a menu sequence. For example, Actions => Confirm instructs you to choose the Confirm command from the Actions menu.
Syntax statements

The following example shows a sample syntax statement:

```
COMMAND KEYWORD1 [KEYWORD2 | KEYWORD3] KEYWORD4={YES | NO} fileName...
```

The following table explains conventions for syntax statements and provides examples:

<table>
<thead>
<tr>
<th>Item</th>
<th>Example</th>
</tr>
</thead>
</table>
| Items in italic type represent variables that you must replace with a name or value. If a variable is represented by two or more words, initial capitals distinguish the second and subsequent words. | alias
|                                                                    | databaseDirectory                           |
|                                                                    | serverHostName                              |
| Brackets indicate a group of optional items. Do not type the brackets when you enter the option. A comma means that you can choose one or more of the listed options. You must use a comma to separate the options if you choose more than one option. | [tableName, columnName, field]
|                                                                    | [-full, -incremental, -level] (Unix)        |
| Braces indicate that at least one of the enclosed items is required. Do not type the braces when you enter the item. | {DBDName | tableName}
|                                                                    | UNLOAD device={disk | tape. fileName | deviceName}
|                                                                    | (-a | -c) (Unix)                              |
| A vertical bar means that you can choose only one of the listed items. In the example, you would choose either commit or cancel. | {commit | cancel}
|                                                                    | {-commit | -cancel} (Unix)                     |
| An ellipsis indicates that you can repeat the previous item or items as many times as necessary. | columnName . . .                           |
Getting started and setting up

This part presents the following topics:

Chapter 1
Essentials ................................................................. 27

Chapter 2
Connecting components ........................................... 49

Chapter 3
Setting up and managing the scheduling environment .......... 79
Chapter 1 Essentials

This chapter presents the following topics:

CONTROL-M architecture .......................................................... 27
  CONTROL-M/EM components .................................................... 28
  CONTROL-M/Server and Agent components ............................... 30
  CONTROL-M/EM, CONTROL-M/Server, and CONTROL-M Agent
    Infrastructure processes ....................................................... 32
Who is a CONTROL-M Administrator? ........................................ 33
Key terms—user, owner, author ................................................ 35
Starting and stopping infrastructure processes ............................ 35
  Starting and stopping infrastructure processes in Windows .......... 36
  Starting and stopping infrastructure processes in UNIX and Linux .... 36
Using CONTROL-M Configuration Manager ................................ 39
  Starting CONTROL-M Configuration Manager ........................... 39
  Understanding the display .................................................... 40
  Adjusting the display ........................................................ 42
  Filtering the display .......................................................... 43
  Viewing a component’s properties ......................................... 44
  Changing your password ...................................................... 44
  Setting your CONTROL-M Configuration Manager preferences .... 44
Using interactive menus .......................................................... 45
  Using the CONTROL-M/EM Root Menu .................................... 46
  Using the CONTROL-M/Server Main Menu ............................... 47
  Using the CONTROL-M System Maintenance Utility Main Menu .... 47

CONTROL-M architecture

This section describes and illustrates the basic CONTROL-M/EM and
CONTROL-M/Server architectural structures. These structures communicate by
using the TCP/IP protocol.
CONTROL-M/EM components

Figure 1 on page 28 illustrates CONTROL-M/EM component architecture. A brief description of the main CONTROL-M/EM components follows.

**Figure 1  CONTROL-M/EM architectural structure**

- **client components**

The primary client components include:

- CONTROL-M Configuration Manager GUI—the main CONTROL-M administrator interface to CONTROL-M/EM, CONTROL-M/Server and CONTROL-M/Agent. It provides a single point of control for administering the CONTROL-M environment and enables you to manage many of your CONTROL-M administrative tasks from a central location. Its usage is described in detail throughout this guide.
CONTROL-M/EM components

— CONTROL-M/Desktop—GUI interface used by end-users for modeling the production environment (defining jobs). Its usage is described in detail in the CONTROL-M User Guide.

— CONTROL-M/EM GUI—GUI interface used by end-users and administrators for monitoring the production environment and intervening when necessary. Its usage is described in detail in the CONTROL-M User Guide.

— CONTROL-M Reporting facility—facility and GUI used by end-users and administrators for generating useful reports of many types. Described in the CONTROL-M User Guide.

— Command line utilities—Many functions that are available through the GUIs are also available through the use of interactive and batch utilities. Utilities are described in the CONTROL-M Utility Guide. Where appropriate, this guide also describes certain interactive utility functions.

■ CONTROL-M/EM server components

— GUI Server—provides information to, and handles user requests issued through, the CONTROL-M/Enterprise Manager window.

— Gateway—interface that handles communication between CONTROL-M/EM and CONTROL-M/Server. A different gateway is dedicated to each CONTROL-M/Server. The gateway is defined when the CONTROL-M/Server is defined. CONTROL-M/EM and CONTROL-M for z/OS also interface through a gateway.

— Configuration Management Server (CMS)—interfaces with the configuration agents of CONTROL-M/Server and CONTROL-M for z/OS to provide information to, and handle administrator requests issued through, the CONTROL-M Configuration Manager.

— Global Alerts server (GAS)—manages alerts to CONTROL-M/EM GUIs

— Global Conditions server (GCS)—distributes global conditions to different CONTROL-Ms.

— Batch Impact Manager (BIM) server—monitors critical batch services when your site uses the BMC Batch Impact Manager add-on.

— Forecast server—helps you predict job patterns in order to forecast schedules for running jobs in the future, when your site uses the CONTROL-M/Forecast add-on.
CONTROL-M/Server and Agent components

- **infrastructure components**

These components include:

- CONTROL-M/EM Configuration Agent—interface between CONTROL-M/EM Configuration Manager Server and other CONTROL-M/EM servers that provides CONTROL-M/EM server information to, and handles administrator requests issued through, the CONTROL-M Configuration Manager.

- CONTROL-M/EM database (Oracle, Sybase, MSSQL, or PostgreSQL) where CONTROL-M/EM data resides

- CORBA-based naming services, which enables the client to locate the server to which it must connect. For more information, see Appendix A, “Configuring CORBA components.”

- CONTROL-M Web Server, used for deploying CONTROL-M client components on client computers

---

**CONTROL-M/Server and Agent components**

Figure 2 on page 31 illustrates CONTROL-M/Server and Agent component architecture. A brief description of the main CONTROL-M/Server and Agent components follows.
CONTROL-M/Server

Heart of the CONTROL-M family of products, CONTROL-M/Server submits jobs for execution on Agent or remote host computers, monitors the jobs and performs post-processing analysis, after which it may perform post-processing actions. The completion status of jobs and the results of post-processing analysis are transmitted to CONTROL-M/Enterprise Manager.

Agent computers

An agent computer is one on which CONTROL-M/Agent has been installed. CONTROL-M/Agent submits jobs for execution, monitors the jobs, and performs post-processing analysis of output files. The completion status of jobs and the results of post-processing analysis are transmitted back to CONTROL-M/Server. CONTROL-M/Agent can submit jobs to a remote host for execution.
■ Remote host computers

Agentless computer on which jobs can run. Each remote host is identified by its node ID.

■ Control Modules

Control Modules (CMs) enable CONTROL-M/Agents to interface with the external applications (for example SAP and Oracle E-Business Suite).

■ infrastructure components

These components include:

— CONTROL-M/Server Configuration Agent — interfaces with CONTROL-M/EM Configuration Manager Server to provide CONTROL-M/Server information to, and handle administrator requests issued through, the CONTROL-M Configuration Manager.

— CONTROL-M/Server database (Oracle, Sybase, MSSQL, or PostgreSQL)— repository of CONTROL-M/Server data. One database exists for each CONTROL-M/Server, which maintains the database by using a dedicated or shared SQL server.

**CONTROL-M/EM, CONTROL-M/Server, and CONTROL-M Agent Infrastructure processes**

**CONTROL-M/EM processes**

CONTROL-M/EM provides the following processes:

■ Naming Service: TAO NT Naming Service

■ CONTROL-M/EM processes:

— CONTROL-M Configuration Management Server (CMS)
— CONTROL-M Web Server
— CONTROL-M/Enterprise Manager Configuration Agent

■ Databases
CONTROL-M/Server processes

CONTROL-M/Server provides the following processes:

- ctmsrv_service (Windows only, where it runs as a service)
- p_ctmsu (Unix only)
- p_ctmrt
- p_ctmsl
- p_ctmtr
- p_ctmcd
- p_ctmcs
- p_ctmlg
- p_ctmwd
- p_ctmco
- p_ctmns
- p_ctmca (Unix only; Known as CONTROL-M/Server Configuration Agent)
- ctmsca_service (Windows only, where it runs as a service; Known as CONTROL-M/Server Configuration Agent)

CONTROL-M/Agent processes

CONTROL-M/Agent provides the following processes:

- p_ctmar
- p_ctmag (Known as CONTROL-M/Agent Listener, which on Windows runs as a service).
- p_ctmat (Known as CONTROL-M/Agent Tracker)
- ctmfw_service (Windows only, where it runs as a service; Known as CONTROL-M File Watcher)
- CONTROL-M/Agent (on Unix and Windows it runs as a service)
- CONTROL-M FileWatcher (Windows only, where it runs as a service)

Who is a CONTROL-M Administrator?

CONTROL-M administrators are responsible for defining and maintaining
CONTROL-M components, maintaining the CONTROL-M databases, implementing
CONTROL-M security, and various other administrator tasks.
The term **CONTROL-M administrator** can refer to anyone who has at least one of the following sets of credentials:

- accounts and passwords that allow you to log into CONTROL-M/EM with the permissions and privileges (defined in the Privileges tab) needed to manage CONTROL-M/EM, CONTROL-M/Server and CONTROL-M/Agent

- database owner credentials that allow you to log into the database and run utilities that update the database

- access (user name and password) to a CONTROL-M/Server account that allows you to change configuration files and start and stop processes

- access (user name and password) to a CONTROL-M/Agent account that allows you to change configuration files and start and stop processes

As a CONTROL-M administrator, your key responsibilities might be summarized as follows:

- defining CONTROL-M/Servers and their corresponding agents and remote hosts
- ensuring that CONTROL-M components are up, active, and connected
- maintaining security by setting and assigning user and group permissions
- ensuring that maintenance, job scheduling, and data backup are performed correctly

CONTROL-M administrators perform their administrative functions from any of several locations, depending on the function:

- Administrators perform many administrative functions for CONTROL-M/EM, CONTROL-M/Server, and CONTROL-M/Agent environments from the CONTROL-M Configuration Manager.

- To administer user permissions, CONTROL-M administrators use the CONTROL-M/EM GUI. This requires that they have high level (Update or Full) Authorizations privileges.

- To perform certain administrative functions in the CONTROL-M/Server environment, the administrator must log into the CONTROL-M/Server account.

- To perform certain administrative functions in the CONTROL-M/Agent environment, the administrator must log into the CONTROL-M/Agent account.
The discussions in this guide, especially in the chapters dealing with security, assume the following meanings for users, owners, and authors.

■ Users

Users are defined in CONTROL-M/EM. Each user is assigned a user account. Users are central to CONTROL-M/EM security. You define authentication criteria and permissions to ensure that only authenticated users gain access and perform allowable tasks.

■ Owners

Owners are credentials under which jobs will be executed. For operating system jobs, owners are accounts. For application jobs, owners are logical names that reference the credentials of the application account (for example, for SAP, it will reference user, password, host, port, and so on, for the SAP account).

Each job must be assigned an owner. The administrator determines which owners a particular user is allowed to assign to a job.

■ Authors

Author is an automatically-updated field in the job processing definition that identifies the user who last updated the job. Administrators can modify the value of this field.

Starting and stopping infrastructure processes

Infrastructure processes must be started before CONTROL-M can function.

**NOTE**

If the CONTROL-M/EM servers computer has multiple network cards, before you start CONTROL-M/EM processes (specifically, the Naming Service and the CONTROL-M Configuration Management Server) for the first time, modify CORBA configuration (set the publish address policy to a specific IP address or host name, instead of using the default IP address). For instructions, see “Specifying domain settings” on page 393.
Starting and stopping infrastructure processes in Windows

On Windows, all CONTROL-M/EM, CONTROL-M/Server, and CONTROL-M/Agent processes are defined as services. By default, they are automatically started when you bring Windows up, and they are automatically stopped when you bring Windows down.

Therefore, it is normally not necessary for you to perform startup or shutdown of these processes. However, you can bring these services down or up whenever useful.

To stop CONTROL-M/EM, CONTROL-M/Server, or CONTROL-M/Agent services in Windows

2. Right click the service, and choose Stop.

To start CONTROL-M/EM, CONTROL-M/Server, or CONTROL-M/Agent services in Windows

2. Right click the service, and choose Start.

Starting and stopping infrastructure processes in UNIX and Linux

In Unix and Linux, you must start processes after their host computer is booted up, and you must stop them before shutting down the host computer. Although you can do this manually, you can instead add process startup or shutdown commands to the operating system startup and shutdown scripts of the host computer.

Starting and stopping of CONTROL-M/Agent infrastructure components separate from starting and stopping CONTROL-M/Agent itself is unnecessary. For instructions of starting and stopping CONTROL-M/Agent, see page 269.

You can start and stop CONTROL-M/EM infrastructure processes using either of the following methods:

- Using scripts to start and stop CONTROL-M/EM infrastructure processes (recommended)
- Manually starting and stopping CONTROL-M/EM infrastructure processes using the interactive Activation menu
Using scripts to start and stop CONTROL-M/EM infrastructure processes

It is the administrator’s responsibility to update the operating system startup and shutdown scripts with the parameters that are described in this section.

--- NOTE ---

If not all CONTROL-M/EM server components are installed on one account (that is, you have distributed your CONTROL-M/EM components), you need to include the startup and shutdown commands in operating system startup and shutdown scripts of the host computer.

To start processes on Unix and Linux

Add the following commands to the start-up script of your operating system as appropriate:

```
su - ecs_account -c start_ns_daemon
su - ecs_account -c start_server
su - ecs_account -c start_cms
su - ecs_account -c start_config_agent
su - ecs_account -c start_web_server.sh
```

To stop processes on Unix and Linux

Add the following commands to the shut-down script of your operating system as appropriate:

```
esc_ctl -U CONTROL-M/EM_database_owner -P CONTROL-M/EM_database_owner_password -C Maint_Agent -M hostname -cmd shutdown
su - ecs_account -c "stop_server -U db_server_administrator_name -P db_server_administrator_name"

su - ecs_account -c stop_ns_daemon
su - ecs_account -c stop_cms
su - ecs_account -c stop_config_agent
su - ecs_account -c stop_web_server.sh
```

Manually starting and stopping CONTROL-M/EM infrastructure processes using the interactive Activation menu

1 Display the CONTROL-M/EM Root Menu (root_menu). For instructions on displaying the Root menu, see “Using the CONTROL-M/EM Root Menu” on page 46.
2 In the CONTROL-M/EM Root menu, enter the number for the Activation Menu option.

3 In the Activation menu, enter the number of the appropriate start or stop process option (or start all or stop all option).

4 Enter q to exit.

The installation procedure for CONTROL-M/Server includes directions for adding startup and shutdown commands for the SQL Database Server, CONTROL-M/Server, and CONTROL-M/Server Configuration Agent to the boot procedure and shutdown procedure of the server computer.

You can manually shutdown and startup infrastructure components using the following methods:

- CONTROL-M Configuration Manager (to shut down CONTROL-M/Server)
- CONTROL-M Manager Menu, which you access from the CONTROL-M Main Menu (ctm_menu)
- supplied utilities

**Using CONTROL-M Configuration Manager to shut down or start up CONTROL-M/Server**

1 In the CONTROL-M Configuration Manager, right-click the CONTROL-M/Server.

2 Choose Desired State and then choose one of the following submenu options:
   - Up—bring the component up
   - Down—bring the component down

**Using CONTROL-M Manager Menu to shut down or start up CONTROL-M/Server infrastructure components**

1 Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number of the CONTROL-M Manager option.

3 In the CONTROL-M Manager menu, enter the number corresponding to the component activity you want to perform.

4 When done, enter q.
Using pre-supplied utilities to shut down or start up CONTROL-M/Server infrastructure components

To shut down CONTROL-M/Server entities

1 Log on as the CONTROL-M/Server account owner.

2 Enter one of the following commands as appropriate:
   - To stop the SQL database server, specify the command: **shutdb**
   - To stop the CONTROL-M/Server Configuration Agent: **shut_ca**
   - To stop the CONTROL-M/Server, specify the command: **shut_ctm**

To start CONTROL-M/Server entities

1 Log on as the CONTROL-M/Server account owner.

2 Enter one of the following commands as appropriate:
   - To start the SQL server, specify the command: **startdb**
   - To start the CONTROL-M/Server Configuration Agent: **start_ca**
   - To start the CONTROL-M/Server, specify the command: **start_ctm**

Using CONTROL-M Configuration Manager

For basic instructions about using the CONTROL-M Configuration Manager, see the following sections.

Starting CONTROL-M Configuration Manager

1 Choose Start => Programs => CONTROL-M Enterprise Manager => CONTROL-M Configuration Manager (or click the icon on your desktop).

2 Enter your user name and password, and click Login.

3 If change password fields are displayed, your password is soon due to expire. Fill in your new password, and then confirm it.

The CONTROL-M Configuration Manager (Figure 3 on page 40) is displayed.
Understanding the display

Each type of component the CONTROL-M Configuration Manager displays is represented by a different icon. The following table describes the icons used to identify the different component types.

The CONTROL-M Configuration Manager windows contain the following sections:

- **navigation tree pane** — lists components hierarchically. You can expand or collapse the hierarchies. By clicking on different components in the tree, you can determine which components are displayed in the detail pane.

- **detail pane** — displays the important information about each displayed component. By right-clicking a particular component, you can display additional information about the component or perform various actions on the component.

You can drag the headings and columns. You can also customize the console (for more information, see “Setting your CONTROL-M Configuration Manager preferences” on page 44).

### Understanding the display

Each type of component the CONTROL-M Configuration Manager displays is represented by a different icon. The following table describes the icons used to identify the different component types.
You should be aware of the following points about various components:

- Each gateway appears as both a CONTROL-M/EM component and a CONTROL-M/Server component.
  
  — The Gateway appears as a CONTROL-M/EM component because gateways are resident on the CONTROL-M/EM computer and are under the control of CONTROL-M/EM. Each gateway provides CONTROL-M/EM with an interface to a CONTROL-M/Server.
  
  — The Gateway appears as a CONTROL-M/Server component because each CONTROL-M/Server has a gateway dedicated to it, and this gateway is created when you define the CONTROL-M/Server.

- The Configuration Manager Server (CMS, a CONTROL-M/EM component) does not appear because it is the mechanism behind the CONTROL-M Configuration Manager, and its display is unnecessary:
  
  — If you can display and use the CONTROL-M Configuration Manager, it means that the Configuration Manager Server is up and working.
  
  — If the Configuration Manager Server is not up and working, you cannot display and use the CONTROL-M Configuration Manager.

---

**Table 1   Component icons**

<table>
<thead>
<tr>
<th>Symbol</th>
<th>CONTROL-M/EM components</th>
<th>Symbol</th>
<th>CONTROL-M/Server components</th>
</tr>
</thead>
<tbody>
<tr>
<td>🚨</td>
<td>Global Alerts Server (GAS)</td>
<td>📣</td>
<td>CONTROL-M/Server</td>
</tr>
<tr>
<td>🌐</td>
<td>Gateway (also appears as a CONTROL-M/Server component)</td>
<td>🌏</td>
<td>(Gateway—although this is a CONTROL-M/EM component, a different gateway is defined for each CONTROL-M/Server)</td>
</tr>
<tr>
<td>🌟</td>
<td>Global Conditions Server (GCS)</td>
<td>🌟</td>
<td>CONTROL-M/Agent</td>
</tr>
<tr>
<td>🌐</td>
<td>GUI Server</td>
<td>🌐</td>
<td>Remote host</td>
</tr>
</tbody>
</table>

---

You should be aware of the following points about various components:

- Each gateway appears as both a CONTROL-M/EM component and a CONTROL-M/Server component.
  
  — The Gateway appears as a CONTROL-M/EM component because gateways are resident on the CONTROL-M/EM computer and are under the control of CONTROL-M/EM. Each gateway provides CONTROL-M/EM with an interface to a CONTROL-M/Server.
  
  — The Gateway appears as a CONTROL-M/Server component because each CONTROL-M/Server has a gateway dedicated to it, and this gateway is created when you define the CONTROL-M/Server.

- The Configuration Manager Server (CMS, a CONTROL-M/EM component) does not appear because it is the mechanism behind the CONTROL-M Configuration Manager, and its display is unnecessary:
  
  — If you can display and use the CONTROL-M Configuration Manager, it means that the Configuration Manager Server is up and working.
  
  — If the Configuration Manager Server is not up and working, you cannot display and use the CONTROL-M Configuration Manager.
CONTROL-M/Servers and the CONTROL-M Configuration Manager communicate with each other through the Configuration Agent on the Server side, and the Configuration Manager on the CONTROL-M/EM side. (When it comes to job definition and processing, CONTROL-M/Server and CONTROL-M/EM communicate with each other through the gateway.)

**Adjusting the display**

You can adjust the CONTROL-M Configuration Manager display in many ways. The following are some of the more common adjustments:

- Arranging the tree view hierarchy by component or computer
  
  In the View menu, choose By Computer or By Component to rearrange the tree view hierarchy.

- Moving the tree pane to another point on the screen
  
  The tree pane is dockable.
  
  — Click in the title bar and drag to the desired location.
  
  — To help you position the pane, while dragging the pane, move your cursor over one of the positioning arrows that appears on the page. The area where the pane will be positioned when you release the mouse is highlighted.

- Grouping components in the detail pane by column values
  
  You can perform nested grouping of components (for example, you can group components by desired state, and within desired state you can group them by host)
  
  — For each required grouping (beginning from the outer level and moving in), right click on the column name (for example, State) and choose Group By This Column.
  
  The components are grouped as requested. A chart of the nested group levels appears at the top of the detail pane.
  
  — To eliminate a grouping from the nest, right click the group in the chart and choose Ungroup.
Filtering the display

You can define filters of varying complexity.

1  Choose View => Component Filter to display a filtering row at the top of the detail pane.

2  To perform the simplest filtering on any column
   A  Position the cursor in the upper right corner of the column and then click the displayed icon
   B  In the displayed menu, choose the value for filtering.

3  To filtering on a set or range of values for a column
   A  Position the cursor in the upper right corner of the column and then click the displayed icon
   B  In the displayed menu, choose (Custom).
   C  Fill in the Custom AutoFilter by specifying two sets of logical operators and values separated by the appropriate relationship (button). Click OK.

4  To perform complex filtering by defining sets of filtering criteria for a column
   A  Click Edit Filter in the right corner of the Status bar at the bottom of the window.
   B  Fill in the Filter Builder dialog box using the following guidelines:
      ■  Click keywords (for example, And, Type, and begins with) to display valid keywords, and make the appropriate selections.
      ■  To add an additional criterion to a set of criteria, click the icon by the relationship (And or Or) value.
      ■  To add an additional set of criteria, click the relationship (And or Or) value, and choose Add Group.
      ■  To delete a criterion, click .
   C  Click OK.
Viewing a component’s properties

To view a component’s properties, select the component in the detail pane and click .

Changing your password

When your password is soon due to expire, the login dialog box of the CONTROL-M windows (CONTROL-M/Desktop, CONTROL-M/EM, CONTROL-M Reporting Facility, and CONTROL-M Configuration Manager) will display fields that enable you to change your password.

To change your password at any other time, you must issue the request through the CONTROL-M/EM or CONTROL-M/Desktop windows.

Password changes made in one application window (for example CONTROL-M/EM) automatically apply to the other application windows.

To change your password

1 If the change password fields are not already displayed, in the CONTROL-M/EM or CONTROL-M/Desktop window, choose Tools => Change Password.

2 Fill in your current and new passwords, and then confirm the new password.

3 Click OK.

NOTE
Alternatively, you can change passwords using the User Authorizations window, but this is generally not recommended unless you are changing other password criteria, or changing the passwords for other users. For more information, see “Manually modifying a user’s password criteria” on page 169.

Setting your CONTROL-M Configuration Manager preferences

You can set certain viewing preferences for the CONTROL-M Configuration Manager displays.

1 In the CONTROL-M Configuration Manager, choose Tools => Options to display the Options dialog box.
2 In the General panel, set your preferences for the available options. When setting options, consider the following:

- Enabled components are displayed regardless of your preferences. To display disabled CONTROL-M/Server components along with the enabled components, select the Show CONTROL-M/Server components check box.

- Long date format displays the month name in the date instead of using a numeric date format, and displays the time.

3 In the Confirmation panel, select or deselect the confirmations that CONTROL-M Configuration Manager should display. To reassign the originally provided default settings, click Restore Defaults.

4 Click OK.

Using interactive menus

CONTROL-M provides several interactive menus that are used for performing a number of functions.

- CONTROL-M/EM Root Menu (root_menu)—provides access to a variety of functions and utilities that are used to maintain CONTROL-M/EM.
- CONTROL-M Main Menu (ctm_menu)—provides access to a variety of functions and utilities that are used to maintain CONTROL-M/Server.

- CONTROL-M System Maintenance Utility Main Menu (ctmsys)—allows you to define many CONTROL-M system parameters and maintain Shout Destination tables (for directing Shout messages).

Many of the tasks described throughout the chapters of this book are performed from these menus. This chapter provides instructions for accessing these menus, so that the instructions do not need to be repeated for each task.

Using the CONTROL-M/EM Root Menu

**NOTE**
The database server must be running for the Root Menu and its submenus to be displayed.

1. Log on to the CONTROL-M/EM host computer.

2. Enter the `root_menu` command.

3. When prompted, enter the CONTROL-M/EM DBO user name and password.

   The CONTROL-M/EM Root Menu is displayed.

**Figure 5  CONTROL_M/EM Root Menu**

```
CONTROL-M/EM Root Menu
-----------------------------------------------
Select one of the following options:
1 - Activation Menu
2 - Troubleshooting Menu
3 - New Window
4 - Clean Database Schema
5 - Database Maintenance
6 - Users Administration Menu
q - Quits
```

4. To use the Root Menu and its submenus
   
   **A** Enter the number of the menu option.

   **B** Make the required changes.

   **C** When you are done, enter `q` to quit.
Using the CONTROL-M/Server Main Menu

1. Log on to the CONTROL-M/Server computer as the CONTROL-M/Server owner.

2. Enter the `ctm_menu` command to display the CONTROL-M Main Menu.

3. To use CONTROL-M Main Menu and its submenus
   
   A. Enter the number of the menu option.
   
   B. Make the required changes.
   
   C. When you are done, enter `q` to quit.

Using the CONTROL-M System Maintenance Utility Main Menu

1. Log on to the server computer as the CONTROL-M/Server owner (for example, user `controlm`).

2. Do either of the following:
   
   - Enter the `ctmsys` command to display the CONTROL-M System Maintenance Utility Main Menu directly
■ Enter the ctm_menu command to display the CONTROL-M Main Menu, and then

— Enter the number of the Parameter Customization option to display the Parameter Customization menu.

— Enter the number of the System Parameters and Shout Destination Tables option to display the CONTROL-M System Maintenance Utility Main Menu.

Figure 7  CONTROL-M System Maintenance Utility Main Menu

| CONTROL-M SYSTEM MAINTENANCE UTILITY |
| Main Menu |
| 1) Shout Destination Tables |
| 2) System Parameters |
| q) Quit |

Enter option:

3 To use the CONTROL-M System Maintenance Utility Main Menu its submenus

A  Enter the number of the menu option.

B  Make the required changes.

C  When you are done, enter q to quit.
Connecting components

This chapter presents the following topics:

- Conceptual overview ......................................................... 50
  - CONTROL-M/Server definition and management .................. 51
  - CONTROL-M/Agents and remote hosts ............................... 52
  - CONTROL-M/EM Web Launch ........................................... 52
- Recommended task summary ............................................. 54
- Defining CONTROL-M/EM components ................................. 54
  - Defining a new CONTROL-M/EM component .......................... 54
  - Updating a previously defined component .......................... 56
- Defining a CONTROL-M/Server and its Gateway ....................... 56
  - Defining a CONTROL-M/Server (automatic discovery method) .... 57
  - Defining a CONTROL-M/Server (manual definition method) ........ 57
- Defining CONTROL-M/Agents and remote hosts ....................... 61
  - Planning your strategy ................................................ 61
  - Defining a CONTROL-M/Agent ....................................... 64
  - Using multiple agents on the same computer ....................... 65
  - Associating more than one CONTROL-M/Agent on the same host to the same CONTROL-M/Server .................. 66
- Converting a remote host to a CONTROL-M/Agent .................... 67
- Configuring and managing remote hosts .............................. 68
- Testing communication channels ...................................... 71
- Using Web Launch ......................................................... 72
  - Generating a Web Launch package ................................ 72
  - Deploying new packages ............................................ 76
Figure 8 highlights the basic recommended workflow for connecting CONTROL-M components. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 2 on page 54. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

Figure 8  Recommended workflow for connecting CONTROL-M components
CONTROL-M/Server definition and management

Several terms describe the definition and management of a CONTROL-M/Server:

■ Discovery/Define

When defining CONTROL-M/Servers and their gateways (which you do using the CONTROL-M/Server Definition dialog box), you can choose either of the following definition methods:

— Automatic discovery—provides automatic detection of a CONTROL-M/Server and gateway, with minimal information supplied. (This option is available in CONTROL-M/Server version 6.3.01 and later.)

— Manual definition—you manually define a CONTROL-M/Server and corresponding Gateway.

■ Managed / Unmanaged — Managed and Unmanaged are modes of connection between CONTROL-M/EM and CONTROL-M/Server.

— If a CONTROL-M/Server is Managed, the Configuration Agent automatically provides CONTROL-M/EM parameter information about the CONTROL-M/Server, and on an ongoing basis updates that information whenever there is a change.

— If a CONTROL-M/Server is unmanaged, you must manually provide CONTROL-M/EM with the CONTROL-M/Server parameters.

CONTROL-M/EM automatically manages CONTROL-M/Server version 6.3.01 and later, and CONTROL-M for z/OS versions 6.2.A and later. Furthermore, you must manually manage CONTROL-M/Server versions earlier than 6.3.01 and CONTROL-M for z/OS versions prior to 6.2.A.

In certain circumstances, you can choose to bypass automatic management of CONTROL-M/Server versions 6.3.01 and later, and manually manage those versions, though this is generally not recommended.

When you use Discovery to define CONTROL-M/Servers, they are automatically Managed; when you manually define CONTROL-M/Servers, they are Unmanaged.

Using the CONTROL-M Configuration Manager, you can change the connection mode (managed/unmanaged) of existing CONTROL-M/Servers. For more information, see “Setting whether a CONTROL-M/Server is managed or unmanaged from CONTROL-M/EM” on page 274.
CONTROL-M/Agents and remote hosts

In earlier releases of CONTROL-M/Server, each computer on which you planned to run jobs required installation of a CONTROL-M/Agent. Beginning with version 6.3.01, CONTROL-M/Server supports agentless job submission. This method enables submitting and executing jobs on computers that do not have a resident CONTROL-M/Agent installed. These agentless computers are referred to as remote hosts.

Although remote host computers do not require a resident CONTROL-M/Agent, remote hosts come under the control of CONTROL-M/Agents on other computers, as follows:

- When you install CONTROL-M/Server in UNIX, a CONTROL-M/Agent is automatically installed on the same account. When you install CONTROL-M/Server in Windows, a CONTROL-M/Agent is automatically installed on the same computer, unless one already exists or you are performing a cluster install. This automatically installed CONTROL-M/Agent is known as the <Local> agent and is, by default, the agent that is used to connect to remote hosts.

- You can place remote hosts under the control of any other CONTROL-M/Agents installed on computers under the same CONTROL-M/Server.

You will need to define the following information for each remote host:

- **host communication settings**

  You can define specific settings for a host, or use the default settings. For more information, see “Configuring and managing remote hosts” on page 68.

- **owner authentication settings**

  These settings specify the owners of the jobs that are running on the remote host, and owner authentication parameters that are used for connecting to the remote host. In a CONTROL-M job that is destined to be run on a remote host, you must define each job owner that is specified.

CONTROL-M/EM Web Launch

CONTROL-M/EM Web Launch (abbreviated Web Launch) is a powerful tool for deploying CONTROL-M/EM client components.
Rather than requiring individual installation of CONTROL-M/EM client components on each computer, as was necessary prior to this feature, Web Launch enables the administrator to install a single client and use that client as a model to generate a common client package called a Web Launch package. Users can then deploy the Web Launch package to install their client components.

Using a Web Launch package, the administrator can easily do the following from a single point:

- deploy CONTROL-M/EM client components
- propagate user templates and application forms
- apply fix pack and patch binaries
- manage TAO and SSL configurations

**NOTE**
When you use Web Launch for client deployment, CONTROL-M/Desktop, the CONTROL-M/EM GUI, and CONTROL-M Configuration Manager are the only client applications included in the deployment. The following client components do not get included in the Web Launch package, and cannot be manually deployed or used:

- XML and cli utilities
- Reporting facility

Deployed Web Launch packages can exist side-by-side with other Web Launch packages and with other regular CONTROL-M/EM installations. If a Web Launch package is deployed on a computer where a client already exists, the Web Launch package installs a new client; it does not upgrade the existing client. If desired, however, you can remove the old client.

CONTROL-M/EM Web Launch requires a web server. A dedicated web server, called CONTROL-M Web Server, is bundled with CONTROL-M/EM Web Launch and is installed on the computer hosting the CONTROL-M/EM server components. You can use this or any other web server.

**NOTE**
If you will be using CONTROL-M Web Server, and the computer on which it is resident contains multiple versions of Java, you must specify the location of the correct Java version (1.5) in the environment variable called JAVA_HOME. For more information, see the relevant Release Notes.

The first time that users deploy a package, they must access the package from a URL generated with the package. From that time on, any updates will automatically be deployed when the users start CONTROL-M/EM, CONTROL-M/Desktop, or CONTROL-M Configuration Manager.
Recommended task summary

Table 2 lists specific tasks related to each phase of the workflow (Figure 8 on page 50). Subsequent sections provide step-by-step instructions.

Table 2  Task summary: connecting components

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Define CONTROL-M/EM components</td>
<td>Defining a new CONTROL-M/EM component</td>
<td>54</td>
</tr>
<tr>
<td></td>
<td>Updating a previously defined component</td>
<td>56</td>
</tr>
<tr>
<td>Define a CONTROL-M/Server and its Gatewaya</td>
<td>Defining a CONTROL-M/Server (automatic discovery method)</td>
<td>57</td>
</tr>
<tr>
<td></td>
<td>Defining a CONTROL-M/Server (manual definition method)</td>
<td>57</td>
</tr>
<tr>
<td>Define CONTROL-M/Agents and remote hosts</td>
<td>Planning your strategy</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Deciding whether to define remote hosts</td>
<td>61</td>
</tr>
<tr>
<td></td>
<td>Choosing a connection method for a remote host</td>
<td>62</td>
</tr>
<tr>
<td></td>
<td>Defining a CONTROL-M/Agent</td>
<td>64</td>
</tr>
<tr>
<td></td>
<td>Associating more than one CONTROL-M/Agent on the same host to the same CONTROL-M/Server</td>
<td>66</td>
</tr>
<tr>
<td></td>
<td>Converting a remote host to a CONTROL-M/Agent</td>
<td>67</td>
</tr>
<tr>
<td></td>
<td>(optional) Configuring and managing remote hosts</td>
<td>68</td>
</tr>
<tr>
<td>Use Web Launch to prepare and deploy CONTROL-M/EM client components (optional)</td>
<td>Generating a Web Launch package</td>
<td>72</td>
</tr>
<tr>
<td></td>
<td>Deploying new packages</td>
<td>76</td>
</tr>
</tbody>
</table>

a  CONTROL-M/Server can be defined either automatically (using the discovery method), or manually.

Defining CONTROL-M/EM components

This section explains how to define a new CONTROL-M/EM component and how to update component properties.

Defining a new CONTROL-M/EM component

1 In the CONTROL-M Configuration Manager, choose Components => New => CONTROL-M/EM Component.

2 Fill in the CONTROL-M/EM Component dialog box:
A At Desired State, select one of the following states:

- **Up** if you want the component to be started
- **Down** if you do not want the CONTROL-M Configuration Manager to start the component.
- **Ignored**

B At **Type**, select the type of component that you want to add. Valid values are:

- BIM (Batch Impact Manager server)
- GAS (Global Alerts server)
- GCS (Global Conditions server)
- GUI_Server
- Forecast_Server

C Enter the name of the component.

Optional for the GAS and GUI servers, and not relevant for the GCS server. When defining a BIM or Forecast_Server component, you must enter the name of the GUI server with which the component will communicate.

Observe the following guidelines when choosing a name for a new server:

- You can define multiple GUI servers and multiple GAS servers to run simultaneously. (These capabilities allow you to balance job loads as needed in your environment.) These servers can run on the same account or on different hosts. Each instance of a GUI server (or GAS server) must have a unique name. The GUI Server name and the GAS server name are used to reference both components when using the CONTROL-M/EM client components.

- You can specify any logical name for an instance of either component. For example, you can enter the virtual host name of a cluster computer in which the GUI Server (or Global Alerts Server) is installed, without specifying the node on which the component is installed.

- By default, the GUI Server is named according to its host name. Thus, if more than one GUI Server exists on the same host, each instance must have a unique name.

3 Complete the **Running on** box:

A At **Platform**, select the operating system for the host computer on which the component runs.

B At **Host Name**, enter the name of the host computer.
Updating a previously defined component

4 At **Check Interval**, enter how frequently, in number of seconds, you want to check the component’s state.

5 *(optional)* In the **Startup** box, indicate the mode in which the component should start:

- To use a startup command other than the default, select the **Override Manually** check box and enter a command in the **Command** box.

- If you want to use optional arguments for the startup command, enter them in the **Additional Parameters** box.

**Updating a previously defined component**

1 In the Component window of the Configuration Manager, right-click the component and select **Properties**.

2 Modify the values as needed, and click **OK**.

**Defining a CONTROL-M/Server and its Gateway**

CONTROL-M refers to an instance of CONTROL-M/Server and its corresponding Gateway.

When adding a new CONTROL-M/Server and its Gateway, you can use automatic discovery or manual definition:

- Automatic discovery bases the new server on an existing CONTROL-M, retrieving the parameter values and requiring minimal information from you. For instructions, see page 57.

- Manual definition requires that you supply all parameter values. For instructions, see page 57.
Defining a CONTROL-M/Server (*automatic discovery method*)

1 In the CONTROL-M Configuration Manager, choose **Components => New => CONTROL-M/Server and Gateway.**

2 In the CONTROL-M/Server Definition dialog box, choose **Discover.**

3 In the wizard, specify the CONTROL-M/Server connection parameters:
   - At **CONTROL-M Name**, enter the logical name of the required CONTROL-M.
   - At **CONTROL-M ID**, accept the default unique code or enter a unique 3-digit code identifying the CONTROL-M/Server.
   - At **CONTROL-M Host**, enter the name of the host computer on which the CONTROL-M is installed.
   - At **Configuration Agent Port**, enter the port number of the CONTROL-M’s Configuration Agent.
   - Click **Next.**

   The discovery process begins. CONTROL-M automatically retrieves parameters and shows how the discovery is progressing.

4 When the Step 3 wizard panel is displayed, ensure that **Activate Gateway** is selected.

5 Review the list of retrieved parameters, and click **Finish.**

   The new CONTROL-M is displayed in the CONTROL-M Configuration Manager after a short period of time.

---

Defining a CONTROL-M/Server (*manual definition method*)

1 Perform one of the following in the CONTROL-M Configuration Manager:
   - To modify the definition of an existing CONTROL-M/Server, right click the server, and choose **Properties.**
To define a new CONTROL-M/Server

— Choose Components => New => CONTROL-M/Server and Gateway.

— In the prompt, choose Define to display the CONTROL-M Definition dialog box.

Table 3  CONTROL-M Definition dialog box

2 Fill in the CONTROL-M Definition dialog box. Table 4 describes the essential parameter values that you need to provide.
### Defining a CONTROL-M/Server (manual definition method)

**Chapter 2 Connecting components  59**

3. If you are defining a new CONTROL-M/Server, under **Gateway**, click **New**. You must specify a Gateway when you set up your work environment. Otherwise, you can define a new gateway, or modify or delete an existing gateway.

   The CONTROL-M/EM Component dialog box is displayed.

4. Specify the required parameters.

### Table 4  Parameters for manually defining a CONTROL-M/Server and its Gateway

<table>
<thead>
<tr>
<th>Parameter field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Name**        | descriptive name for the CONTROL-M/Server  
You should choose a name that is meaningful enough to identify your CONTROL-M. For example, if the CONTROL-M handles workloads for Division 7, which is associated with the company’s headquarters in Paris, you might use **HQ_PARIS_DIVISION-07**.  
The name can be a maximum of 20 alphanumeric characters long. You can include symbols, but do not use blank spaces. |
| **ID**          | unique 3-character code (such as 999 or NYC) that CONTROL-M/EM uses to identify each CONTROL-M/Server  
The code must be unique. It can consist of numerals and uppercase letters. |
| **Platform**    | operating system on which your CONTROL-M is installed. Note the following:  
|■ If your platform is UNIX, Windows, TANDEM, or not listed, choose **Distributed**.  
■ If your CONTROL-M runs on iSeries (AS/400) but any of the connecting CONTROL-M/Agents run on non-iSeries operating systems, choose **Distributed**. |
| **Version**     | version number of the CONTROL-M/Server  
**Note**: When defining an iSeries (AS/400) CONTROL-M, choose **225**. |
| **Time Zone**   | time zone in which the CONTROL-M is located |
| **Start day**   | day that CONTROL-M/Server should consider to be the first day of the week |
| **New Day Time**| the time that each new day should begin for the CONTROL-M/Server |
| **Communication Protocol** | type of protocol for communication with CONTROL-M |
| **Communication Host** | host name of the CONTROL-M |
| **Communication CONTROL-M/EM Port** | TCP/IP port for communicating with CONTROL-M/EM  
For specific instructions pertaining to CONTROL-M installations on z/OS, see the **INCONTROL for z/OS Installation Guide**. |
A  At **Desired State**, select one of the following states:

- **Up** if you want the gateway to be started
- **Down** if you do not want the CONTROL-M Configuration Manager to start the gateway.
- **Ignored**

B  Enter the name of the gateway. You can define multiple gateways for a CONTROL-M/Server, but only one CONTROL-M can be up (started) at one time. Additionally, each Gateway should be located on a separate computer.

C  In the **Platform** field, select the operating system for the host computer on which the component runs.

D  In the **Host Name**, enter the name of the host computer.

E  In the **Check Interval** field, enter how frequently, in seconds, to check the gateway’s state.

F  *(optional)* In the **Startup** box, indicate the mode in which the gateway should start:

- To use a startup command other than the default, select the **Override Manually** check box and enter a command in the **Command** box.
- You want enter optional arguments for the startup command in the **Additional Parameters** box.

G  Click **OK** to save the changes you made in the CONTROL-M/EM Component dialog box.

5  Click **OK** in the CONTROL-M Definition dialog box to save your CONTROL-M/Server definition.
Defining CONTROL-M/Agents and remote hosts

This section explains how to add a new agent to an existing CONTROL-M, and if and how to configure and manage remote hosts.

Planning your strategy

Completing this section can help you expedite the remaining tasks in this chapter. This section summarizes prerequisites that you should know about before connecting components. The provided worksheets also help you gather data that you will need to provide for tasks in this chapter.

Before proceeding, ensure that you comply with the following requirements and guidelines.

Deciding whether to define remote hosts

Both CONTROL-M/Agents and remote hosts have distinct advantages. Consider the following before deciding which method to use on a particular computer:

- The main advantage of remote hosts over CONTROL-M/Agents is that remote hosts:
  - Can run all jobs assigned to the specific node ID which identifies the remote computer
  - Do not require CONTROL-M/Agent installation on the remote computer
  - Do not require version updates
  - Require less management

- The main advantages of CONTROL-M/Agents over remote hosts are that agents support counters and multiple types of shouts:
  - CONTROL-M/Agents can utilize features that require a CONTROL-M counter. If you need any of these features, you should choose a CONTROL-M/Agent over a remote host. For example, CONTROL-M/Agents can use the File Watching feature, run jobs using CONTROL-M/Agent utilities, and run jobs requiring Control Modules (plug-ins for the CONTROL-M/Agent).
  - CONTROL-M/Agents support many types of shouts. (Remote host support is limited to e-mail shouts and CONTROL-M/Server shouts.)
To use remote hosts, the CONTROL-M/Server must be in Managed state:

— If you discover the CONTROL-M, its default state is Managed.

— If you define the CONTROL-M, the default state is Unmanaged, and you must change it to Managed via the CONTROL-M Configuration Manager.

For more information, see “Defining a CONTROL-M/Server and its Gateway” on page 56 and “Managing CONTROL-M/Servers” on page 274.

**Choosing a connection method for a remote host**

To enable communication between the remote host and a CONTROL-M/Agent. You can use either of the following connection methods, which are available with the operating system:

**Secured Shell (SSH)**

You can use SSH connections for remote hosts running UNIX, Windows, OpenVMS, Z/OS USS (OpenEdition) and PASE (AIX environment) on AS/400:

— Most UNIX operating system packages include SSH.

— To use SSH on Windows computers, you must purchase and install it separately.

— SSH functionality on OpenVMS is available as part of TCP/IP Services Version 5.4 and higher. For older versions of OpenVMS, you must install it separately. Third party packages are also available.

— To use SSH on AS/400 computers, you must install PASE on AS/400.

**NOTE**

When you work with z/OS USS (OpenEdition) or PASE AS/400 remote hosts, set the **RJX_CONN_MODE** system parameter in CONTROL-M/Agent to 0.

If you will be using more simultaneous connections than your current SSH server settings allow, you must increase the value for these settings accordingly.

**EXAMPLE**

For an OpenSSH server, set the MaxStartups and LoginGraceTime parameters in the **sshd_config** file.

For more information, refer to your SSH server documentation.
Planning your strategy

Window Management Instrumentation (WMI)

You can use WMI connections with remote hosts running Windows 2003, Windows XP, or a later version. WMI is part of the Windows operating system.

NOTE

If the CONTROL-M/Agent will be connecting to a remote host on Windows by using the WMI connection method, ensure that the following requirements are satisfied:

- The CONTROL-M/Agent is installed on either Windows 2003, Windows XP, or a later version.
- The Log On as option for the CONTROL-M/Agent service is set to This account.
- The user account that is running the CONTROL-M/Agent service is Administrator and is defined as a Domain user.
- Job owners are members of the Administrator group on the remote host.

Consider the following requirements when deciding which connection method to use for remote hosts:

- For Window Management Instrumentation (WMI) connections, the following requirements apply:

  — To use On statements and the View JCL, Edit JCL, and View Sysout options, you must define a directory named SYSOUT on the remote host. This directory must be writable by all the job owners on that host. This directory must also be shared so that the CONTROL-M/Agent user can access it for reading and writing. When defining the properties of a remote host, specify the full local path (for example, C:\shared documents\SYSOUT) of this directory so that the job output will be written to it.

  — SYSOUTs created on remote hosts must be copied to a CONTROL-M/Agent. If a SYSOUT is large, its file transfer can place a heavy load on system resources. Also, a job will not end until its SYSOUT copying is finished.

- For Secured Shell (SSH) connections, you must ensure that an SSH Server is installed and running on each remote host.
Defining a CONTROL-M/Agent

This procedure describes how you can add a CONTROL-M/Agent to an existing CONTROL-M/Server, or modify an existing CONTROL-M/Agent.

**NOTE**

A CONTROL-M/Agent should be installed first before it is defined. For information about installing CONTROL-M/Agents, see the CONTROL-M Installation Guide.

1. From the CONTROL-M Configuration Manager, perform one of the following:

   - To modify the parameters of an existing CONTROL-M/Agent, right click the agent and choose **Properties**.
     
     The CONTROL-M/Agent Properties dialog box is displayed.
     
     - To add a new CONTROL-M/Agent to a CONTROL-M/Server, right click the CONTROL-M/Server and choose **New CONTROL-M/Agent**.
       
       The Add CONTROL-M/Agent dialog box is displayed. Fill in the name for the agent. Click **Advanced**.

   ![Figure 9 CONTROL-M/Agent Properties dialog box](image)

2. In the appropriate dialog box, fill in the fields in the General, Persistent Connection and Retry/Timeout tabs.

   If communication between CONTROL-M/Server and CONTROL-M/Agent will pass through a firewall, it is important that you define a persistent connection. (For conceptual information about Persistent connections, see “Persistent connection model” on page 221. For the instructions required for establishing persistent connections, see “Enabling communication between agents and CONTROL-M/Server”.)
Using multiple agents on the same computer

3 Click **Test** to check that your settings are correct and workable.

4 Once the test has validated the settings, click **OK**.

### Using multiple agents on the same computer

You can install more than one CONTROL-M/Agent on the same computer. Considerations for this type of configuration are discussed below.

- **Why use multiple Agents?**

  With multiple agents, more than one CONTROL-M/Server can request jobs on the same computer. In this type of configuration, each CONTROL-M/Agent is associated with a different CONTROL-M/Server.

- **Port numbers**

  Each agent must use a different Server-to-Agent port number. During installation, it is important to record the port that you specified for each agent. You will need this port number when you define the communication for that agent in CONTROL-M/Server.

- **Agent names**

  Each CONTROL-M/Agent is identified by a logical name. This name is used in the command line for CONTROL-M/Agent utilities to indicate which agent should handle the command.

  The default agent is always named Default.

- **Default Agent**

  During installation a checkbox in the Agent Name window enables you to specify if you are installing the Default agent. If no specific agent name is specified in a CONTROL-M/Agent utility command, the Default agent handles the commands.

  All CONTROL-M Control Modules work with the default agent. Some CONTROL-M Control Modules work with non-default agents.
Associating more than one CONTROL-M/Agent on the same host to the same CONTROL-M/Server

You can associate more than one CONTROL-M/Agent on the same host to the same CONTROL-M/Server.

1 For each additional agent you are connecting, repeat the steps in “Defining a CONTROL-M/Agent” on page 64, but ensure that you provide each agent with a different logical host name and server-to-agent port number.

2 Configure the CONTROL-M/Server to recognized the different host names, as follows:

   A Log on to the CONTROL-M/Server computer as root (UNIX) or administrator (Windows).

   B Open the hosts file located in the etc directory and add the following line:

       <IP address of the Agent computer> <logical name>

3 For each additional agent, change the value of the Logical Agent name system parameter. You can do this using CONTROL-M Configuration Manager. For instructions, see “Modifying CONTROL-M/Agent system parameters” on page 409.

   EXAMPLE

If two agents are installed on a computer called appserver with the IP address 11.22.33.44, complete the following steps to associate the agents with a CONTROL-M Server on a UNIX computer:

1. On the server, define the second agent as appserver2.

2. Add the line 11.22.33.44 appserver2 to the /etc/hosts file.

3. Change the Logical Agent name field for the second agent to appserver2.
Converting a remote host to a CONTROL-M/Agent

The following procedure describes how to convert a remote host to an agent computer.

**To convert a remote host to an agent computer using CONTROL-M Configuration Manager**

1. Ensure that no jobs have been submitted to, or are running on, the required remote host.

2. In the CONTROL-M Configuration Manager, right-click the remote host and choose Delete.

3. Define the agent on the computer in the CONTROL-M/Server environment. For instructions, see “Defining a CONTROL-M/Agent” on page 64.

The agent computer is now configured.

**To convert a remote host to an agent computer using CONTROL-M Main Menu**

*NOTE*

When you perform this procedure, you will be disabling and deleting the remote host. Alternatively, you can use the ctm_agstat utility to disable the remote host and the ctmhostmap to delete the remote host. For more information, see the CONTROL-M Utility Guide.

1. Ensure that no jobs have been submitted to, or are running on, the required remote host.

2. Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

3. From the CONTROL-M Main menu, enter the number of the Agent Status option.

4. In the Agent Status menu, enter the number of the Change Agent Platform Status to Disabled option.

5. At the prompt, enter the name of the remote host you want to disable.

6. At the next prompt, enter the number of the Delete Agent Platform Entry option. This will delete the remote host.

7. Use ctmping to discover the agent. For more information, see CONTROL-M Utility Guide.

The agent computer is now configured.
Configuring and managing remote hosts

Defining remote hosts is optional since CONTROL-M can automatically discover the remote host settings at job submission time, even if you did not previously define the settings. The automatic discovery process uses the default settings for the connection properties. If there are specific settings that you want to use instead of the default settings or you do not want to wait for the automatic discovery process, you can define the remote host in the CONTROL-M Configuration Manager. This section provides the following procedures for configuring and managing remote hosts:

- map remote hosts to CONTROL-M/Agents and define default connection settings
- update a remote host’s connection settings
- override default settings for a remote host
- convert a CONTROL-M/Agent computer to a remote host computer
- list CONTROL-M/Agents that route to a remote host
- list remote hosts to which a CONTROL-M/Agent can route

To map remote hosts to CONTROL-M/Agents and define default connection settings

1. In the CONTROL-M Configuration Manager, display the Default Remote Settings dialog box by right clicking the CONTROL-M/Server, and clicking Default Remote Settings.

**NOTE**

Alternatively, you can run the CONTROL-M/Server ctmhostmap utility (described in the CONTROL-M Utility Guide) to map a remote host.
2 Click the CONTROL-M/Agents that will use both a particular connection method and a particular set of connection parameters to access remote hosts. (Later on, you can add remote hosts with different settings than the defaults.)

3 For the selected CONTROL-M/Agents, choose the default connection method (SSH or WMI) to be used when agents communicate with remote hosts.

4 For the selected connection method, fill in the parameters, as follows:

   - For SSH, supply the SSH Server port number, select the encryption algorithm, and if data should be compressed for transfer, click compression.
   - For WMI, specify the full path to a Sysout directory on the remote host that is shared and has the name SYSOUT. For example, c:\temp.

5 Click Save.

6 Repeat this process as often as necessary.

To update a remote host’s connection settings

1 In the CONTROL-M Configuration Manager, right click the remote host and choose Properties.

2 Select the appropriate CONTROL-M/Agents.

3 Modify the remote host’s communication protocol and parameters as needed.

4 Click Test to check that your modifications to the original settings are correct and workable.

5 Once the test has validated the settings, click Save.

---

NOTE

Once you have defined default connection and host-owner authentication settings, you do not need to perform this task unless you want to override the defaults for particular remote hosts.

If you submit a job to a remote host that you haven’t manually defined, CONTROL-M/Server submits the job based on the default connection settings. Once the job has been submitted, the new remote host appears in the CONTROL-M Configuration Manager.
Configuring and managing remote hosts

To override default settings for a remote host

1 In the CONTROL-M Configuration Manager, right click the CONTROL-M/Server, and click **New => Remote Host** to display Step 1 of the New Remote Host wizard.

   **NOTE**
   Alternatively, you can run the CONTROL-M/Server ctmhostmap utility (described in the *CONTROL-M Utility Guide*).

2 Type the name of the remote host, and select the CONTROL-M/Agents that will connect with the remote hosts. Click **Next**.

3 In Step 2 of the wizard, select the connection method, and fill in the required connection parameters (for details, see “To map remote hosts to CONTROL-M/Agents and define default connection settings” on page 68). Click **Test** to check that your settings are correct and workable. Click **Next**.

4 To define an owner for running jobs on the host being defined, fill in the job owner and authentication information in Step 3 of the wizard (for details, see “Defining job owner and authentication settings for CONTROL-M/Agents and remote hosts” on page 173). (If you already have an owner defined for this host, skip this step, click **Next**, and proceed to step 6.)

5 Click **Test** to check that your settings are correct and workable. Click **Next**.

6 In Step 4 of the wizard, check the summary and if it is acceptable click **Finish**.

To convert a CONTROL-M/Agent computer to a remote host computer

**NOTE**
Alternatively, you can convert by using one of the following methods:

- Run the CONTROL-M/Server ctmhostmap utility (described in the utilities chapter of the *CONTROL-M Utility Guide*).

- Run a mass conversion (described in *Appendix E, “Mass conversion of agents and remote hosts.”*

1 Ensure that no jobs are submitted or running on the CONTROL-M/Agent computer.

2 Determine all owners that use the CONTROL-M/Agent computer. You will need this information for step 5.

3 Shut down the CONTROL-M/Agent.
4 In the CONTROL-M Configuration Manager, right click the CONTROL-M/Agent, and choose Convert to Remote Host.

5 Fill in the rest of the remote host details as you would if you were defining a new remote host. For details, see “To override default settings for a remote host” on page 70.

**To list CONTROL-M/Agents that route to a remote host**

In the CONTROL-M Configuration Manager, right click the remote host and choose Show agents.

---

**NOTE**

Alternatively, you can run the CONTROL-M/Server ctm_diag_comm utility (described in the CONTROL-M Utility Guide).

---

**To list remote hosts to which a CONTROL-M/Agent can route**

In the CONTROL-M Configuration Manager, right click the CONTROL-M/Agent and choose Show remote hosts.

---

**NOTE**

Alternatively, you can run the CONTROL-M/Server ctm_diag_comm utility (described in the utilities chapter of the CONTROL-M Utility Guide).

---

**Testing communication channels**

You can test the communication channel between a CONTROL-M/Agent and its CONTROL-M/Server, or between a remote host and its CONTROL-M/Agent, at any time, as follows:

- To test communication between a CONTROL-M/Agent and its CONTROL-M/Server, right click the CONTROL-M/Agent in the CONTROL-M Configuration Manager, and choose Ping.

- To test communication between a remote host and its CONTROL-M/Agent, right click the remote host in the CONTROL-M Configuration Manager, and choose Ping.

When the communication channel test is complete, a dialog box displays the result.
Using Web Launch

Web Launch is used to prepare and deploy CONTROL-M/EM client components.

Generating a Web Launch package

1. Decide on which Windows computer containing CONTROL-M/EM client components you will create the Web Launch package, and perform any needed preparations:

A. The Web Launch package is generated out of a computer containing a CONTROL-M/EM installation. Therefore, select a CONTROL-M/EM installation that reflects the environment (configuration and data) that you want to deploy.

B. If you have already generated a Web Launch package, decide whether you are updating the existing package or creating a new instance of CONTROL-M/EM client components to exist side-by-side with the previous instance (for example, two different release levels).

If you are creating a new instance, you should use a different CONTROL-M/EM Server installation, execute the empackui again on the same computer where the first instance was packed, but specify a different instance name. Different instances require different web servers or URLs.

NOTE
You cannot use a new Web Launch package to remove contents that have already been deployed.

C. On the computer on which you are creating the package, navigate to:

<emHomeDir>\bin
Generating a Web Launch package

2

Create the Web Launch package as follows:

A Run `empackui.exe` which opens the Web Launch – Prepare Package dialog box.

B In the dialog box, fill in the Host Name and Port Number fields with the values for the web server computer.

If you are creating the package on a computer that contains both client components and server components (a full installation), the default values for CONTROL-M Web Server computer are automatically inserted into these fields.

C If you are using CONTROL-M Web Server, ensure that the default port (18080) is free and available or change the port. The following scripts can help you when defining the port for CONTROL-M Web Server:

To check which port CONTROL-M Web Server is configured to use, run the following script, as appropriate:

- On UNIX: `<emHome>/scripts/handle_emweb_port.sh get`
- On Windows: `<emHome>/bin/handle_emweb_port.bat get`

To change the default port, run one of the following scripts, as appropriate:

- On UNIX: `<emHome>/scripts/handle_emweb_port.sh set <newPortNumber>`
- On Windows: `<emHome>/bin/handle_emweb_port.bat set <newPortNumber>`

---

**NOTE**

If you are creating the package on a computer that contains a full installation, and the web server that will be used to deploy the package is up, bring down the web server before continuing with the next step.

To bring down CONTROL-M Web Server, perform one of the following as appropriate:

- On Unix: Run `<emHome>/scripts/stop_web_server.sh`
- On Windows:
  2. Right click the CONTROL-M Web Server service, and choose Stop.
Generating a Web Launch package

**NOTE**

- The port and host values are embedded in the Web Launch package. If after generating a Web Launch package you modify either value, you must
  - regenerate the Web Launch package
  - notify the end users of the new URL

- If you are using your own web server and creating multiple instances of Web Launch packages, ensure that you are using different URLs for each instance.

**D** In the **Instance** field, supply an instance name for the Web Launch package, in the format `web_<name>`, where `<name>` is the CONTROL-M/EM installation instance name. The use of unique instance names enables users to access different Web Launch packages (for example, a package for production and a different package for testing). The following characters are not valid for use in the **Instance** field: `\/:*?"<>|` and `blank`.

**E** Optionally, add a description. This description later appears at the bottom of the Web Launch page when the user enters the URL. The following characters are not valid for use in the **Description** field: " <> () &

**F** If you are using certificate data from a security product, provide the file name and password (optional).

**NOTE**

If you do not provide certificate data, the end user will receive a **Publisher:** `publisher unknown` message when deploying the updates for the first time. This does not affect Web Launch package deployment.

**G** Click **Package Now**.

The empackui application generates the following:

- A Web Launch package, which includes a directory containing all files needed to deploy the client component updates.

- A URL that points to a BMC-supplied HTML web page that allows users to access the Web Launch package. (You should not edit or change the web page HTML or icons.) The referenced URL is displayed only in full installations, but whether or not it is displayed, its value is:
  ```
  http://<host>:<port>/web-launch/
  ```
A .zip and a .tar file which can be used in the optional step below.

NOTE
Each time you generate a new package, the new .zip and .tar files override the earlier .zip and .tar files.

3 If you created the Web Launch package in a different location than the instance of a full CONTROL-M/EM installation, do the following:

A Stop the web server. To stop CONTROL-M Web Server, run one of the following scripts, as appropriate:

- On Unix: `<emHome>/scripts/stop_web_server.sh`
- On Windows:
  2. Right click the CONTROL-M Web Server service, and choose Stop.

B If you are using a web server that was not supplied by BMC Software, create a physical directory in the web server host and then define the directory as a virtual directory called web-launch.

C Copy the appropriate package file (either the .zip file for Windows, or the .tar file for UNIX) from

`<clientHomeDir>\emweb\deploy`

to the appropriate web server location, as follows:

- If you are using CONTROL-M Web Server, the location is:
  - On Unix: `<emHomeDir>/appl/emweb/jetty/webapps/`
  - On Windows: `<emHomeDir>\emweb\jetty\webapps`

- If you are using a different web server, copy it to the physical directory you created in substep 3B.

D Continue as follows:

- For Windows, extract the files to the same directory mentioned in substep 3C.
- For UNIX, uncompress the files to the same directory mentioned in substep 3C by entering `tar -xvf <tarFilename>`.
Deploying new packages

4 Start the web server. To start CONTROL-M Web Server, do one of the following, as appropriate:

- On Unix: Run `<emHome>/scripts/start_web_server.sh`
- On Windows:
  2. Right click the CONTROL-M Web Server service, and choose Start.

The Web Launch package is now ready for deployment on all computers.

5 If you are updating of an existing Web Launch package, the package is automatically deployed, and there are no more steps for you to perform. If, however, this a new instance of a Web Launch package, continue by implementing the steps in “Deploying new packages”.

Deploying new packages

**NOTE**

Users do not require administrative privileges to deploy packages.

Each time a new package is to be deployed, provide your users (for example, through e-mail) with the following information they need to deploy the package. (You do not need to provide this information for upgrades to existing packages; upgrades to existing packages are automatically deployed when the user launches CONTROL-M/EM, CONTROL-M/Desktop, or CONTROL-M Configuration Manager.)

- The URL that they must access for first-time deployment (generated when the Web Launch package was created).
- The Web Launch package will not overwrite their existing data.
They must perform the following steps the first time they deploy the Web Launch package on computers containing CONTROL-M/EM clients, but they will not need to perform these steps for subsequent upgrades:

1. Open the CONTROL-M/EM Web Launch page by entering the supplied URL in the web browser.

2. In the Web Launch page, click to open any of the available applications (CONTROL-M/Desktop, CONTROL-M/Enterprise Manager, or CONTROL-M Configuration Manager). The package will be deployed across the entire suite of CONTROL-M/EM applications.

3. In the Install window, click Install. (Even if indicated Publisher value is Publisher Unknown, the user should still install.)

When the installation is complete, the application is launched and users are prompted to log in.

Web Launch adds the following links to the Start menu (in addition to the links for launching CONTROL-M/Enterprise Manager GUI, CONTROL-M/Desktop, and CONTROL-M Configuration Manager):

- Browse Home Directory
- Browse Data Directory

These links enable users to access the files related to the Web Launch instance. (These files are not placed in the regular Windows\Program Files directory.)

All work with a specific Web Launch CONTROL-M/EM instance (install, work, uninstall) must be performed with the same Windows user.

Users that need to uninstall a CONTROL-M/EM Web Launch instance, or an older non-Web Launch CONTROL-M/EM instance, can do so by choosing Start => Control Panel => Add/Remove from the Microsoft Windows Desktop.
## Setting up and managing the scheduling environment

This chapter presents the following topics:

1. **Conceptual overview** ......................................................... 80
2. **Methods for automating daily job scheduling** ......................... 81
3. **Automatic prerequisite condition cleanup** ............................... 86
4. **Job version management** .................................................... 87
5. **Global condition distribution time limits** ................................ 88
6. **Alert processing** ............................................................... 88
7. **Time zone support** ............................................................ 89
8. **Daylight Saving Time support** ............................................. 90
9. **Load balancing** ................................................................. 90
10. **Shout facility and Shout Destination tables** ............................. 91
11. **CONTROL-M/EM periodic job statistics** ................................ 92
12. **Job statistics generated by CONTROL-M/Server** .................... 93
13. **Group scheduling table displays in ViewPoints** ...................... 93
14. **CONTROL-M/Agent FileWatcher (ctmfw)** ............................. 94
15. **User exits** ................................................................. 95
16. **Shell scripts** ............................................................... 95

### Recommended task summary

- **Automating job scheduling** ............................................. 97
  - **Preparing for automation** ............................................ 98
  - **Customizing the New Day procedure** ................................ 98
  - **Setting up User Daily jobs** .......................................... 101
    - **Defining jobs that use ctmorder to schedule other jobs** ....... 103
  - **Handling interruptions in User Daily job processing** .......... 103
  - **Collecting and viewing application server information** ........ 104
  - **Implementing job version management** ............................. 105
  - **Defining quantitative resources, control resources, and global conditions** ........ 107
  - **Modifying the time limit on Global conditions distribution** .... 107
  - **Activating scripts with alert data** .................................. 108
  - **Implementing time zone support (optional)** ....................... 110
    - **Setting up time zone support for jobs** ......................... 110
    - **Ensuring correct time zones for jobs in the Active Jobs file** .. 111
Conceptual overview

The main goal in setting up a scheduling environment is to model your production batch processing flows. Figure 10 on page 81 highlights the basic recommended workflow for setting up the scheduling environment. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 5 on page 96. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

NOTE

This chapter assumes that the administrator is responsible for setting up the scheduling environment at your site. However, at some sites, end-users with administrator privileges perform some of the relevant tasks.
Methods for automating daily job scheduling

The following table briefly defines key terms that you will encounter in this section.
To automate daily job scheduling, maintenance, and cleanup, you can choose any of the following methods, or a combination of them:

- **New Day procedure**

A procedure, called the New Day procedure, is defined for each CONTROL-M/Server. Each day, at its designated New Day time, each CONTROL-M/Server runs its New Day procedure. This procedure automatically starts process and functions required at the start of a new day under CONTROL-M, including daily cleanup and housekeeping, and the scheduling of current day’s production jobs.

At the beginning of the New Day procedure, the procedure calculates a new CONTROL-M working date, and displays the message **FORMATTING AJF** in the CONTROL-M/EM Communication Status window for the CONTROL-M.

The following is a list of some of the more important cleanup and housekeeping functions that the New Day procedure automatically initiates. You can adjust or disabled many of them:

- partial cleanup of the CONTROL-M/Server log (based on system parameter **Maximum Days Retained By CONTROL-M Log**)

- partial cleanup of job SYSOUT directories on agent computers (based on system parameter **Maximum Days to Retain Sysout Files**)

### Table: Key Terms and Definitions

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ctmudly</td>
<td>utility run by a User Daily job (command: ctmudly <em>name</em>) that scans scheduling tables associated with the User Daily <em>name</em>, and schedules jobs in the table that should be scheduled that day</td>
</tr>
<tr>
<td>New Day procedure</td>
<td>daily scheduling and housekeeping procedure run at New Day time, that cleans up the database from the previous day’s processing and loads new jobs to the Active Jobs file for the current day’s processing</td>
</tr>
<tr>
<td>New Day time</td>
<td>site-defined time when the new processing day begins and CONTROL-M runs the New Day procedure</td>
</tr>
<tr>
<td>User Daily (name)</td>
<td>logical name, associated with one or more scheduling tables, that can be specified when the ctmudly utility is run (command: ctmudly <em>name</em>)</td>
</tr>
<tr>
<td>User Daily job</td>
<td>user-defined job that can be used to help automate the ordering of production jobs by running the ctmudly utility</td>
</tr>
<tr>
<td>Date Control record</td>
<td>record that indicates (in the UDLAST field) the date on which the User Daily last ran</td>
</tr>
</tbody>
</table>
Methods for automating daily job scheduling

Chapter 3  Setting up and managing the scheduling environment  83

- Selective cleanup of the Active Jobs file—jobs that have already executed and ended OK, and jobs whose parameter Max Wait has been exceeded (and are not Held), are erased from the Active Jobs file.

- Selective cleanup of prerequisite conditions—to prevent jobs from being triggered by prerequisite conditions remaining from the previous year, prerequisite conditions are deleted if they are one year old (prerequisite conditions whose month and day date reference is equal to tomorrow’s date—the new CONTROL-M working date +1. For more information on prerequisite condition deletion, see “Automatic prerequisite condition cleanup” on page 86.

- Partial cleanup of the statistics in the CONTROL-M/Server database (the number of successful executions for which statistics are retained can be adjusted using the RUNINF_PURGE_LIMIT parameter in the CONTROL-M config.dat file; Default: 20).

- Partial cleanup of the information in the JOBINF table that is specific to any one instance of a job run.

The New Day procedure can also schedule jobs (place job orders in the Active Jobs file) if the job’s scheduling criteria are satisfied that day. The procedure only schedules those jobs that belong to scheduling tables assigned to the reserved User Daily called SYSTEM. (For more information, see “More about User Daily jobs” on page 84.)

If your site has a small number of production jobs, using the New Day procedure to schedule all of them might be advantageous. However, it is frequently more efficient to use User Daily jobs with the New Day procedure.

CONTROL-M downloads the new Active Jobs file to CONTROL-M/EM. During download, CONTROL-M processes are suspended.

- User Dailies

User Dailies are optional, but when used, they are used with the New Day procedure. Many sites prefer to split the task of job ordering among multiple User Dailies. This is especially true if two or more of the following conditions exist:

- The site has a large number of production jobs.
- Jobs can be meaningfully split into different categories.
- Different people manage different jobs.
User Dailies offer several advantages:

— When you use User Dailies, the New Day procedure finishes more quickly.

— User Dailies enable you to schedule jobs at any time during the day. Thus, you can prevent Product Name from having to load the full day’s production job load at New Day time.

— You can delegate responsibility for User Dailies to other users at your site.

■ ctmorder utility

The ctmorder utility performs job scheduling from a scheduling table in the CONTROL-M/Server database. You can define jobs that will automatically run this utility.

In practice, most sites prefer a combined approach, using both the New Day procedure and User Daily jobs.

More about User Daily jobs

A User Daily job runs the ctmudly utility through the ctmudly name command. The variable name represents a specific User Daily name that is associated with one or more scheduling tables. The utility scans those scheduling tables, looking for jobs that should be scheduled that day, and then schedules them.

The User Daily name is merely a logical name or label:

■ When creating a scheduling table, you can associate a User Daily name with that table.

Each scheduling table can have more than one User Daily name associated with it, and you can associate a User Daily name with multiple scheduling tables.

■ A special User Daily name, SYSTEM, identifies the “master” User Daily. When the New Day procedure runs, it scans all scheduling tables whose associated User Daily name is SYSTEM. The New Day procedure looks for jobs in those tables that should be ordered on that day, and then orders them.
Date Control records and the UDLAST field

To enable CONTROL-M to track when a User Daily job last ran, each User Daily job has a Date Control record associated with it. This record contains a field, **UDLAST**, that records the last running date of the User Daily. By comparing the value of **UDLAST** to the current working date, CONTROL-M can determine whether a User Daily job has already run that day.

In general, you should not change the UDLAST field. In certain circumstances, adjusting this date might be useful. For example, to enable the User Daily to run again on a given day, you can adjust the UDLAST date to be earlier than the current working date. When necessary, you can use the ctmudlst utility to update the UDLAST date.

**WARNING**
Changing the UDLAST value can have unintended, harmful results. BMC Software recommends that you contact BMC customer support before undertaking such a step.
Automatic prerequisite condition cleanup

By default (the **Ignore New Day Conditions** system parameter is set to N), the New Day procedure cleans up prerequisite conditions that are one year old. BMC Software recommends that you do not modify the value of this parameter.

Changing the value of **Ignore New Day Conditions** to Y, so that the New Day procedure does not clean up old conditions would only be useful if your site has jobs that are triggered by prerequisite jobs that ran the year before.

But changing **Ignore New Day Conditions** to Y could greatly increase the risk that jobs will be prematurely triggered—jobs that are waiting for a prerequisite job that will run in the future can be triggered by a job that ran in the past.

BMC Software provides a much better and safer alternative to enable you to retain prerequisite conditions for more than one year without changing the default value of the **Ignore New Day Conditions** parameter: You can have those conditions added to the Conditions file with a date reference value of STAT—conditions with a STAT reference are not automatically cleaned by the New Day procedure.

However, because you do have the capability to change the value of the **Ignore New Day Conditions** parameter, to minimize the risks involved, CONTROL-M requires that you perform an additional step if you do set **Ignore New Day Conditions** to Y: You must identify the prefixes or masks of the conditions that should be ignored (that is, not deleted) in the Ignore Conditions file (**dbs_ignrcond.dat**). Any conditions whose prefixes or masks are not specified in the file are treated as if you did not change the default.

Therefore, if your site will be retaining prerequisite conditions beyond one year, it is recommended that you provide them with a prefix not used by conditions that should be deleted on time.

**Example**

Assume the **Ignore New Day Conditions** parameter is set to Y and the Ignore Conditions file contains the following prefixes:

```
prq_rs_*rpt
tre_prn
srt_def_?
```

If the new CONTROL-M working date is 15-01-00, the following table demonstrates which prerequisite conditions will be deleted from the CONTROL-M/Server database by the New Day procedure:
Job version management

The job version management feature allows CONTROL-M/EM to save earlier versions of job processing definitions. End users can use and manipulate these job versions using CONTROL-M/Desktop (or other interfaces such as XML utilities).

By default, CONTROL-M/EM saves both the current version and the most recent earlier version of your jobs.

Job version management also allows retention of deleted jobs for a specified period of time. They are logically deleted (marked as deleted), but retained until they are physically deleted. Until then, you can restore deleted jobs.

CONTROL-M administrators implement job version management by setting CONTROL-M/EM system parameters which instruct CONTROL-M/EM how to manage job versions, including:

- whether or not to save earlier versions of jobs
- how many job versions to save and for how long to save them
- how long to retain deleted jobs

If job version management is implemented and active at your site, the CMS server automatically deletes older job versions according to the relevant system parameter settings, as follows:

- If the retention period for a logically deleted table has passed, the CMS physically deletes the whole table, with its jobs and their history.

<table>
<thead>
<tr>
<th>Conditions existing before executing New Day Procedure</th>
<th>Conditions remaining after executing New Day Procedure</th>
</tr>
</thead>
<tbody>
<tr>
<td>bra_fn_01 14/01</td>
<td>bra_fn_01 14/01</td>
</tr>
<tr>
<td>bra_fn_01 15/01</td>
<td></td>
</tr>
<tr>
<td>prq_rs_21rpts 14/01</td>
<td>prq_rs_21rpts 14/01</td>
</tr>
<tr>
<td>prq_rs_21rpts 15/01</td>
<td>prq_rs_21rpts 15/01</td>
</tr>
<tr>
<td>pre_prn 15/01</td>
<td>pre_prn 15/01</td>
</tr>
<tr>
<td>pre_prn_01 15/01</td>
<td></td>
</tr>
<tr>
<td>srt_def_a 15/01</td>
<td>srt_def_a 15/01</td>
</tr>
<tr>
<td>srt_def_a1 15/01</td>
<td></td>
</tr>
</tbody>
</table>
If the retention period for a logically deleted job has passed, the CMS physically deletes the job and its history from the table.

If the retention period for a logically deleted job’s history has passed, but the retention period for the deleted job itself has not passed, the CMS physically deletes the job’s history (but not the job).

For non-deleted jobs, if both the time limit for keeping past versions and number of past versions to keep has been exceeded, the CMS physically deletes those versions of the jobs which are expired according to both sets of deletion criteria.

Once you have implemented job version management, if you later switch it off, the CMS immediately deletes all previously saved job versions (it ignores the time limit and number of versions values that were defined to determine how long to keep the job’s version history).

You can also manually delete job versions by running the ccmcli utility.

Global condition distribution time limits

The Global Conditions Distribution facility enables the user to specify or remove date limitations for distributing global conditions. The default specifies that global conditions are distributed to data centers only within seven days of their defined condition date.

With the Global Conditions Distribution facility, the user can indicate whether to limit the distribution of global conditions, specify a range of days for which global conditions can be distributed, and provide a list of condition dates that are excluded from the limitation process (so that global conditions with these dates are distributed without limitations).

Alert processing

The Alert Data Processing facility is used to activate processes based on data in a generated Alert. By default, the data is sent from an alert to an SNMP trap. The facility allows you to use the alert data as input to a script, in addition to or in place of sending it to an SNMP trap. For information about SNMP, see Appendix D, “SNMP interface.”

When Alert data is sent as input to a script, the parameters are sent in the following format:
Time zone support

Whenever useful, you can define time zones for jobs in their job processing definitions. Generally, time zone support is relevant if the time by which the job must run is determined by a time zone different than the time zone of the CONTROL-M/Server computer responsible for the job.

EXAMPLE


Time zone support

A job run that should run by 10:00 a.m. in Houston, Texas (Central Standard Time) is ordered by a CONTROL-M/Server in New York (Eastern Standard Time).

To ensure that the job is submitted on time, you could manipulate the Submit By time in the job processing definition to compensate for the hour difference (for example, define the submission time as 11:00 a.m.). However, making such adjustments manually can be an error prone process.

A better method would be to define the job as belonging to the Central Standard Time, and indicate the local time (Central Standard Time) by which the job should be submitted (10:00 a.m.).

Time zone support is especially useful when it impacts the day a job is ordered during New Day processing. This often occurs only if the time zone for the computer that will run the job is far ahead of the time zone of the CONTROL-M/Server computer—so far ahead that the job must be ordered a day early so that it will be available for execution on the correct day on the remote computer.
**Daylight Saving Time support**

_A EXAMPLE_

A job must be run at 6:00 a.m. Tokyo time (before the opening of the stock exchange in Tokyo). However, the New Day procedure that schedules the job runs on a CONTROL-M/Server computer in Paris at 7:00 a.m.

Without time zone support, the CONTROL-M/Server would run at 7:00 A.M. in Paris and schedule the Tokyo job, but it would be 2:00 P.M. in Tokyo, well past the time for submitting the job in Tokyo.

With time zone support implemented, CONTROL-M/Server in Paris will order the job the day before. For example, to enable job submission at 6:00 a.m. on August 23 in Tokyo, the CONTROL-M/Server in Paris will order the job during New Day processing on August 22.

The time zones definitions are maintained in _TimeZone.dat_ files in CONTROL-M/EM and each CONTROL-M/Server. You identify to which time zone a CONTROL-M/Server belongs in the CONTROL-M/Server definition.

The _TimeZone.dat_ files contain a pre-supplied list of time zone definitions. You can modify or add time zone definitions in these files, but you must keep the CONTROL-M/EM and CONTROL-M/Server time zone files synchronized so that they contain the same time zones.

**Daylight Saving Time support**

If the CONTROL-M/Server resides in a location that uses Daylight Saving Time, you can implement Daylight Saving Time (DST). To implement Daylight Saving Time support, you change the format of the _TimeZone.dat_ file for the relevant CONTROL-M/Servers. You cannot, and there is no need to, change the format of time zone definitions in CONTROL-M/EM.

For instructions, see “Implementing Daylight Saving Time support” on page 111.

**Load balancing**

The load balancing feature enables you to submit a job to a _node group_ rather than to a specific agent or remote host computer. (A node group is a user-defined list of agent and remote host computers that are capable of running a given job.) After using a load balancing algorithm to determine which agent or remote host computer in the node group is best equipped to run the job at the moment, CONTROL-M/Server submits the job to that node.

This feature enables CONTROL-M to optimize utilization of available resources and ensure maximum production throughput.
Shout facility and Shout Destination tables

As part of scheduling environment setup, you should create and maintain Shout Destination tables. The CONTROL-M Shout facility sends messages to specified recipients (for example, users, terminals, files, and the CONTROL-M/Server log) based on a destination specified by the Shout or Do Shout parameters in a job processing definition.

**NOTE**
You can also use the ctmshout utility to issue a Shout message to an indicated destination. For more information, see the CONTROL-M Utility Guide.

The Shout Destination table contains a list of logical destinations and the equivalent physical destination of each logical destination.

**Figure 11  Using the Active Shout Destination Table to direct shouts**

![Diagram](image)

**EXAMPLE**
The system administrator defined two Shout Destination tables, DAYSHIFT and NIGHTSHIFT:

- In DAYSHIFT, the logical recipient SYS_MANAGER is equated to user Susan, who is the daytime systems manager.

- In NIGHTSHIFT, the logical recipient SYS_MANAGER is equated to user Robert, the nighttime systems manager.

When the DAYSHIFT Shout Destination table is active, Shout messages that are addressed to SYS_MANAGER go to Susan’s terminal. At 5 P.M., a job runs and changes the active Shout Destination table to NIGHTSHIFT. Starting then, Shout messages that are addressed to SYS_MANAGER go to Robert’s terminal.
CONTROL-M/EM periodic job statistics

CONTROL-M/EM collects job runtime statistics that are used for a number of runtime statistic calculations purposes, including:

- CONTROL-M/Forecast
- BMC Batch Impact Manager
- Critical path analysis for jobs
- Statistics details in the Active tab in the job editing form in CONTROL-M/EM

**NOTE**

When right-clicking a job node in the CONTROL-M/EM GUI and selecting Statistics, the data is displayed as follows:

- For jobs defined on a CONTROL-M server version 6.4.01 or later, CONTROL-M/EM statistics are displayed.

- For jobs defined on a CONTROL-M server version 6.3.01 or earlier, CONTROL-M statistics are displayed.

The statistics that CONTROL-M/EM collects are periodic. This means that CONTROL-M can accumulate different sets of a job’s statistics for different periods. The periods are defined using periodic calendars.

**EXAMPLE**

A particular job that runs daily takes about 10 minutes to run on most days. However, on Fridays, this job usually takes about 40 minutes to run, due to the processing load on that day. Collecting a single set of statistics would give an inaccurate view of required processing time (too much time for most days; too little time for Fridays).

However, if you define two periods in a periodic calendar—one period having all days but Friday, and the other period having only Fridays—CONTROL-M/EM will collect two separate, but very useful and representative, sets of statistics for the job.

The first set of statistics will then be used in calculations for all days but Fridays, and the second set will only be used for Friday’s calculations.

Periodic calendars are defined in the CONTROL-M/Desktop using the Calendar Manager. Prior to CONTROL-M/EM version 6.4.01, periodic calendars were only used for job scheduling. Now, the same or different periodic calendars can be used for defining statistic collection periods. End-users or administrators can use the Periodic Statistics Manager in the CONTROL-M/Desktop to relate specific jobs to specific periodic calendars for statistical purposes. If a job is not related to a periodic calendar for statistics collection, CONTROL-M/EM collects a single set of statistics, spanning all days, for the job. For more information, see the chapter related to periodic statistics collection in the CONTROL-M User Guide.
Collection of periodic statistics in CONTROL-M/EM is automatically enabled; it requires no special activation by the administrator. However, by modifying system parameter defaults, the CONTROL-M administrator can determine the sample to be used for collecting periodic statistics, how long CONTROL-M will retain periodic statistics, and the interval between periodic statistic purges.

Job statistics generated by CONTROL-M/Server

CONTROL-M includes an option for collecting and analyzing runtime statistics for each defined job. If you enable the job statistics feature, CONTROL-M/Server automatically collects job statistics and stores them in the Statistical Details table of the CONTROL-M/Server database. Then, whenever you run the ctmjsa utility, the utility analyzes the accumulated statistics and generates and stores a summary in the Statistical Summary table.

These statistics are used for the following purposes:

- The Shout job processing parameter can be specified to issue a message if the execution time that is required by a job varies from its average runtime by more than a stated interval. This message can help highlight possible errors. (The Shout parameter is described in the CONTROL-M Parameter Guide.)

- The following CONTROL-M for z/OS features also use CONTROL-M job statistics (for more information, see the INCONTROL for z/OS Administrator Guide):
  - Critical path and expected Due Out calculation for Deadline scheduling
  - Shouting when a job is not submitted by the calculated Due In time
  - Shouting when a job runs longer than expected

Group scheduling table displays in ViewPoints

When you define ViewPoint filtering criteria, it can happen that a scheduling group satisfies the criteria but none of the jobs in the group scheduling table satisfy the criteria. By default, when a scheduling group, but no jobs in the Group scheduling table, satisfy the ViewPoint filtering criteria, the GUI Server does not display the Group scheduling table in the ViewPoint.
By modifying the appropriate system parameter, you can display the Group scheduling table in the ViewPoint, even though no jobs will be displayed in the table.

**EXAMPLE**

According to the filtering criteria for the ABC ViewPoint, only jobs having an In prerequisite condition called CondA are displayed.

The scheduling group in the XYZ Group scheduling table has CondA as an In prerequisite condition, but none of the jobs in that Group scheduling table have A as a prerequisite condition.

By default, the group scheduling table is not displayed in the ViewPoint.

An important usage is to activate it before the running of a job or performance of task (for example, sending a shout message or adding/deleting conditions) that is dependent upon creation or deletion of a file. The process waits for the creation or deletion of specified files:

- For a file transfer activity, when the file is detected, the job continues to monitor the size of the file. When the file reaches a specified minimum size and does not increase in size for a specified period of time, the FileWatcher utility either completes with a status of **OK** or executes a specified **DO** action. **DO** actions can consist of adding or deleting conditions or executing a command.

- For file creation, file size is ignored if a wildcard is specified as part of the filename unless the **mon_size_wildcard** parameter is set to **Y**.

- For file deletion, **ctmfw** must first detect the existence of the file before it can detect its deletion.

**ctmfw** utility can also be run from the command line, or be invoked to detect either a single file or multiple files.
User exits

A user exit is a user-defined procedure that can be used to modify certain information before it is processed. At certain points in processing, a flat text file is produced describing information that is to be passed to the next step in a procedure. This text file can be modified by a user-defined exit script before it is passed on for processing.

CONTROL-M/Server user exits can be used to enforce site standards (for example, file naming conventions or valid date formats), and to apply security definitions to limit certain user’s actions. Exits can also be used to trigger other actions prior or subsequent to execution of a CONTROL-M job.

--- EXAMPLE ---
The following steps illustrate what happens when a user exit is enabled:

1. A flat text file is produced containing parameters to be processed by CONTROL-M.
2. The name of the text file is passed as a parameter to the user exit script.
3. The user exit script is run. This script is often used to modify the contents of the text file. However, it can also be used to perform any other action (for example, to copy information from the text file to another location).
4. CONTROL-M continues processing using the modified text file.

User exits are implemented only if they have been enabled by setting the appropriate configuration parameters. For a summary of available user exits, see Table 8 on page 129.

Shell scripts

You can write shell scripts to be run as CONTROL-M/Server jobs on an agent computer.

- When writing a shell script to be run as a CONTROL-M/Server job on a Unix agent computer, you must consider and handle the issues:
  - Specifying the shell type
  - Factoring in the run-time environment
  - Using the On Statement/Code parameter to interpret script lines
When writing a shell script to be run as a CONTROL-M/Server job on a Windows agent computer, you must consider and handle the issues:

— Implementing basic guidelines
— Using On Statement/Code parameters correctly
— Enabling CONTROL-M/Server to distinguish between exit codes
— Using script utilities
— Translating DOS files and REXX scripts to UNC

**Recommended task summary**

Table 5 lists specific tasks related to each phase of the workflow (Figure 10 on page 81). Subsequent sections provide step-by-step instructions.

**NOTE**

This chapter assumes that the administrator is responsible for setting up the scheduling environment. However, at your site, users might perform some or all of these tasks.

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Automate job scheduling</td>
<td>Preparing for automation</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Customizing the New Day procedure</td>
<td>98</td>
</tr>
<tr>
<td></td>
<td>Setting up User Daily jobs</td>
<td>101</td>
</tr>
<tr>
<td></td>
<td>Defining jobs that use ctmorder to schedule other jobs</td>
<td>103</td>
</tr>
<tr>
<td>Implement job version management</td>
<td>Implementing job version management</td>
<td>105</td>
</tr>
<tr>
<td>Define quantitative and control resources, and global conditions</td>
<td>Defining quantitative resources, control resources, and global conditions</td>
<td>107</td>
</tr>
<tr>
<td>Activate scripts with alert data (optional)</td>
<td>Activating scripts with alert data</td>
<td>108</td>
</tr>
<tr>
<td>Implement time zone support (optional)</td>
<td>Setting up time zone support for jobs</td>
<td>110</td>
</tr>
<tr>
<td></td>
<td>Ensuring correct time zones for jobs in the Active Jobs file</td>
<td>111</td>
</tr>
<tr>
<td>Implement Daylight Saving Time support (optional)</td>
<td>Editing definitions to support Daylight Saving Time</td>
<td>112</td>
</tr>
<tr>
<td>Implement load balancing</td>
<td>Defining and maintaining a node group</td>
<td>113</td>
</tr>
<tr>
<td></td>
<td>Identifying jobs that can be load balanced</td>
<td>115</td>
</tr>
<tr>
<td>Set up Shout Destination tables</td>
<td>Defining and maintaining Shout Destination tables</td>
<td>116</td>
</tr>
<tr>
<td></td>
<td>Making a Shout Destination table the currently active table</td>
<td>121</td>
</tr>
<tr>
<td>Modify CONTROL-M/EM periodic statistic cleanup defaults</td>
<td>Modifying CONTROL-M/EM periodic statistic retention and cleanup defaults</td>
<td>121</td>
</tr>
</tbody>
</table>
Automating job scheduling

The process of automating job scheduling involves the following tasks:

- Preparing for automation
- Customizing the New Day procedure
- Setting up User Daily jobs
- Defining jobs that use ctmorder to schedule other jobs

---

Table 5   Task summary: setting up the scheduling environment (part 2 of 2)

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement CONTROL-M runtime statistics collection</td>
<td>Setting whether CONTROL-M/Server collects job statistics</td>
</tr>
<tr>
<td></td>
<td>Defining the CONTROL-M/Server statistics collection mode</td>
</tr>
<tr>
<td></td>
<td>Ensuring that the ctmjsa utility runs daily to collect CONTROL-M/Server statistics</td>
</tr>
<tr>
<td></td>
<td>Displaying (or deleting) CONTROL-M/Server statistics as needed</td>
</tr>
<tr>
<td>Implement user exits</td>
<td>Implementing user exits</td>
</tr>
<tr>
<td>Write scripts (UNIX only)</td>
<td>Specifying the shell type</td>
</tr>
<tr>
<td></td>
<td>Factoring in the run-time environment</td>
</tr>
<tr>
<td></td>
<td>Using the On Statement/Code parameter to interpret script lines</td>
</tr>
<tr>
<td>Write scripts (Windows only)</td>
<td>Implementing basic guidelines</td>
</tr>
<tr>
<td></td>
<td>Using On Statement/Code parameters correctly</td>
</tr>
<tr>
<td></td>
<td>Enabling CONTROL-M/Server to distinguish between exit codes</td>
</tr>
<tr>
<td></td>
<td>Using script utilities</td>
</tr>
<tr>
<td></td>
<td>Translating DOS files and REXX scripts to UNC</td>
</tr>
</tbody>
</table>

---

*a* You need to implement time zone support only if time zone differences between local and remote computers impact job ordering at your site. For more information, see “Time zone support” on page 89.

*b* You need to implement Daylight Saving Time support only if your CONTROL-M/Server resides in a location that uses Daylight Saving Time (DST).
Preparing for automation

1 Before proceeding, make sure that you have created the job processing definitions, scheduling tables, and scheduling groups that you will need.

You can perform these tasks either online or in batch, or a combination.

■ To perform these tasks online, follow the instructions that are provided in the CONTROL-M User Guide.

■ To perform these tasks in batch you can use any combination of:
  — the API facility
  — CONTROL-M/Server utilities such as ctmdefine and ctmgrpdef
  — CONTROL-M/EM utilities such as deftable and defjob

For details, see the CONTROL-M/Enterprise Manager API Developer Guide and the CONTROL-M Utility Guide.

2 Make sure that scheduling tables are associated with relevant User Dailies. For instructions, see the CONTROL-M User Guide.

3 Define resources and conditions. These ensure that CONTROL-M/Server does not submit a job unless all required resources are available. For instructions on defining resources and conditions, see the CONTROL-M User Guide.

Customizing the New Day procedure

The New Day procedure is supplied with the product, and generally requires only a small amount of site customization. To customize the New Day procedure, for each CONTROL-M/Server you should determine and define appropriate values for configuration and system parameters, as follows:

1 Set appropriate system parameter values as follows:

   A Display the CONTROL-M System Maintenance Utility Main Menu (ctmsys). For instructions on displaying the menu, see “Using the CONTROL-M System Maintenance Utility Main Menu” on page 47.

   B In the CONTROL-M System Maintenance Utility Main Menu, enter the number of the System Parameters option to display the CONTROL-M System Parameters menu.

   C To set the New day time (default: +0700):
1. Enter 1 (Day Time)

2. At the prompt, enter the value of the New Day Time preceded by a + (for example, +08:00).

D Enter N to display the next page of the System Parameters menu.

E To set the retention period for CONTROL-M/Server logs (default: 2 days)

1. Enter 6 (Maximum Days Retained by CONTROL-M Log)

2. At the prompt, enter the value for the number of days to retain log information (for example, 4).

F To set the retention period for CONTROL-M/Server SYSOUTS (default: 1 day)

1. Enter 7 (Maximum Days to Retain SYSOUT files)

2. At the prompt, enter the value for the number of days to retain log information (for example, 2).

G To define that the New Day procedure should ignore (not cleanup) conditions, enter 8 to toggle the Ignore New Day Conditions system parameter to Y.

WARNING

BMC Software recommends that you not change the default. If you are considering changing it, see “Automatic prerequisite condition cleanup” on page 86 before making your decision.

If you do change the Ignore New Day Conditions system parameter to Y, perform the following:

1. Edit the following file in the home directory of the CONTROL-M owner account:

~<controlm_owner>/ctm_server/data/dbs_ignrcond.dat

2. Ensure the file contains the list of prefixes of prerequisite conditions, and/or including masks, that should not be deleted by the New Day procedure. Prerequisite condition names are case-sensitive; the mask character * and ? are supported.

H Enter S to save the changes and return to the Main Menu.

I Enter q to exit the Main Menu.
Customizing the New Day procedure

2 Set appropriate configuration parameter values in the CONTROL-M/Server configuration parameter file (~<controlm_owner>/ctm_server/data/config.dat on the server computer), as follows:

- Define whether the New Day procedure should cleanup (delete) job runtime statistics, by running the ctmruninf utility. (You can also run this utility manually, and use the utility to display runtime statistics summaries.)

  — By default, the New Day procedure cleans up statistics (the STATISTICS_CLEANUP_IN_NEWDAY configuration parameter is set to Y).

  — To speed up the New Day procedure, set the STATISTICS_CLEANUP_IN_NEWDAY configuration parameter to N, but be sure to periodically run ctmruninf - PURGE manually. For information, see the ctmruninf utility in the CONTROL-M Utility Guide.

- Define whether the New Day procedure should cleanup (delete) SYSOUT files and unneeded user exit status files from CONTROL-M/Agent computers (using the ctmagcln utility.)

  — By default, the New Day procedure cleans up the SYSOUT and User exit status file (the AGENTS_CLEANUP_IN_NEWDAY configuration parameter is set to Y).

  — To speed up the New Day procedure, set the AGENTS_CLEANUP_IN_NEWDAY configuration parameter to N, but be sure to periodically run the ctmagcln utility manually. For information, see the ctmagcln utility in the CONTROL-M Utility Guide.

3 If any scheduling tables should be ordered by the New Day procedure (instead of User Daily jobs), associate them with the SYSTEM User Daily as follows:

A In CONTROL-M/Desktop, select Tools => Scheduling Table Manager.

B In the Scheduling Table Manager window, select the scheduling table and click (Table Details).

C In the Scheduling Table dialog box, specify SYSTEM (uppercase only) in the User daily field.

D Click OK, which saves the changes in the CONTROL-M/EM database.

E To apply the changes to the table definition in the CONTROL-M database, upload the table by it in the Scheduling Table Manager and clicking . If you are prompted for confirmation, confirm.
**Setting up User Daily jobs**

**NOTE**
If you are defining a z/OS scheduling table, any value you specify in the User daily field is for documentation purposes only. To actually assign the scheduling table to the New Day procedure or to a specific User Daily job, follow the instructions in the *CONTROL-M for z/OS User Guide*.

---

**Setting up User Daily jobs**

**NOTE**
If your site will not be using User Daily jobs, you should associate with the User Daily name SYSTEM those scheduling tables that you want scanned by the New Day procedure.

---

**1** Plan the implementation. This includes considering the following:

- Do you want any of your scheduling tables scanned by the New Day procedure. If so, they should be associated with the SYSTEM User Daily name.

- If you are using User Dailies other than SYSTEM, how many will you use and according to what criteria will you associate the scheduling tables to them? Departmental control issues should be factored in. Also, it can be more efficient to define multiple User Daily jobs, each to be scheduled at a different time during the day. This ensures that jobs are not loaded to the Active Jobs file until close to the time that they will need to be submitted.

- Do you want to put all User Daily jobs in only one scheduling table or in multiple scheduling tables (each scheduling table containing User Daily jobs should be associated with the SYSTEM User Daily name).

- Do you want the scheduling tables that contain User Daily jobs to contain any other types of jobs?

**2** Create the scheduling tables that will contain User Daily jobs, and associate them with the SYSTEM User Daily, as follows:

   **A** In CONTROL-M/Desktop, select **Tools => Scheduling Table Manager**.

   **B** In the Scheduling Table Manager window, click **New**.

   **C** In the Scheduling Table dialog box, fill in the details for the new scheduling table, as follows:
Setting up User Daily jobs

1. Choose the CONTROL-M and specify a name for the scheduling table.

   **NOTE**
   Each scheduling table is associated with the platform of its CONTROL-M.

2. If you are creating a z/OS scheduling table, specify the library name.

3. In the **User daily** field, specify **SYSTEM** (uppercase only).

   **NOTE**
   If you are defining a z/OS scheduling table, any value you specify in the User daily field is for documentation purposes only. To actually assign the scheduling table to the New Day procedure or to a specific User Daily job, follow the instructions in the **CONTROL-M for z/OS User Guide**.

D Click **OK**, which saves the scheduling table in the CONTROL-M/EM database (and displays the name in the Scheduling Table Manager window).

3 Associate all other scheduling tables with the appropriate User Daily name according to your planned implementation, as follows:

   A In the Scheduling Table Manager window, select the scheduling table and click *(Table Details)*.

   B In the **Scheduling Table** dialog box, specify in the **User daily** field the name of the User Daily job (1-10 characters, case sensitive) that should order the table.

   C Click **OK**, which saves the changes in the CONTROL-M/EM database.

4 To apply the changes to the table definition in the CONTROL-M database, upload the table by it in the Scheduling Table Manager and clicking **Upload**. If you are prompted for confirmation, confirm.

5 In the scheduling table(s) you created to hold User Daily jobs, define the User Daily jobs that will invoke the ctmdly utility. The utility is invoked by the `ctmdly name` command, where `name` is the User Daily name associated with scheduling tables.

   You can have User Daily jobs invoke the ctmdly utility in either of the following ways:

   - You can define the User Daily job as a Command-type job, and have it issue the `ctmdly name` command. Such a User Daily job can only invoke the utility for a single User Daily name.
Defining jobs that use ctmorder to schedule other jobs

You can define the User Daily job as a Job-type job, and have it run a script that issues the `ctmudly name` command. The script can contain multiple instances of the `ctmudly name` command. The name can be stated explicitly in the script file or it can be specified using AutoEdit Assignment statements.

Be sure to define appropriate scheduling criteria for the User Daily jobs. It is often useful to define User Daily jobs in such a way that they are scheduled to run sequentially, not concurrently.

Defining jobs that use ctmorder to schedule other jobs

You can use the ctmorder utility in any of several ways to order or force jobs from a scheduling table. You can:

- manually run the utility
- define a job to run the utility (this job can be run by the SYSTEM User Daily)

Usage of the ctmorder utility is described in the *CONTROL-M Utility Guide*. For information on defining jobs, see the chapter on defining jobs in the *CONTROL-M User Guide*.

Handling interruptions in User Daily job processing

If a User Daily job is interrupted for any reason (for example, operating system crashes, User Daily job errors), the ctmudchk utility can determine which jobs in the affected user daily ended okay, which jobs had interruptions, and which jobs had not yet run.

You will have to examine the outputs and logs related to the jobs that were in process to decide what to do, but the utility can reorder the jobs that did not yet run.

To handle an interruption in User Daily processing

Run the ctmudchk utility for the affected User Daily to order jobs that were not ordered because of the interruption.

Before ordering the job, ctmudchk verifies that a job is not already present in the Active Jobs file.

The CONTROL-M Main Menu options enables you to access a variety of functions and utilities used to maintain CONTROL-M/Server.
Collecting and viewing application server information

You can use the ctmgetcm utility (in batch or interactively) to collect and display application server information from CONTROL-M/Agent computers. (For details on running the utility in batch, see the CONTROL-M Utility Guide.)

**To collect and view application server information interactively**

1. Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. In the CONTROL-M Main menu, enter the number for the View NodeID details option. This invokes the ctmgetcm utility interactively.

3. At the prompts, enter the following information:
   - Node ID—Host name of the agent computer.
   - Application type—name of the application server (for example, SAP). You can use a mask character to specify more than one application (for example, O* to retrieve information from OAP_11, OAP_11I, and OS). Specify * to retrieve information from all applications.
   - Action—To collect and display updated information, enter GET. To display previously collected information, enter VIEW.

**NOTE**
CONTROL-M/CM information is updated only after ctmgetcm is run, or each time ctmgetcm is reconfigured.

**Example 1**

You want to view existing information for all applications on the CONTROL-M/Agent sahara computer.

Enter the following information: Node id—sahara; Application type—*; Action—VIEW.
Output similar to the following is displayed:

<table>
<thead>
<tr>
<th>NODEID</th>
<th>APPLTYPE</th>
<th>APPLVER</th>
<th>CMVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>sahara</td>
<td>OS</td>
<td>6.4.01</td>
<td>6.4.01</td>
</tr>
<tr>
<td>sahara</td>
<td>SAP</td>
<td>46C/46D</td>
<td>6.3.01</td>
</tr>
<tr>
<td>sahara</td>
<td>OAP_11</td>
<td>11</td>
<td>6.2.01</td>
</tr>
<tr>
<td>sahara</td>
<td>OAP_11I</td>
<td>11I</td>
<td>6.2.01</td>
</tr>
</tbody>
</table>

Example 2

You want to update the CONTROL-M/Server database with new information for all applications with prefix O on the CONTROL-M/Agent sahara computer (and view the update information).

Enter the following information: Node id—sahara; Application type—O*; Action—GET.

The CONTROL-M/Server database is updated and output similar to the following is displayed:

<table>
<thead>
<tr>
<th>NODEID</th>
<th>APPLTYPE</th>
<th>APPLVER</th>
<th>CMVER</th>
</tr>
</thead>
<tbody>
<tr>
<td>sahara</td>
<td>OS</td>
<td>6.4.01</td>
<td>6.4.01</td>
</tr>
<tr>
<td>sahara</td>
<td>OAP_11</td>
<td>11</td>
<td>6.2.01</td>
</tr>
<tr>
<td>sahara</td>
<td>OAP_11I</td>
<td>11I</td>
<td>6.2.01</td>
</tr>
</tbody>
</table>

Implementing job version management

1. In the CONTROL-M Configuration Manager, choose Tools => System Parameters => CONTROL-M/EM System Parameters to display the CONTROL-M/EM System Parameters window.

2. To define how the job version management should work, for each of the following system parameters, double click the parameter, set its value appropriately, and click Save.

   - VMVersionsNumberToKeep—number of versions of the job to keep, including the current version. Default: 2 (current version, and one history version). BMC Software recommends not setting a value greater than 30 because of possible performance degradation. This parameter is used only after the CONTROL-M Configuration Manager performs cleanup.

   To deactivate version history, set the parameter to 1 (keep current version only).
Implementing job version management

- **VMMaxDaysRetainCurrentJobsHistory**—number of days after which the history of the current jobs should be deleted automatically. Default: 0.

**NOTE**
The CMS deletes a job version only when the limits set in both the VMVersionsNumberToKeep and the VMMaxDaysRetainCurrentJobsHistory system parameters are exceeded.

- **VMNumDaysRetainDeletedJobs**—number of days to retain deleted jobs and their history. Deleted tables will also be deleted according to this value. Default: 180.

- **VMCleanupIntervalMinutes**—interval, in minutes, between activations of automatic job history cleanup. To disable automatic cleanup, set the value to 0. Default: 30.

- **VMAdditionalJobsRelateFields**—If you use the same job name (or mem name, in CONTROL-M for z/OS) for multiple jobs, use this field to identify additional key fields that CONTROL-M/EM can use to distinguish between different jobs with the same name /mem name, so as not to confuse or switch their job histories. Default: <empty>. Recommended key words—some combination of: MEM_LIB, DESCRIPTION, NODE_ID, OWNER, DAYS_CAL, WEEKS_CAL, CONF_CAL, CMD_LINE, FROM_TIME, TO_TIME, ACTIVE_FROM, ACTIVE_TILL. Example: VMAdditionalJobsRelateFields = "DESCRIPTION TIME_FROM"

3 In the CONTROL-M Configuration Manager, refresh the parameters that require manual refresh (VMVersionsNumberToKeep and VMAdditionalJobsRelateFields; the rest of the parameters are automatically refreshed), as follows:

A In the CONTROL-M Configuration Manager, right-click the GUI Server component and choose Control Shell.

B In the Control Shell dialog box, enter the REFRESH_HISTORY command and click Apply.

C Close the dialog box.
Defining quantitative resources, control resources, and global conditions

You must define quantitative resources, control resources, and global prerequisite conditions that are used in your production environment. You perform these tasks from the CONTROL-M/EM GUI.

For instructions on defining, viewing and deleting these items, see the chapter on identifying data center resources to CONTROL-Ms and the chapter on establishing job dependencies across CONTROL-Ms, in the CONTROL-M User Guide.

Modifying the time limit on Global conditions distribution

By default, global conditions are distributed to data centers only within seven days of their defined condition date. You can

- indicate whether or not to limit the distribution of global conditions
- specify a range of days for which global conditions can be distributed
- provide a list of condition dates that are excluded from the limitation process (so that global conditions with these dates are distributed without limitations)

To change the defaults

Modify the values of the parameters listed in Table 6 on page 108. These parameters are defined in the \$HOME\appl\ecs\resource\Defaults.rsc file. The format for parameter settings in the Defaults.rsc file is:

```
group * parameter 'value'
```
Activating scripts with alert data

By default, alert data is sent to SNMP traps. You can define that alert data should activate scripts.

---

Table 6  Parameters for the Global Conditions distribution facility

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>limit_gcs_distrib_activate</code></td>
<td>Enable and Disable limitations on the distribution of global conditions using the Global Conditions Distribution facility. Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ 1 – The Global Conditions Distribution facility distributes global conditions according to limitations defined using the limit_gcs_distrib_max_days and limit_gcs_distrib_disable_dates parameters. Default.</td>
</tr>
<tr>
<td></td>
<td>■ 0 – The Global Conditions Distribution facility imposes no limitations on the distribution of global conditions.</td>
</tr>
<tr>
<td><code>limit_gcs_distrib_max_days</code></td>
<td>Range of days within which conditions can be distributed. Default: 7</td>
</tr>
<tr>
<td></td>
<td><code>limit_gcs_distrib_disable_dates</code></td>
</tr>
</tbody>
</table>

---

**EXAMPLE**

To specify that global conditions can be distributed within 28 days from their original condition date, excluding conditions with special dates that indicate any date (0101 and STAT):

```
namevalue * limit_gcs_distrib_max_days 28
namevalue * limit_gcs_distrib_activate 1
namevalue * limit_gcs_distrib_disable_dates STAT, 0101
```

In this example, global conditions with special dates 0101 and STAT are distributed even after 28 days from their original scheduling date passed. All other global conditions are not distributed after 28 days passed.

---

**EXAMPLE**

To remove all date limitations on the distribution of global conditions:

```
namevalue * limit_gcs_distrib_activate 0
```

---

Activating scripts with alert data
1 Set the **SendSnmp** parameter to one of the following values to indicate where the alert data should be sent:

- 0 — Send data to SNMP only. Default.
- 1 — Send data to script only.
- 2 — Send data to both script and SNMP.

2 If data is to be sent to the SNMP trap, (the value of **SendSnmp** is either 0 or 2):

   A Set the value of the **SendSnmpActive** parameter to 1, or the SNMP data will not be generated and there will be nothing to send to the SNMP trap. (If data is not going to the SNMP trap, the value of the **SendSnmpActive** parameter should be 0. Default.)

   B Identify the SNMP host in the **SnmpHost** parameter. This parameter can contain a single host name, or a list of host names separated by semi-colon (;) delimiters. Specific ports can be set using a colon. For example, `dhost1;jhost2;myhost3:2000`

3 If data will be sent to a script, specify the full path name of the script that is activated when an alert is generated in the **SendaAlarmToScript** parameter. (This script is activated only if the value of **SendSnmp** is either 1 or 2.)

---

**NOTE**

If the file does not exist, a message is displayed on the gateway trace. If the gateway is started with Trace Level 3 (most detailed), a message is displayed when the data is sent to the script.

---

**EXAMPLE**

Example for testing SNMP traps when enabling this parameter:

**On UNIX:**

```
#!/bin/sh
echo $* > /tmp/snmptest.out
```

**On Windows:**

```
echo %1% %2% %3% %4% %5% > c:\snmptest.out
```

**Note:** On Windows, double backslashes should be used as a delimiter.
Implementing time zone support (optional)

NOTE
You need to implement time zone support only if time zone differences between local and remote computers impact job ordering at your site. For more information, see “Time zone support” on page 89.

This section provides the following procedures related to time zone support:

- “Setting up time zone support for jobs”
- “Ensuring correct time zones for jobs in the Active Jobs file” on page 111

Setting up time zone support for jobs

1. Optionally, edit the TimeZone.dat file to add or modify time zone definitions.

   The TimeZone.dat files contain a pre-supplied list of 3-character time zones and their corresponding time offsets from Greenwich Mean Time (GMT). For example, the Eastern Standard Time time zone appears as EST GMT -05:00.

   The location of the TimeZone.dat file is:

   - In CONTROL-M/EM (on Windows only): <HOME>\Data
   - In CONTROL-M/Server: CONTROL-M_ home/data

   NOTE
   - If you edit time zone definitions, ensure that you maintain the same time zone names in CONTROL-M/Server and CONTROL-M/EM time zone files.
   - For Daylight Saving Time support, you can also modify the format of the time zone definitions in the CONTROL-M/Server files (only). For more information, see “Editing definitions to support Daylight Saving Time” on page 112.

2. Ensure that the CONTROL-M/Server on which time zone support is needed has a time zone defined for it. For instructions, see “Defining a CONTROL-M/Server (manual definition method)” on page 57.

3. In the job processing definition of each job that requires time zone support, indicate the time zone according to which the job should run. For instructions, see the job definition chapter of the CONTROL-M User Guide.
Ensuring correct time zones for jobs in the Active Jobs file

Jobs with specified time zones can be ordered as early as 48 hours before their actual run, and they might remain in the Active Jobs file after their specified scheduling date. Because these jobs must normally be ordered from the New Day procedure, an unusually large number of jobs can accumulate in the Active Jobs file for a long period of time, which can result in slower processing. Use this procedure to avoid the problem.

**NOTE**

- BMC Software recommends that you do not combine jobs that have time zone specifications with jobs that do not specify a time zone in the same scheduling table or group scheduling table.

- You must save newly defined jobs with specified time zones at least 48 hours before their intended execution dates to ensure that they are ordered automatically by the appropriate New Day Procedure or User Daily.

If the jobs must run “today,” you should order them manually (for example, by using the ctmorder utility).

1. Create a separate scheduling table for each time zone that you will be using and place the jobs definitions for that time zone in that table.

2. Define a User Daily job (by using the ctmudly utility) for each scheduling table that was created in Step 1.

   - Specify a time for the User daily that corresponds to a time just after the beginning of the working day in that time zone.
   - In the `-odate` parameter, specify the working date for the time zone (usually either the current CONTROL-M/Server working date, or the next day).
   - In the `-odate_option` parameter, specify `run_date`, to indicate that the odate value should be used to determine the working day on which the jobs should run.

Implementing Daylight Saving Time support

You need to implement this only if a CONTROL-M/Server resides in a location that uses Daylight Saving Time (DST). Implement Daylight Saving Time support by editing the `TimeZone.dat` file.
Editing definitions to support Daylight Saving Time

1 Use your text editor to open the TimeZone.dat file in the CONTROL-M_ home/data directory.

2 Change the relevant time zone definition so that it includes Daylight Saving Time adjustments.

Normally, the format for the definition is timeZone (GMT±hh:mm), where timeZone represents the time zone label (for example, the label EST represents the Eastern Standard time zone, and the regularly formatted entry for the Eastern Standard Time time is EST GMT -05:00. Change the format by appending the needed Daylight Saving Time data, so the entry is formatted as follows:

timeZone (GMT±hh:mm) FROM dd.mm hh:mm TO dd.mm hh:mm (GMT±hh:mm)

■ The first part of the entry (timeZone (GMT±hh:mm)) indicates the regular time zone value (for example, CET (GMT+02:00)).

■ The FROM and TO values indicate the time frame during which Daylight Saving Time is in effect. (For example, FROM 01.03 01:59 TO 24.10 02:00)

■ The second GMT value (following the FROM and TO values) indicates the Daylight Saving Time time-offset relative to GMT (for example, (GMT+03:00)).

This syntax is reversed for the southern hemisphere. The FROM and TO keywords specify the start and end settings for daylight saving to take effect.

EXAMPLE

Bill needs to create a new time zone label for Japan, where the time is nine hours later than Greenwich Mean Time (GMT). Daylight Saving Time begins March 1 at 01:59 and ends October 24 at 02:00. Bill uses the following entry to create the new label (JST):

JST (GMT+09:00) FROM 01.03 01:59 TO 24.10 02:00 (GMT+10:00)

EXAMPLE

Although time zone definitions in the northern hemisphere are set to summer Daylight Saving Time, definitions in the southern hemisphere are set to winter. In Sydney, Australia, winter time (GMT+09:00) is from March 25 at 03:00 until October 1 at 02:00. All other dates are GMT+10:00 (summer time). The time label for Sydney is defined as follows:

SYD (GMT+10:00) FROM 25.03 03:00 TO 01.10. 02:00 (GMT+09:00)

3 If a relevant time zone contains several countries, some of which observe Daylight Saving Time and some of which do not (or if they change the clock on different days), add additional time zone definitions to cover the variations.
Be sure to update the relevant job processing definitions, using the appropriate variations.

---

**NOTE**

If you delete a time zone from `TimeZone.dat` or modify a three-character name in that file, be sure to change any job processing definitions that specify that time zone. Otherwise, those job processing definitions will be invalid.

---

**Implementing load balancing (node groups)**

This section provides the following procedures for implementing load balancing:

- “Defining and maintaining a node group” on page 113
- “Identifying jobs that can be load balanced” on page 115

---

**Defining and maintaining a node group**

---

**NOTE**

You can also perform the functions listed in this section using the `ctmnodegrp` utility. For details, see the CONTROL-M Utility Guide.

---

**To view the list of node groups and their node ids for a CONTROL-M/Server**

1. In the CONTROL-M Configuration Manager, choose **Tools => Node Group Management**. The Node Group Management window for CONTROL-M/Server is displayed.

2. In the **CONTROL-M/Server** field, select the relevant CONTROL-M/Server. The window displays a tree of the node groups and their node IDs for the CONTROL-M.

**To add or modify a node group**

1. In the CONTROL-M Configuration Manager, choose **Tools => Node Group Management**. The Node Group Management window for CONTROL-M/Server is displayed.

2. In the **CONTROL-M/Server** field, select the relevant CONTROL-M/Server. The window displays a tree of the node groups and their node IDs for the CONTROL-M.
Defining and maintaining a node group

3 Perform either of the following:

■ To add a node group, in the Node Group Management window, click (Add Node Group).

■ To modify the properties of an existing node group, click (Update Node Group).

4 Fill in, or modify as needed, the values in the node group properties dialog box:

A Specify the node group name and select the application type. (Select the OS application type if the node group is not for third-party applications.)

B Perform the following as needed:

■ To add node IDs to the node group, select the node IDs in the Disassociated Node ID field and click the right arrow to move them to the Associated Node ID field.

■ To add and associate a node ID that is not yet defined in the enterprise, specify the name (maximum: 50 characters) in the New Node ID field and click the right arrow.

■ To remove (disassociate) node IDs from the node group, select the node IDs in the Associated Node ID field and click the left arrow to move them to the Disassociated Node ID field.

5 When done, click OK. CONTROL-M is immediately updated with the changes.

To delete a node group

1 In the CONTROL-M Configuration Manager, choose Tools => Node Group Management. The Node Group Management window for CONTROL-M/Servers is displayed.

2 In the CONTROL-M/Server field, select the relevant CONTROL-M/Server. The window displays a tree of the node groups and their node IDs for the CONTROL-M.

3 In the tree, select the node group and click (Delete).

All node IDs are disassociated from the node group and the node group is deleted.
To disassociate a node ID from its node group

1 In the CONTROL-M Configuration Manager, choose **Tools => Node Group Management**. The Node Group Management window for CONTROL-M/Servers is displayed.

2 In the **CONTROL-M/Server** field, select the relevant CONTROL-M/Server. The window displays a tree of the node groups and their node IDs for the CONTROL-M.

3 In the tree, select the node ID and click ![Disassociate Node ID](image). (Disassociate Node ID).

*NOTE*
- If you disassociate the last remaining node ID from a node group, the node group is also deleted.
- You can disassociate all node IDs from a node group by deleting the node group. For instructions, see “To delete a node group” on page 114

Identifying jobs that can be load balanced

If a job should be load balanced, you identify the load balance group to which it belongs (rather than a specific computer Node ID for execution) in its job processing definition.

To enable the job to be included in the load balancing algorithm

In the **Node ID/Group** field in the Execution tab, select the group. (If the groups do not appear in the selection list, click **Load**; then select the group.)

For instructions on defining job processing definitions, see the **CONTROL-M User Guide**.

Setting up Shout Destination Tables

The Shout Destination table contains a list of logical destinations and the equivalent physical destination of each logical destination.

You can create any number of Shout Destination tables, but only one of them can be designated as the **active** Shout Destination table at any given time. By changing the designation of the active table, you can change the actual recipients of messages sent to specific logical recipients.
Defining and maintaining Shout Destination tables

This section explains

- how to define and maintain Shout Destination tables
- how to make a particular Shout Destination table the active one

Defining and maintaining Shout Destination tables

You define and maintain Shout Destination tables by means of the ctmsys utility. (This utility is also used to define system parameters.) This section provides the following procedures:

- “To display the Shout Destination Tables menu of the ctmsys utility” on page 116
- “To create or modify a shout destination table” on page 117
- “To change the active shout destination table” on page 119
- “To list existing shout destination tables” on page 120
- “To delete an existing shout destination table by name” on page 120

To display the Shout Destination Tables menu of the ctmsys utility

1. Display the CONTROL-M System Maintenance Utility Main Menu (ctmsys). For instructions on displaying the menu, see “Using the CONTROL-M System Maintenance Utility Main Menu” on page 47.

2. In the CONTROL-M System Maintenance Utility Main Menu, enter the number of the Shout Destination Tables option.

   Shout Destination Tables Menu
   -----------------------------
   Active Shout Destination Table: <table_name>

   1) Create/Modify a Table
   2) Set Active Table
   3) List Tables
   4) Delete Table
   q) Quit and return to main menu

   Enter option:

   The name of the currently-active Shout Destination table is displayed in the <table_name> field on the menu.
**To create or modify a shout destination table**

1. Enter the number of the Create/Modify a Table option.

A list of available tables, similar to the following, is displayed:

```
Shout Destination Tables
------------------------
SYSTEM
NIGHT_SHIFT
Table to create/modify or 'q' to quit [SYSTEM]:
```

2. Enter the name of the table to be created or modified (or press <Enter> to accept the default).

(If the name you specify is not the name of an existing Shout Destination table, a new table will be created with the specified name.)

A display similar to the following is displayed. For an existing table, the display lists the defined destinations.

```
Shout Destination Table 'SYSTEM'
--------------------------------
#  Destination Type  Addr  Logical Name  Physical Name
-  ----------------  ----  ------------  -------------
1  E                 S     EM
2  T                 S     Term_B   $TTB.#B
q) Quit  e#) Edit entry #  n) New entry  d#) Delete entry #
```

Enter option:

Table 7 describes the fields and valid values of the Shout Destination table.

**Table 7  Fields and values of the Shout Destination table (part 1 of 2)**

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>#</td>
<td>Entry number in the table.</td>
</tr>
</tbody>
</table>
To create a new entry in the table

A Specify n.

The following prompts appear:

Dest. Type: (U)ser (M)ail (T)erminal c(O)nsole (L)og
(P)rogram CONTROL-M/(E)M:

B Specify the letter corresponding to the desired destination type.

The following prompt is displayed:

Address Type (S)erver or (A)gent:
C For Destination types U, M, P, T, or O, specify whether the destination is on the server (S) or agent (A). For Destination type E, specify S.

D At the Logical Name prompt, specify the logical name for this destination.

The following prompt is displayed:

Physical Name:

E For Destination types U, M, P, or T, specify the physical name. For Destination types O and E, leave this field blank.

The new entry is added to the table.

4 To modify an existing entry (physical name only) in the table

A Specify e<entry_number>. For example, to modify entry number 2, specify e2.

The following prompt is displayed:

Dest Type:
Address Type:
Physical Name:

This option cannot be used to modify a logical name.

B Specify a new physical name for the entry. The table is redisplayed with the modified entry.

5 To delete an existing entry in the table

A Specify d<entry/Number>. For example, to delete entry # 2, specify d2.

The entry is deleted.

6 Specify q to return to the Shout Destination Tables menu.

To change the active shout destination table

1 Select Option 2 from the Shout Destination Tables menu.

A list similar to the following is displayed:

<table>
<thead>
<tr>
<th>Existing Shout Destination Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
</tr>
</tbody>
</table>
Defining and maintaining Shout Destination tables

1. Specify the name of the table to set as the active Shout Destination table.

   The following message is displayed:

<table>
<thead>
<tr>
<th>NIGHT_SHIFT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter name of table to make active or q to quit [SYSTEM]:</td>
</tr>
</tbody>
</table>

2. Press <Enter> to return to the Shout Destination Tables menu.

   The active Shout Destination table is changed immediately, affecting **Shout** and **Do Shout** operations performed by CONTROL-M.

   **NOTE**

   To specify the active Shout Destination table using a job, run the ctmshb utility, described in the **CONTROL-M Utility Guide**.

---

**To list existing shout destination tables**

1. Select Option 3 from the Shout Destination Tables menu.

   A list similar to the following is displayed:

<table>
<thead>
<tr>
<th>Shout Destination Tables</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSTEM</td>
</tr>
<tr>
<td>NIGHT_SHIFT</td>
</tr>
</tbody>
</table>

2. Press <Enter> to return to the Shout Destination Tables menu.

**To delete an existing shout destination table by name**

1. Select Option 4 from the Shout Destination Tables menu.

   A list of existing Shout Destination Tables is displayed.

2. Specify the name of the table to delete.

   The following message is displayed:
Delete completed successfully.
Press ENTER to continue.

3 Press <Enter> to return to the Shout Destination Tables menu.

NOTE
It is not possible to delete the active Shout Destination table.

Making a Shout Destination table the currently active table

Enter the following command to invoke the ctmshlb utility. (Set the variable <table> to the name of the Shout Destination table name that should become current.)

ctmshlb <table>

TIP
To automate the process of making different Shout Destination Tables current at different times (for example to automatically change between a Dayshift and Nightshift Shout Destination Table), define CONTROL-M jobs to execute this utility at the required times.

Modifying CONTROL-M/EM periodic statistic retention and cleanup defaults

By default, the CONTROL-M/EM periodic statistics feature

- ignores those job run instances with the 2 highest and 2 lowest elapsed run times
- retains a maximum sample of 20 periodic statistics per job
- retains periodic statistics for 100 days
- performs purge of those periodic statistics whose retention period has passed every 30 minutes.

You can change these defaults.
Implementing job statistics generated by CONTROL-M/Server

1 In the CONTROL-M Configuration Manager, choose Tools => System Parameters => CONTROL-M/EM System Parameters to display the CONTROL-M/EM System Parameters window.

2 To modify periodic statistic cleanup defaults, double click the system parameter you are modifying, set its value appropriately, and click Save. Both of the following parameters are CONTROL-M/EM system parameters of the CMS type.

- **RunInfoIgnoreDevCnt**—Number of highest and number of lowest elapsed run time job instances to ignore when collecting periodic statistics. For example, a value of 2 will result in the two job run instances with the highest elapsed runtimes, and the two job run instances with the lowest elapsed runtimes, being ignored when statistics are collected. Default: 2. Parameter type: Gateway.

- **RunInfoMaxSamples**—maximum number of run samples to be kept per job. Default: 20. Parameter type: Gateway.

- **RunInfoStatsPurgeDays**—number of days to retain statistics, after which the statistics will be deleted when automatic purge is performed. Default: 100. Parameter type: CMS.

- **RunInfoStatsPurgeInterval**—interval, in minutes, between activations of automatic purging of periodic statistics the CMS. Default: 30.

To disable automatic purging, set the value to 0.

Implementing job statistics generated by CONTROL-M/Server

This section provides the following procedures for setting up your environment to record, compile, and use CONTROL-M/Server job statistics:

- “Setting whether CONTROL-M/Server collects job statistics” on page 122
- “Defining the CONTROL-M/Server statistics collection mode” on page 123
- “Ensuring that the ctmjsa utility runs daily to collect CONTROL-M/Server statistics” on page 124
- “Displaying (or deleting) CONTROL-M/Server statistics as needed” on page 125

Setting whether CONTROL-M/Server collects job statistics

Whether or not CONTROL-M/Server collects job statistics is determined by the value of the Statistics parameter.
By default, CONTROL-M/Server collects job statistics. If this default has been changed but you want CONTROL-M/Server to collect statistics, or if you do not want CONTROL-M/Server to collect statistics, you need to modify the values of this parameter.

- If CONTROL-M/Server should collect statistics, ensure that the Statistics parameter is set to Y. (default)
- If CONTROL-M/Server should not collect statistics, ensure that the Statistics parameter is set to N.

To set the Statistics system parameter

1. Display the CONTROL-M System Maintenance Utility main menu. For instructions on displaying the menu, see “Using the CONTROL-M System Maintenance Utility Main Menu” on page 47.

2. In the CONTROL-M System Maintenance Utility main menu, enter the number for the System Parameters option.

3. In the System Parameters page, do the following as needed
   
   A. If the Statistics parameter is not displayed, enter N (Next) to display the next System Parameters page, until the Statistics parameter is displayed.

   B. If the Statistics parameter is set to Y, enter C (Cancel) to exit the page without making changes.

   C. If the Statistics parameter is set to N
      1. Enter the option number of the Statistics parameter.
      2. At the prompt, enter Y to change the value of the parameter to Y.
      3. Enter S to save the changes.

4. In the main menu, enter q to exit the menu.

Defining the CONTROL-M/Server statistics collection mode

The CONTROL-M operational parameter Statistics Mode indicates the mode used by the ctmjsa utility to collect summary statistics. You set and modify operational parameters using the Parameter Customization menu in the CONTROL-M Menu system.
To set the CONTROL-M Statistics Mode operational parameter

1. Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. In the CONTROL-M Main menu, enter the number for the Parameter Customization menu option, which is used to maintain various groups of CONTROL-M/Server parameters.

3. In the Parameter customization menu, enter the number for the Advanced Communication and Operational Parameter option.

4. In the Advanced Communication and Operational Parameter menu, enter the number for the Statistics Mode parameter.

5. Enter one of the following values, as appropriate, for the Statistics Mode:
   - To compile statistics for each CONTROL-M Job Name, Scheduling table, and Node ID where the job was submitted, enter JOBNAME.
   - To compile statistics for each CONTROL-M Mem Name/Mem Lib and Node ID, enter MEMNAME (default).

6. When you are done, enter q to quit.

Ensuring that the ctmjsa utility runs daily to collect CONTROL-M/Server statistics

The CONTROL-M ctmjsa utility compiles the data in the Statistical Details table and store the results in a Statistical Summary table in the CONTROL-M/Server database.

To help ensure that the CONTROL-M/Server database contains current statistics on all jobs that are executed under CONTROL-M, you should ensure that the ctmjsa utility runs on a daily basis.

**TIP**

BMC Software recommends that you define a CONTROL-M job to run the ctmjsa utility on a daily basis.

A partial cleanup of the Statistical Details table is performed by the New Day procedure.
Displaying (or deleting) CONTROL-M/Server statistics as needed

You can use the following utilities to display (and delete) statistical data:

- The ctmruninf utility displays and deletes data from the Statistical Details table.
- The ctmstats utility displays and deletes data from the Statistical Summary table.

Both utilities can be filtered according to date and job information.

For information regarding usage of these utilities, see the utility descriptions in the CONTROL-M Utility Guide.

Displaying empty Group scheduling tables in ViewPoints

By default, when a scheduling group but no jobs in a group scheduling table satisfy ViewPoint filtering criteria, the GUI server does not display the Group scheduling table in the ViewPoint. You can override this default for all users or for specific users.

To override the default so that “empty” Group scheduling tables are displayed for all users

Set the value of the ViewpointPolicy system parameter to SELECT_JOBS_AND_SG.

(To filter out the “empty” group scheduling tables, reset the ViewpointPolicy system parameter to its default value: SELECT_JOBS.)

NOTE
If ViewpointPolicy is set to SELECT_JOBS_AND_SG, users can still hide any empty group scheduling tables displayed in the ViewPoint by choosing the Hide Empty Scheduling Groups option from the View menu in CONTROL-M/EM.

To set whether empty group scheduling tables are displayed for specific users

1 In the CONTROL-M Configuration Manager, choose Tools => System Parameters. The CONTROL-M/EM System Parameters window is displayed.

2 Locate the ViewPointPolicy system parameter, and click New.
Ensuring that Collection data is retrieved at startup

3 In the **Component Name** field, specify the user name for which different behavior is required.

**NOTE**
For other system parameters, **Comp. Name** identifies the data center. For the **ViewpointPolicy** system parameter, **Comp. Name** indicates the user names of the exceptions.

4 Ensure that the **Value** field is defined as required for this specific user, and click **Save**.

Ensuring that Collection data is retrieved at startup

Collection data that is retrieved on startup and retained in memory is called pinned data. You can specify the collection names that are pinned in the default `pin_collection.ini` configuration file in the `ini` folder or directory.

**NOTE**
You can override this default file for any GUI Server by creating a `pin_collection.{Logical_Name}.ini` file in the same `ini` folder or directory.

1 Navigate to the `ini` folder or directory, and open the `pin_collection.{Logical_Name}.ini` for editing.

**NOTE**
Ensure that each collection name is specified in the `pin_collection.{Logical_Name}.ini` file on a separate line.

2 After being configured, the `ctl` and `rsi` utilities can be used to dynamically modify which collections are pinned (for more information, see the CONTROL-M Utility Guide). When using these utilities, the following commands are relevant:

- **CPIN** – pins the specified collections.
- **CUNPIN** – unpins the specified collections.
Detecting file activity with FileWatcher (ctmfw)

NOTE
The CPIN and CUNPIN commands only affect the currently running GUI server. If you want your settings to remain after the server ends its current run, you should specify whichever is applicable of these commands in the pin_collection.[Logical_Name].ini file.

- PPINNED – prints out the current pinned collections.

As a service, ctmfw takes its parameters (rules) during startup from the rull.dat file whose full path name is specified in <CONTROL-M/Agent>\data\ctmfw.cfg.

To change one or more rules, change the contents of the rull.dat file or specify the full path name of a different file.

NOTE
The rull.dat file provided with CONTROL-M/Agent is a sample file and should be changed to reflect your requirements.

The full path name to the ctmfw.cfg configuration file must be specified under the following Microsoft Windows registry key that is generated automatically by the installation script:

HKEY_LOCAL_MACHINE\SOFTWARE\BMC Software\CONTROL-M/FileWatcher\SYSPRM\File Watcher Configuration File

The default value for this key is

<CONTROL-M/Agent_install_directory>\DATA\ctmfw.cfg

NOTE
This section describes how to use ctmfw as a service. You can also run ctmfw as a utility. For more information, see the CONTROL-M Utility Guide.
The configuration file must contain the following line:
-\texttt{input <ruleFileName>}

The variable \texttt{<ruleFileName>} is the full path name of a rule file containing the FileWatcher rules. The following is a sample rule file.

### Figure 12 Sample Rule.dat file

<table>
<thead>
<tr>
<th>INTERVAL 5</th>
</tr>
</thead>
<tbody>
<tr>
<td>FROM_TIME 0001</td>
</tr>
<tr>
<td>MIN_SIZE 50</td>
</tr>
<tr>
<td>MIN_DETECT 5</td>
</tr>
<tr>
<td>WAIT_TIME 2</td>
</tr>
<tr>
<td>ON_FILEWATCH NONEXIST CREATE 10 3 1</td>
</tr>
<tr>
<td>\texttt{THEN}</td>
</tr>
<tr>
<td>\texttt{DO_CMD } &quot;BAD FILE WAS CREATED IN 1 MINUTE&quot;</td>
</tr>
<tr>
<td>\texttt{DO_COND ON_2 0101 +}</td>
</tr>
<tr>
<td>\texttt{ELSE}</td>
</tr>
<tr>
<td>\texttt{DO_CMD } &quot;GOOD FILE WAS NOT CREATED IN 1 MINUTE&quot;</td>
</tr>
<tr>
<td>\texttt{DO_CMD ctmshout -USER ECS -MESSAGE &quot;Running the Filewatcher on with default configuration!&quot;}</td>
</tr>
<tr>
<td>\texttt{END_ON}</td>
</tr>
</tbody>
</table>

### Network Resources

The FileWatcher service running under the local system account cannot detect network resources (files located on remote systems).

If you want the FileWatcher to detect network resources, configure the FileWatcher Service to run under a regular user account.

### FileWatcher Service Trace

When running as a service, \texttt{ctmfw} generates an execution log file. This file is saved in the CONTROL-M/Agent \texttt{proclog} directory under the following name:

\texttt{U\_CTMFW\_<process_id>.log}

By default, logs in the \texttt{proclog} directory are retained for 3 days. If the “maximum days to retain SYSOUT” parameter is set to a number higher than 3, logs are retained for the number of days specified in that parameter.
Sample trace file

Table 8 briefly describes available CONTROL-M user exits. For more information about each exit, see Appendix C, “Exits.”

Table 8  CONTROL-M General User Exits (part 1 of 2)

<table>
<thead>
<tr>
<th>User Exit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTMUE101 (Job Ordering)</td>
<td>executed for each CONTROL-M job before it is ordered</td>
</tr>
<tr>
<td>CTMUE102 (Job Submission)</td>
<td>executed for each CONTROL-M job before it is submitted for execution</td>
</tr>
<tr>
<td>CTMUE103 (Before New Day Procedure)</td>
<td>executed before the New Day procedure is run</td>
</tr>
</tbody>
</table>
To implement user exits in the CONTROL-M/Server system

1. Decide which user exits you are implementing.

2. Set appropriate values to exit configuration parameters in the `config.dat` file, as explained in the following substeps. This file location is:

   - For UNIX: `<controlmOwner>/ctm_server/data/config.dat`
   - For Windows: `<productDirectory>\ctm_server\data\config.dat`

   **A** To enable CONTROL-M exits, ensure that the value of the `CTM_PRM_ENABLE_UE` parameter is set to `Y` (default).

   **B** Where relevant, enable specific user exits by setting the value of the relevant `CTM_PRM_ENABLE_UEnnn` configuration parameters (where `nnn` is the numeric part of the user exit name, valid values 101-106) to `Y`. (To disable specific user exits, set the value to `N`.) Default: `N`.

   **C** In the `CTM_PRM_TIMEOUT_UEnnn` configuration parameter (where `nnn` is the numeric part of the user exit name, valid values 101-106), set the maximum time to wait for the associated user exit script to run before it is terminated, as follows (default: 20):

   - For UNIX, time is measured in units of seconds.
   - For Windows, time is measured in units of milliseconds.

3. In the user exit directory, define the scripts for the implemented user exits and assign the scripts default file names in the format:

   - For Unix: `ctm_exitnnn.sh`, (where `nnn` is the numeric part of the user exit name, valid values 101-106).

### Table 8  CONTROL-M General User Exits (part 2 of 2)

<table>
<thead>
<tr>
<th>User Exit</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTMUE104 (After New Day Procedure)</td>
<td>executed after the New Day procedure is run</td>
</tr>
<tr>
<td>CTMUE105 (Before User Daily)</td>
<td>executed before each run of a CONTROL-M User Daily job (except SYSTEM)</td>
</tr>
<tr>
<td>CTMUE106 (After User Daily)</td>
<td>executed after each run of a CONTROL-M User Daily job (except SYSTEM)</td>
</tr>
</tbody>
</table>

---

**NOTE**

A special category of user exits can be defined for the Watchdog facility. For more information, see “Watchdog facility exits” on page 528.
Writing scripts (UNIX only)

When writing a shell script to be run as a CONTROL-M/Server job on an agent computer, you should consider and handle the issues:

- Specifying the shell type
- Factoring in the run-time environment
- Using the On Statement/Code parameter to interpret script lines

BMC Software recommends that you run each script manually to validate the script syntax before running the script under CONTROL-M/Server.

Specifying the shell type

To enable CONTROL-M to recognize the script shell type, specify the shell path (as listed in Table 9) on the first line of the script:

```
#!/ <shell path>
```

<table>
<thead>
<tr>
<th>Shell type</th>
<th>Shell path</th>
<th>Default switch</th>
<th>Other switches</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bourne</td>
<td>/bin/sh</td>
<td>-x</td>
<td>-v/n</td>
</tr>
<tr>
<td>Korn</td>
<td>/bin/ksh</td>
<td>-x</td>
<td>-v/n</td>
</tr>
<tr>
<td>csh</td>
<td>/bin/csh</td>
<td>-v</td>
<td></td>
</tr>
<tr>
<td>tcsh</td>
<td>/bin/tcsh</td>
<td>-v</td>
<td></td>
</tr>
</tbody>
</table>

**NOTE**

The command line of command type jobs must be in Bourne shell syntax only.
Table 10 describes the affect Shell parameter switches have on CONTROL-M/Agent processing.

### Table 10  Shell parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>-x</td>
<td>This parameter causes CONTROL-M/Agent to submit the script as is. The script runs under the specified shell and prints commands and related arguments as they are executed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> In the SYSOUT file, the command arguments contain the value of the variable and not the variable name.</td>
</tr>
<tr>
<td></td>
<td>Each command is prefixed by the ‘+’ sign. This sign is later used during an On statement post-processing phase of the job’s output to distinguish between different commands and their output.</td>
</tr>
<tr>
<td>-v</td>
<td>This parameter causes CONTROL-M/Agent to parse the original script to a temporary script. The script commands are appended with an identifying string. This temporary script is then executed, where the -v switch causes the shell to print each command before its output. The added identifying string is later used during an On statement post-processing phase of the job’s output to distinguish between commands and their output.</td>
</tr>
<tr>
<td>n</td>
<td>This CONTROL-M/Agent-specific flag is used to indicate that the script should be executed as is and no commands will be included in the job’s output. As a result no On-statement processing is possible.</td>
</tr>
</tbody>
</table>

For more information about the different flags, see the example on page 132.

**NOTE**

Arguments specified after the shell name are ignored by CONTROL-M/Agent with the following exception: -x is supported when running a script under the Bourne shell or Korn shell. If -x is specified as an argument after the shell name, it overrides any option set in the CTM_PRM_SH_FLAGS or CTM_PRM_KSH_FLAGS parameters.

### Example

The following script uses the app, dbadmin, and stx111 parameters. The app parameter sets an environment variable. The script uses the dbadmin and stx111 parameters to call a utility that performs an action. The output of the job varies depending on the shell flag.

```
#!/bin/sh
DBNAME=$1
export DBNAME
dbrefresh -U $2 -P $3
exit $?
```
If the `-x` flag was set when running the sample script, the job produces the following output.

```bash
DBNAME=app
+ export DBNAME
+ dbrefresh -U dbadmin -P stx111
DB refreshed
+ exit 0
```

If the `-v` flag was set when running the sample script, the job produces the following output.

```bash
#!/bin/sh -v
CTM_RSVD=
CTM_RSVD_START=
CTM_RSVD_END=
CTM0="/home2/ag620/refreshDB.sh"
CTM00=$0
DBNAME=$1 $CTM_RSVD
export DBNAME $CTM_RSVD
dbrefresh -U $2 -P $3 $CTM_RSVD
DB refreshed
exit $? $CTM_RSVD
```

If the `-n` flag was set when running the sample script, the job produces the following output.

```
DB refreshed
```

**Support for REXX-Language scripts**

REXX job scripts are supported on the following computers: AIX, SunOS, and Solaris.

**To activate a REXX script**

1. Ensure the REXX product is installed on the agent computer.
2. Specify the full path under which REXX is installed in the first line of the REXX script.

---

**EXAMPLE**

```bash
#!/usr/local/bin/rxx
```
Factoring in the run-time environment

CONTROL-M runs a job script under the environment specified for the job owner (that is, the user specified in the **Owner** parameter). The environment affects these factors in the execution of the script:

- Establishing the User log on process
- Establishing the shell script startup process
- Indicating the Working directory

Each of these factors is described below.

**Establishing the User log on process**

As jobs are submitted for execution, CONTROL-M/Agent logs on as the user and executes the job (the shell script) using the following command:

```
su - <owner> -c <script name>
```

During the logon process, the user environment is set according to the shell type specified in `/etc/passwd`.

**Establishing the shell script startup process**

The startup process for running the script depends upon the type of shell under which the script will run.

- When a csh or tcsh script is run, the `.cshrc` file of the job owner is executed as part of the startup process for the script.

- For all other shell types, the `.profile` file of the job owner is executed as part of the startup process for the script.

**NOTE**

The `.login` file is not executed as part of the startup process.
1 When CONTROL-M executes job scripts, there is no terminal associated with the job. Therefore, do not use commands in a script that query terminal characteristics or take input from a terminal.

2 The shell script startup process sets the environment variables that will be available when the script is run. Use the `#!` statement to indicate the shell under which the script is intended to run.

**Indicating the Working directory**

The working directory at the time the script runs is initially set to the home directory of the job owner (the home directory for each user is set by the UNIX administrator in `/etc/passwd`).

When writing scripts that access files, specify the file name in the script with a full path or with a path relative to the home directory of the job owner.

**Using the On Statement/Code parameter to interpret script lines**

The following items describe how the **On Statement/Code** job processing parameter interprets script lines.

- **Type of Script Statement**

  Depending on the shell used, CONTROL-M/Agent does not process certain types of script statements for comparison with the text specified in the `Stmt` subparameter of the **On Statement/Code** parameter.

  Therefore, in the `Stmt` subparameter, do not specify text contained in the following script statements:

  — For a Bourne shell, text in `if`, `for`, `while`, and `case` statements.
  — For a csh shell, text in `if` statements.

  **EXAMPLE**
  
  No part of the following script line should be used in the `Stmt` subparameter of the **On Statement/Code** parameter:
  
  ```
  if [ ‘baseline’ - eq 0 ]; then
  ```
Therefore, in the **Stmt** subparameter do not specify text that is on a script continuation line.

### Length of Script Statement

CONTROL-M/Agent only processes the first 132 characters of a script statement for comparison with the text specified in the **Stmt** subparameter of the **On Statement/Code** parameter.

Therefore, in the **Stmt** subparameter do not specify text that occurs after the first 132 characters of a script statement.

### HERE Documents

The term HERE document refers to lines of text in a script that are passed to a command as input, but are not passed to the shell.

The current version of CONTROL-M/Agent does not support the **On Statement/Code** job processing parameter for HERE documents.

---

**EXAMPLE**

In the following script, **line 1** and **line 2** of a **HERE** document are passed to the specified **cat** command:

```plaintext
cat > /tmp/junk << EOF_EOF
line 1
line 2
EOF_EOF
echo "DONE"
```

For more information about the **On Statement/Code** parameter, see the **CONTROL-M Parameter Guide**. Job processing parameters are described in the **CONTROL-M User Guide**.

### Ensuring utilization of Exit Codes by CONTROL-M/Server

To cause CONTROL-M/Server to distinguish between different exit codes, use the following expression in the **Code** subparameter of the **On Statement/Code** job processing parameter:

```
COMPSTAT=<value>
```

<value> is the exit code of the script.
Using the On Statement/Code parameter to interpret script lines

Assume that a script exits with an exit code of 5.
This condition can be detected by defining the following On Statement/Code parameters:
Stmt: *
Code: COMPSTAT=5

Using the $0 Reserved Variable

The $0 reserved variable can be used in a script to retrieve the name of the script. This variable is automatically replaced by a file name before the script is run.

When a script runs as a CONTROL-M/Server job using the –v flag (see Specifying the shell type), it is parsed into a temporary script. In this case, any reference to $0 in the script is resolved to the temporary script name rather than the original script name, and the name of the original script is saved in the CTM0 variable. This differentiates between a script run from the command line run and a script run from a CONTROL-M/Server job.

To ensure that the $0 variable resolves to the original name as run from the command line, not the temporary script name, set the Translate_$0 flag using the CONTROL-M Configuration Manager. For more information, see “Modifying CONTROL-M/Agent system parameters” on page 409.

Setting the flag causes CONTROL-M/Agent to replace any occurrence of $0 in the original script with $CTM0 when it parses the original script to the temporary script. This will restore the original functionality of the script as if it ran from the command line.

The following example shows the dollar0.sh script, which is supposed to print out the script name.

--- EXAMPLE ---
#!/bin/sh
echo $0
--- EXAMPLE ---

When the script runs as part of a CONTROL-M/Server job using the -v flag, the name of the temporary script is printed.

--- EXAMPLE ---
#!/bin/sh -v
CTM_RSVD=
CTM_RSVD_START=
CTM_RSVD_END=
CTM0='''/home/ag620/dollar0.sh'''
CTM00=$0
echo $0 $CTM_RSVD
/tmp/ctm/CM_SH.11939
--- EXAMPLE ---
When the script runs in a CONTROL-M/Server job using the \(-v\) flag and the Translate_$0 flag is set, the name of the original script is printed.

```bash
#!/bin/sh -v
CTM_RSVD=
CTM_RSVD_START=
CTM_RSVD_END=
CTM0=\'/home/ag620/dollar0.sh\'
CTM00=$0
echo $CTM0 $CTM_RSVD
/home/ag6220/dollar0.sh
```

**Writing scripts (Windows only)**

When operating in the Microsoft Windows environment, CONTROL-M/Agent can run any type of job scripts (vbs, perl, DOS bat or cmd, Rexx, and so on).

To correctly implement scripts for Windows, you need to consider and handle the following factors:

- Implementing basic guidelines
- Using On Statement/Code parameters correctly
- Enabling CONTROL-M/Server to distinguish between exit codes
- Using script utilities
- Translating DOS files and REXX scripts to UNC

**Implementing basic guidelines**

You must do the following to scripts analyzed by CONTROL-M/Server as part of the post-processing of a job:

1. Begin the script with the `echo on` command.
   
   This step ensures that job script statements will be written to the SYSOUT file.

2. End each prompt with the `>` or `J` character.
   
   These characters and embedded spaces should not be used inside the prompt text string.
Using On Statement/Code parameters correctly

CONTROL-M/Agent can use the On Statement/Code job processing parameters to perform post-processing analysis of the SYSOUT of jobs that are submitted by using these scripts.

The following items describe how the On Statement/Code job processing parameter interprets script lines:

- **Analysis of the Sysout for On Statement/Code**

  Text in a SYSOUT file that follows a > prompt or ] prompt is treated by CONTROL-M/Server as part of the job script. All other text is treated as part of the operating system response.

  When specifying an On Statement/Code statement (format 1) in a job processing definition, place text that follows either of these prompts in the Stmt parameter. Place other text in the Code parameter.

- **Continuation Lines**

  CONTROL-M/Server does not process continuation lines for comparison with text in a Stmt subparameter.

  Therefore, do not specify script continuation line text in the Stmt subparameter.

- **Length of script statement**

  CONTROL-M/Server compares the first 512 characters of a script statement with the text in subparameter Stmt.

  Therefore, in subparameter Stmt, do not specify text that comes after the first 512 characters of a script statement.

  The maximum length of the On Code parameter is 1024 characters.

For more information about the On Statement/Code parameter, see Chapter 7 of the CONTROL-M Parameter Guide. Job processing parameters are described in Chapter 5 of the CONTROL-M User Guide.
Enabling CONTROL-M/Server to distinguish between exit codes

Both DOS .bat scripts and REXX .cmd scripts can return an exit code to CONTROL-M/Server upon completion. The _exit utility described below is used by .bat scripts.

To enable CONTROL-M/Server to distinguish between exit codes, use the following expression in the Code subparameter of the On Statement/Code job processing parameter:

\[
\text{COMPSTAT} = \langle \text{value} \rangle
\]

**Example**

In this example, a REXX script exits with an exit code of 5, as shown below:

```
exit 5
```

This condition can be detected by defining the following On Statement/Code parameter:

```
Stmt: *
Code: COMPSTAT=5
```

**Using script utilities**

The _exit and _sleep script utilities can be accessed from within job scripts. These utilities are located in the `<CONTRL-M/Agent>\EXE` directory under the Product directory, for example:

```
c:\Program Files\BMC Software\CONTRL-M Agent\<agent name>\EXE
```

If this directory is not defined as part of the operating system search path, specify the full path when using one of these utilities.
_exit utility

This utility is similar to the UNIX exit built-in shell function.

**Format**

```
_exit [<exit code>]
```

The variable <exit code> is any integer. Default: 0

The program exits with %errorlevel% = <exit code>

**Examples**

- `_exit 0` in a script causes the job to end with `%errorlevel% 0`.

  ```
  ctmcreate -tasktype command -cmdline "_exit 0"
  ```

- `_exit 1` in a script causes the job to end with `%errorlevel% 1`.

  ```
  ctmcreate -tasktype command -cmdline "_exit 1"
  ```

_sleep utility

This utility is similar to the UNIX sleep built-in shell function.

**Format**

```
"... _sleep" <seconds>
```

The <seconds> variable is any integer.

**NOTE**

If _sleep is specified, you must specify a whole integer number.

**Example**

Suspend execution of the script for 5 seconds.

```
ctmcreate -tasktype command -cmdline "_sleep 5"
```
Translating DOS files and REXX scripts to UNC

The CTMBAT2UNC utility translates DOS batch files (.bat) and REXX-language (.cmd) scripts containing mapped path names into scripts that use Universal Naming Convention (UNC) equivalents, to reference remote disk resources. These translated scripts enable CONTROL-M/Agent to execute multiple scripts simultaneously.

The owners of the jobs do not have to be logged on to provide the drive mappings for the scripts.

Use the following command to invoke the CTMBAT2UNC utility:

```
ctmbat2unc.exe <batch_file_to_translate> <output_file_name>
```

Table 11 describes the CTMBAT2UNC utility parameters.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;batch_file_to_translate&gt;</td>
<td>Original .bat or .cmd script</td>
</tr>
<tr>
<td>&lt;output_file_name&gt;</td>
<td>New script after translation</td>
</tr>
</tbody>
</table>

Example

Two job owners, A and B, are executing ScriptA.bat and ScriptB.bat, respectively. Owner A has drive M mapped to \nt-A\share. Owner B has drive M mapped to \nt-B\share.

Table 12 describes these scripts before and after executing the CTMBAT2UNC utility.

<table>
<thead>
<tr>
<th>Owner</th>
<th>Original script</th>
<th>Translated script</th>
</tr>
</thead>
<tbody>
<tr>
<td>A</td>
<td>@echo off</td>
<td>@echo off</td>
</tr>
<tr>
<td></td>
<td>dir M:\jobs</td>
<td>REM Following line was changed by</td>
</tr>
<tr>
<td></td>
<td>dir \nt-A\share\jobs</td>
<td>CTMBAT2UNC</td>
</tr>
<tr>
<td>B</td>
<td>@echo off</td>
<td>@echo off</td>
</tr>
<tr>
<td></td>
<td>dir M:\jobs</td>
<td>REM Following line was changed by</td>
</tr>
<tr>
<td></td>
<td>dir \nt-B\share\jobs</td>
<td>CTMBAT2UNC</td>
</tr>
</tbody>
</table>

As shown above, every line changed by the CTMBAT2UNC utility is marked by a REM comment inserted before the translated line.
NOTE

Under the current version of Microsoft Windows, command interpreters do not change a
current directory to a UNC path (for example, cd \nt-A\share\jobs will not be
executed).

BMC Software recommends that you review the translated script after invoking the
cmbat2unc utility.
Implementing security and high availability

This part presents the following topics:

Chapter 4
Introduction to implementing CONTROL-M security ........................................ 147

Chapter 5
Setting up CONTROL-M authentication security .............................................. 149

Chapter 6
Setting up CONTROL-M authorization security .............................................. 177

Chapter 7
Implementing CONTROL-M security auditing .............................................. 211

Chapter 8
Setting up CONTROL-M firewall security .................................................... 217

Chapter 9
Configuring CONTROL-M for high availability ........................................... 227
Chapter 4 Introduction to implementing CONTROL-M security

This chapter presents the following topics:

Basic CONTROL-M security concepts ............................................. 147
Security flow ............................................................................. 148

Basic CONTROL-M security concepts

To keep all CONTROL-M components secure, CONTROL-M integrates several different types of security:

■ *Authentication security* checks and validates the user’s identity.

■ *Authorization security* checks whether the user is authorized to access the requested components and to perform the requested actions.

■ *Auditing security* flags problematic user actions and threats to the system.

■ *Firewall security* enables components to communicate securely through a firewall.

With the exception of firewall security, the different types of security are implemented in an integrated flow that encompasses CONTROL-M/EM, CONTROL-M/Server, and CONTROL-M/Agent.
Security flow

1. CONTROL-M requests a user password to authenticate the user.

2. After authenticating the user, CONTROL-M checks authorization on the CONTROL-M/EM side to confirm that the user is authorized to perform the requested operation (for example, hold or rerun) on the requested object (for example, a job, resource, or ViewPoint).

3. If authorization is granted on the CONTROL-M/EM side, CONTROL-M checks for authorization on the CONTROL-M/Server (and CONTROL-M for z/OS) side. (For information regarding security for CONTROL-M for z/OS, see the INCONTROL for z/OS Administrator Guide.)

   (Implementation of CONTROL-M/Server is often unnecessary. For information on when you might want to implement CONTROL-M/EM security, see “CONTROL-M/Server authorization security” on page 180.)

Some operations can also require authorizations in both CONTROL-M/EM and CONTROL-M/Server. For example, to hold a job, a user must be authorized in CONTROL-M/EM to access that job, and in CONTROL-M/Server to hold jobs for the associated job owner.

4. CONTROL-M/Agents, which actually process the jobs, use operating system security.

   **NOTE**
   
   If you use CONTROL-M at a z/OS site, CONTROL-M security also interacts with the external security tools that are used at the site (such as RACF, ACF2/SAF, and TOP SECRET).

5. Auditing security watches for and flags any problematic user actions or prohibited attempts to access CONTROL-M components and scheduling entities.

   **NOTE**
   
   Firewall security is implemented for communication between components and, as such, is outside this flow.
Setting up CONTROL-M authentication security

Chapter 5

Conceptual overview ................................................. 150
Authentication methods .............................................. 151
Password requirements and expiration warnings ............. 152
Administrator passwords ............................................. 153
Recommended task summary ....................................... 153
Setting the authentication method ................................. 154
  Authenticating CONTROL-M/EM users against an LDAP or Active Directory server ............................................. 155
  Implementing external plug-in authentication .................. 158
Defining password requirements ................................... 160
  Refreshing password-related system parameters .............. 160
  Setting allowable password lengths .............................. 161
  Setting password complexity rules (required character types) ............................................................. 161
  Setting password reuse limits ...................................... 162
  Implementing password expiration policy ....................... 163
  Implementing password policy for all users using the set_pwd_def_lifetime script ........................................... 164
  Setting automatic account locking after consecutive failed logon attempts ................................................. 165
  Unlocking multiple accounts with the unlock_user script ................................................................. 166
Defining users and their authentication criteria to CONTROL-M/EM .......... 166
Manually modifying a user’s password criteria ................. 169
Changing the DBO password ................................. 170
Defining a CONTROL-M/Agent account (Windows only) ........ 170
Defining job owner and authentication settings for CONTROL-M/Agents and remote hosts ................................. 173
**Conceptual overview**

Figure 14 highlights the basic recommended workflow for setting up CONTROL-M authentication security. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 13 on page 154. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

**Figure 14  Recommended workflow for setting up authentication security**
Authentication methods

As part of the logon process, CONTROL-M/EM client components send user name and password information to CONTROL-M/EM server components for authentication. User passwords can be validated internally or externally.

Authentication security and data privacy and protection can be enhanced by using Secure Sockets Layer (SSL) security.

Internal authentication

Internal authentication is performed within the product. It validates a client’s user name and password against information stored in the server. The method of choice for internal authentication is challenge-response.

Challenge-response enables the server to prove a client’s identity over an insecure communication channel without password exposure and without allowing eavesdroppers to pretend to be the user by replaying the authentication packet.

When using challenge-response, the client acquires a challenge (a unique random string for each logon) from the server and uses the challenge to encrypt the user password. The client sends a response (the password encrypted using the challenge) to the server. By knowing the issued challenge, the server can verify that the password matches the user password stored in its database.

You can use SSL to augment challenge-response security.

External authentication

Some sites, especially those using centralized authentication mechanism, prefer to perform their own authentication. CONTROL-M/EM allows those sites to implement a plug-in that replaces CONTROL-M/EM authentication with their own implementation.

External authentication can be performed in several ways:

- LDAP/Active Directory

  LDAP (Lightweight Directory Access Protocol) is an application protocol for querying and modifying directory services running over TCP/IP. Administrators can use the LDAP protocol to authenticate CONTROL-M/EM users. LDAP protocol enables authentication for all types of environments.
Active Directory is a subset of LDAP. It is the distributed directory service that is included with Microsoft Windows 2003 Server. Active Directory provides for centralized, secure management of an entire network by enabling authentication against an Active Directory server.

When using LDAP or Active Directory, you can connect in Secured Socket Layer (SSL) mode. Doing so requires that you configure your LDAP or Active Directory to work with SSL. (For details, see the CONTROL-M SSL Guide.)

- External plug-in enables the site to connect to other external authentication applications. This method requires that you code a shared library to be loaded by CONTROL-M and connected to the external authentication mechanism used at your site.

**Secured Socket Layer (SSL) security**

*SSL security* is a strong authentication method that can provide additional security to whichever authentication method (internal or external) you choose.

- **Client–server authentication**

  Using certificates on the client and server side, SSL authenticates the connection between the client and server components

- **Data protection through encryption**

  SSL’s strong data encryption protects data privacy by preventing unauthorized access.

- **Attack protection through keys**

  By requiring keys that are not available to unauthorized users, SSL also protects the system from deliberate data corruption.

SSL security and its implementation are described in the CONTROL-M SSL Guide.

**Password requirements and expiration warnings**

To enhance password security, you can define several types of password characteristics or requirements. Most are defined using system parameters:

- password length—minimum and maximum password lengths
Administrator passwords

During CONTROL-M/EM installation, a CONTROL-M administrator is defined with full administrator privileges, and a DBO (Database owner) is defined with full DBO privileges. They are assigned the same default passwords. You can assign these entities to the same, or different people, and you can change the passwords accordingly.

You can change the CONTROL-M/EM administrator password as you would for any CONTROL-M/EM user. For instructions on changing the DBO password, see “Changing the DBO password” on page 170.

Recommended task summary

Table 13 lists specific tasks related to each phase of the workflow (Figure 14 on page 150). Subsequent sections provide step-by-step instructions.
Setting the authentication method

The default authentication method is internal authentication using Challenge-response. Use of this method require no further customization.

To implement external authentication using either Active Directory or external plug-in, use either of the following procedures.

- Authenticating CONTROL-M/EM users against an LDAP or Active Directory server
- Implementing external plug-in authentication
Authenticating CONTROL-M/EM users against an LDAP or Active Directory server

1 Log on to the CONTROL-M Configuration Manager.

2 Choose Tools > System Parameters.

3 Prepare the system for External authentication by setting the value of the DirectoryServiceAuth system parameter to PrepExt.

At this stage another authentication method is still in use allowing you to complete CONTROL-M/EM user definitions for external authentication.

4 Define the LDAP or Active Directory parameters for the CONTROL-M/EM users, as follows:

   A From CONTROL-M/EM (or CONTROL-M/Desktop), choose Tools => Authorizations to access the Authorizations window.

   B In the Users tab of the Authorizations window, select a user from the list and click Update or click New to create a new user definition.

   C Enter the user name and domain as they are defined in the LDAP or Active Directory server in the LDAP Directory Service User and Domain Name field.

In the following example, the user em belongs to a group called adminuser, which resides in the domain admins.bmc.com.

--- EXAMPLE ---
em.adminuser@admins.bmc.com

If the user belongs to a specific organizational unit (OU) defined in LDAP or Active Directory, the OU needs to precede the domain separator (@), and must be distinguished using a slash (/).

--- EXAMPLE ---
em.adminuser/org.unit@admins.bmc.com
NOTE
If any part of the user definition in LDAP or Active Directory includes @, /, or . characters, these characters must be preceded by a backslash.

Examples:

- If the group name in LDAP or Active Directory is admin/user, you must define it in CONTROL-M/EM as em.admin\user/org.unit@admins.bmc.com.

- If the user name in LDAP or Active Directory includes initials, for example EU, you must define it in CONTROL-M/EM as emuser EU\..adminuser/org.unit@admins.bmc.com.

5 Define at least one emergency user, if you have not already done so. (Optional step.)

An emergency user is an administrator definition that is especially useful for situations where external authentication is not available. For example, if the LDAP or Active Directory does not work, the emergency user can enter the system and correct the problem or work until the problem is solved.

You define an emergency user as you would any user (see step 4), except that you must also do the following in the General tab of the User Authorizations window:

- Select the Emergency User check box. (This check box is displayed only when external authorization is enabled.)

- Supply and confirm a password (not optional for emergency users).

6 Set the value for the PasswordEncode system parameter to 0 (clear text mode), so that CONTROL-M/EM does not encrypt the password. (External applications, such as LDAP or Active Directory, cannot read passwords if they are encrypted by CONTROL-M/EM.)

7 Enable the external authentication by setting the value of the DirectoryServiceAuth system parameter to On.

NOTE
When the DirectoryServiceAuth system parameter is set to On, the AuthenticationMethod system parameter is ignored.

8 To use the SSL protocol to communicate with LDAP or Active Directory, configure your LDAP or Active Directory to work with SSL. For instructions, see the CONTROL-M SSL Guide. (You can perform this optional step at any time. If you perform it later, ensure that you rerun step 9.)
Authenticating CONTROL-M/EM users against an LDAP or Active Directory server

Chapter 5 Setting up CONTROL-M authentication security

9 Refresh the servers with the changes. For instructions, see “Refreshing LDAP or Active Directory system parameters” on page 157.

Returning to internal authentication from LDAP or Active Directory authentication in CONTROL-M/EM

1 Log on to the CONTROL-M Configuration Manager.

2 Choose Tools > System Parameters.

3 Prepare the system for internal authentication by setting the value of the DirectoryServiceAuth system parameter to PrepInt.

4 Apply passwords for all CONTROL-M/EM users (in the General tab of the User Authorization window).

5 Set the value for the PasswordEncode system parameter to 2 (for challenge-response mode).

6 Enable the external authentication by setting the value of the DirectoryServiceAuth system parameter to Off.

7 Refresh the servers with the changes. For instructions, see “Refreshing LDAP or Active Directory system parameters” on page 157.

Refreshing LDAP or Active Directory system parameters

Security settings are handled separately by the Global Alerts Server (GAS), the GUI Server (GSR), and the Configuration Manager Server (CMS). Changes to certain LDAP or Active Directory security settings are not implemented until you refresh the settings for those servers.

NOTE

You should apply changes in any of the following scenarios:

■ When you change the value of the DirectoryServiceAuth system parameter.
■ When you connect to a different LDAP or Active Directory server.
■ When you change the communication protocol to or from SSL.

To apply the changes to those servers, run the following refresh commands.

■ To apply your changes to the GUI Server, use the following command:
Implementing external plug-in authentication

Implement the following functions using C or C++:

- **get_plugin_info** – returns a structure containing the common plug-in information.
- **get_auth_plugin_info** – returns a structure containing both authentication plug-in information and the common plug-in information.
- **auth_userpassword** – accepts user name, password, pointer to the message buffer, and message buffer size. By default, AUTH_MSG_BUFF_SIZE is the buffer size, but the plug-in implementation should use the buffer size passed at the time of the call.

The function definitions and related source and header files are contained in the Plug-in SDK (Software Development Kit) – plugin-sdk.zip – in the tools folder on the product CD. The following files are contained in plugin-sdk.zip:

- sample/myauth/ – a simple example of an external authentication plug-in.
- sdk/ – header files needed to build an external plug-in

The plug-in implementation authenticates the user and password and returns one of the following return codes:

- **AUTH_SUCCESS** – Authentication successful
- **AUTH_FAILED** – Authentication failed
- **AUTH_SIZE_NOT_ENOUGH** – Message buffer size is not large enough

Warning and information messages can be written to the buffer and displayed in the CONTROL-M/EM GUI.
Implementing external plug-in authentication

Chapter 5 Setting up CONTROL-M authentication security

The plug-in is implemented as a DLL/shared library.

2 Place the plug-in in the `CONTROL-M/EM_installation/plugins` folder.

CONTROL-M/EM is provided with sample plug-in code that can be used and adapted when you write your site’s plug-in. The following is a list of supported platforms and compilers used to build the sample plug-in code. BMC Software recommends that you use the same compiler versions.

- AIX 5.3 - IBM XLC++ 8.0
- Solaris 2.9 - Sun Studio 11
- HP-UX RISC 11.23 - HP aCC A.3.63
- HP-UX Itanium 11.23 - HP aCC A.06.12
- Red Hat Enterprise Linux, 4.0 - GNU/gcc C++ 4.1.2
- SUSE Linux, 9.0 SP3 - GNU/gcc C++ 4.1.2

3 Set the following external password authentication system parameters:

- PasswordEncode – Set this parameter to 0 so that the External Authentication procedure will receive an unencrypted password. If your site uses SSL, SSL secures the communication.

- AuthenticationMethod – Specify one of the following values:
  
  - `<name>`—the logical name (not the actual file name) of the external plug-in to be used for authentication. The CONTROL-M/EM GUI Server, Global Alerts Server, and Configuration Manager Server will load the plug-in and uses it to authenticate the user name and password.
  
  - `empty` – indicates that no external plug-in name is specified. The internal CONTROL-M/EM database user password check is used. Default.

4 Restart the CONTROL-M/EM GUI Server, Global Alerts Server, and Configuration Manager Server.

**NOTE**

If the external authentication plug-in fails to load (for example, due to an incorrect system parameter value, an incorrect interface version, or a general loading error), default internal authentication is used. The CONTROL-M/EM Server diagnostic log identifies the authentication method used by the server. If the plug-in fails to load, this log contains an error message.

You can also define an emergency user for situations where the external authentication is not available. For more information about the emergency user, see “Defining users and their authentication criteria to CONTROL-M/EM” on page 166.
Defining password requirements

You can define several types of password characteristics and requirements.

NOTE
To authenticate a user in an external system, the same user name must exist in CONTROL-M/EM. The first stage of authentication checks that the user exists in CONTROL-M/EM. If the user exists, the user’s password is authenticated externally.

NOTE
Because the Global Alerts Server (GAS), the GUI Server (GSR), and the Configuration Manager Server (CMS) handle security settings separately, if you modify certain password-related system parameters while these servers are running, be sure to perform a refresh to those servers. For instructions, see “Refreshing password-related system parameters” on page 160

Refreshing password-related system parameters

The following parameters require refresh of the servers:

- PasswordExpirationOnOff
- PasswordLifetimeDays
- WarningPasswordExpirationDays
- NumberOfPasswordReplacements
- NumberOfFailedLogins
- LockAccountForMinutes
- PasswordHistoryOnOff

To refresh a server, execute the appropriate command for that server:

- To apply your changes to the GUI Server, use the following command:
  
  `ctl -U EM_DBO -P EM_DBO_password -C GUI_Server {-M GSR_hostname | -name logical_name_of_GUI_Server | -all} -cmdstr "REFRESH_SECURITY_PARAMS"`

- To apply your changes to the Global Alerts Server, use the following command:
Setting allowable password lengths

You can set minimum and maximum password lengths.


3. When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

Setting password complexity rules (required character types)

To implement password complexity rules

1. Activate the usage of password complexity rules by setting the PasswordComplexityOnOff system parameter to 1 (password complexity on). By default, usage of password complexity rules is deactivated (the system parameter is set to 0).

2. Define the combination of required character types by specifying the appropriate keywords separated by a blank space in the PasswordComplexityRules system parameter, as follows. (An AND logic is assumed between specified values.)

   — Use of at least one digit mandatory—specify PWD_DIGIT.
   — Use of at least one uppercase letter mandatory—specify PWD_UPPER.
   — Use of at least one lowercase letter mandatory—specify PWD_LOWER.
   — Use of at least one non-alphanumeric character mandatory—specify PWD_NON_LETDIG.
Setting password reuse limits

By default, all four types of characters must be satisfied (the default value is: `PWD_DIGIT` `PWD_UPPER` `PWD_LOW` `PWD_NON_LETDIG`).

3 When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

To deactivate usage of password complexity rules

Set the `PasswordComplexityOnOff` system parameter to 0 (password complexity off). Default.

When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

Setting password reuse limits

To set the number of times a user must change a password before reusing a password

1 Set `PasswordHistoryOnOff` system parameter to 1 (on). If this parameter is set to 0 (default), new passwords are not checked against previous passwords, and users can reuse passwords without any reuse limits.

2 Set the `NumberOfPasswordReplacements` system parameter to the number of password changes must occur before a password can be reused. Default: 10. Valid values: 1 to 20. (This parameter also determines the maximum number of most recently used passwords that are stored for each user in the CONTROL-M/EM database.)

3 When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

To remove all limits on password reuse

Set `PasswordHistoryOnOff` system parameter to 0 (off). Default.

When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.
Implementing password expiration policy

You can define and implement a password expiration policy that

- determines how long passwords can be used before expiring
- defines when warnings should be issued that a password will soon expire

These warnings are issued as follows:

- Before password expiration—if the password has not yet expired, the following warning message is generated:
  Your password will expire in \( n \) days.
  — When a user runs cli or XML utilities, this warning is returned and the process continues.
  — When a user logs in to CONTROL-M/EM GUI, CONTROL-M/Desktop, or the Reporting Facility, the application displays a message box containing an option to change the password. The user can change the password and continue, or continue without changing the password.

- After password expiration—if the password has expired, the following message is generated:
  Your password has expired. Please change the password.
  — When a user attempts to run XML utilities or the cli utility, this message is returned and the process exits.
  — When a user logs into CONTROL-M/EM GUI, CONTROL-M/Desktop, or the Reporting Facility, the application displays a message box containing an option to change the password. The user can change the password and continue, or exit the process.

To implement password expiration policy

1. In the PasswordLifetimeDays system parameter, define the number of days that passwords should be valid before expiring. Default: 60. Valid values: 1 - 365.

2. Run the set_pwd_def_lifetime script. For instructions, see “Implementing password policy for all users using the set_pwd_def_lifetime script” on page 164.

This script propagates the value defined in the PasswordLifetimeDays system parameter into the Password will expire every \( n \) days field for each user, in the General panel of the User Authorizations window. The script then computes and resets the password expiration date for each CONTROL-M/EM user (excluding BMC Batch Impact Manager users) according to this value.
Implementing password policy for all users using the set_pwd_def_lifetime script

3 Manually define the exceptions for these users to whom the site-wide expiration limits should not apply. For instructions, see “Manually modifying a user’s password criteria” on page 169.

4 In the WarningPasswordExpirationDays system parameter, define the number of days prior to password expiration during which a warning message should generated. Default: 0, which indicates that a warning message is not generated. Valid values: 0 - 90.

NOTE

Warnings are issued only when certain utilities or scripts are run or a successful logon is performed.

5 Activate the password expiration feature by setting the PasswordExpirationOnOff system parameter to 1 (On).

6 When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

To disable limits on how long a password can be used before expiring

Set the PasswordExpirationOnOff system parameter to 0 (Off). Default.

When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

Implementing password policy for all users using the set_pwd_def_lifetime script

The General tab in the User Authorization window contains the Password will expire every n days option which determines how often a user’s password will expire.

By running the set_pwd_def_lifetime script, you can use the value defined in the PasswordLifetimeDays system parameter to compute and reset the password expiration date for each CONTROL-M/EM user (excluding BMC Batch Impact Manager users).

This script performs the following, for each user, in the General tab of the User Authorization window:
Setting automatic account locking after consecutive failed logon attempts

- sets the value of **Password will expire every n days** to the value set in the **PasswordLifetimeDays** system parameter. (If a user’s **Password never expires** option was selected, the script clears this option.)

- sets the user’s password expiration date to the date obtained by adding that number of days to the current date.

**To run the set_pwd_def_lifetime script**

1. Invoke the script from the appropriate location:

   - On UNIX, select **Users Administration Menu => Set Password Default Lifetime** from the **Root** menu.

   - On Windows, the script is available in the directory where the CONTROL-M/EM server components are installed.

   The format for invoking this script is:
   ```
   set_pwd_def_lifetime [-U EM_DBO_name] [-P EM_DBO_password]
   ```

2. If the script prompts you for the DBO user name and password, supply them. (This happens if you do not include them in the command line.)

**Setting automatic account locking after consecutive failed logon attempts**

You can define the number of failed logon attempts that will result in automatic locking of the account, and the number of minutes for which the account will be locked before logon can again be attempted.

1. In the **NumberOfFailedLogins** system parameter, set the number of failed logon attempts after which an account will automatically be locked. Default: 0, which means that accounts are not automatically locked. Valid values: 0 - 100.

2. In the **LockAccountForMinutes** system parameter, set the number of minutes for which an automatically locked account will remain locked. Default: 0.

**NOTE**

- A value of 0 (default) in the **LockAccountForMinutes** system parameter means that the account will remain locked until it is manually unlocked by the administrator.

- Accounts that were manually locked by a CONTROL-M/EM administrator are not affected by the **LockAccountForMinutes** system parameter; they cannot be automatically unlocked.
Unlocking multiple accounts with the unlock_user script

3 When you have finished changing all password-related parameters, refresh the relevant servers. For instructions, see “Refreshing password-related system parameters” on page 160.

Unlocking multiple accounts with the unlock_user script

There might be instances when you would want to unlock accounts using a script. For example, though such a scenario is unlikely, it is possible that all administrator accounts can become locked. (For example, hackers may attempt consecutive unsuccessful logons to all administrator accounts, causing the accounts to become locked.)

The CONTROL-M/EM administrator can manually unlock an account using the unlock_user script.

To run the unlock_user script

1 Invoke the script from the appropriate location:

- On UNIX, select Users Administration Menu => Unlock User from the Root menu.
- On Windows, the script is available in the directory where the CONTROL-M/EM server components are installed.

The format for invoking this script is:

```
unlock_user -username EM_user [-U EM_DBO_name] [-P EM_DBO_password]
```

- `EM_user` specifies the account to unlock
- `EM_DBO_name` specifies the CONTROL-M/EM database owner
- `EM_DBO_password` specifies the password of the database owner.

2 If the script prompts you for the -U and -P DBO values, supply them. (This happens if you do not include them in the command line.)

Defining users and their authentication criteria to CONTROL-M/EM

To implement user authentication, you must define users to CONTROL-M/EM, and provide their authentication criteria. You do this using the User Authorization window. New authorizations or changes to existing authorizations will not take effect until the associated user logs off of all CONTROL-M/EM sessions.
When creating users, you can create them “from scratch,” or you can copy an existing user (saving the details of an existing user under a new name).

**NOTE**
When you copy an existing user, the groups to which the existing user belongs are associated with the new user, but the existing password is not copied. You can define the password for the new user by using the General tab of the User Authorizations window.

**To define user authentication**

1. From CONTROL-M/EM or CONTROL-M/Desktop, access the Authorizations window by choosing Tools => Authorizations.

2. To create a new user either from scratch or by copying the details of an existing user, do the following in the Users tab of the Authorizations window:
   - To create a new user from scratch:
     A. Click New.
     B. In the New Name dialog box, enter the name of the user, and click OK.
   - To create a new user by copying the details of an existing user:
     A. Choose the user.
     B. Click Copy.
     C. In the New Name dialog box, enter the name of the user and click OK.

3. In the Users tab of the Authorizations window, choose the user and click Update.

4. In the General tab of the User Authorization window, define the logon authentication data for the user. Most information that you must provide in the fields of the tab is intuitive.
   
   Use the following pointers to help you when you define this information:

   - To identify the user to the system, specify a unique name without blanks in the User Name field. You can include blanks when you identify the full user name in the Full Name field.
Defining users and their authentication criteria to CONTROL-M/EM

--- EXAMPLE ---

To identify the user

- In the User Name field, enter BillHS.
- In the Full Name field, enter William Howard Smith

---

- If you enable external authentication (for details, see page 151 and page 158), an Emergency User check box is displayed. Select this box if you want to provide the user with the ability to circumvent external authentication.

- If you select this box, you must specify a password in the Password and Confirm Password fields.

- The Password field is disabled when you use Active Directory authentication. For more information, see “Authentication methods” on page 151.

- If you do not want automatic password expiration, click Password Never Expires. To force the user to change the password the next time the user logs on, click User must change password at next login. For these changes to take effect, set the appropriate system parameters. For more information, see “Implementing password expiration policy” on page 163.

- To manually lock a user out of an account, click Lock Account.

--- NOTE ---

By default (UserChangePassword system parameter = 1), all users can change their own password using the Tools=> Change Password option.

To enable only users having Full or Update level access to the Authorizations privilege to change their passwords using the Tools=> Change Password option, set the UserChangePassword system parameter to 0. Generally, this value serves to restrict password change authorization to CONTROL-M/EM administrators.

If a CONTROL-M/EM administrator uses the Authorization dialog to set a password, the password complexity, length, and history requirements are ignored.

---

To delete a user

1 From CONTROL-M/EM or CONTROL-M/Desktop, access the Authorizations window by choosing Tools => Authorizations.

2 In the Users tab of the Authorizations window, choose the user and click Delete.

3 In the confirmation window, click OK.
Manually modifying a user’s password criteria

Users can change their own passwords using the Change Password menu option in CONTROL-M/EM or CONTROL-M/Desktop.

However, CONTROL-M/EM administrators can manually perform a number of password criteria modifications for individual users in the General panel of the User Authorizations window in the CONTROL-M/EM GUI, including the following:

- changing passwords
- changing password expiration dates
- locking and unlock a user’s account

To manually modify a user’s password criteria

1. From CONTROL-M/EM (or CONTROL-M/Desktop), choose Tools => Authorizations to access the Authorizations window.

2. In the Users tab of the Authorizations window, choose the user and click Update.

3. In the General panel of the User Authorizations window, perform the following as needed:
   
   A. To modify the password value, type in the new password in both the Password and Confirm Password fields.

   **NOTE**

   If a CONTROL-M/EM administrator uses the Authorization facility to set a password, the password complexity, length, and reuse requirements are ignored.

   B. To modify the password expiration period, in the Password expiration area, set appropriate value to the password management parameters.

   C. To lock or unlock the user’s account choose (or unselect) Lock account.

4. Click OK.
Changing the DBO password

1. Enter one of the following SQL commands:
   - For Sybase: `sp_password oldPassword, newPassword, userName`
   - For Oracle: `alter user <userName> identified by newPassword`
   - For MSSQL: `sp_password <oldPassword>, newPassword, userName`

   **NOTE**
   The following step must be run on each computer on which CONTROL-M/EM is installed, except those with only client components that do not have the Reporting Facility installed.

2. Run the `cryptocli` utility using the following syntax.

   **NOTE**
   `<EMHomedir>` here indicates the directory in which CONTROL-M was installed.

   - On UNIX: `cryptocli ecs user_name new_password <EMHomedir>/ini/mcs.ini`
   - On Windows: `cryptocli user_name new_password emHome\default\ini\mcs.ini`

   **NOTE**
   This user name and encrypted password are stored in the `mcs.ini` file in the `EMHome/ini/` directory on every computer on which CONTROL-M/EM server components are installed.

   For more information on the `cryptocli` utility, see the CONTROL-M Utility Guide.

Defining a CONTROL-M/Agent account

*(Windows only)*

On Windows, the CONTROL-M/Agent is a service called the Listener Service, and to implement general Agent security, the administrator must specify an account (Local System or User) for the Listener service.
Defining a CONTROL-M/Agent account (Windows only)

You must define a user account in the following situations:

- If the owner of any jobs run by CONTROL-M/Agent has a “Roaming Profile.” For more information, see “Support for a Roaming Profile” on page 172.
- If WMI jobs will run on remote hosts

If the job must access the network, the owner of the job must be a domain user with access rights to the network

- If the Logon As User parameter is set to Y, the owner of the job will be the owner specified in the CONTROL-M job processing definition.
- If Logon As User is set to N, the Listener Service should run from a user domain account and the owner of the service will be an owner of the job.

**NOTE**

(Windows Vista or Windows 2008 only) If the Logon As User parameter is set to Y, the Agent service should be set to This Account.

**To specify a Local System account for the Listener service**

1. In the Services window, right-click on the relevant agent service and select Properties.

2. In the Log On tab in the Properties window, select Local System account.

The service will run in the administrative group and in the native system account environment. By installation default, the following options are selected:

- (Log on as:) “Local System Account”
- “Allow service to interact with desktop”

These options enable the Listener service to open windows in the Microsoft Windows desktop. However, the Local System Account cannot access files across a network and cannot send a Shout message to an e-mail destination.

**To specify a user account for the Listener service**

1. In the Services window, right-click on the relevant agent service and select Properties.

2. In the Log On tab in the Properties window, select This Account.

3. In the This Account text box, specify account information. The account must be a member of the Local Administrative Group. The format is <Domain>\<User>. 
Defining a CONTROL-M/Agent account (Windows only)

NOTE
The administrator selected as part of This Account, must have the following permissions in the Local Security Settings window:

- Adjust memory quotas for a process
- Replace a process level token
- Log on as a service

4 Specify the password and confirm.

5 If the owner of any jobs run by CONTROL-M/Agent has a Roaming Profile, ensure that the criteria specified in “Support for a Roaming Profile” on page 172 are satisfied.

The service will run in the specified user environment.

Support for a Roaming Profile

CONTROL-M/Agent support for Roaming Profile requires the following:

- The profile must reside on the network. If the network path includes the environment variable, CONTROL-M/Agent expands the path and loads the User Profile from the expanded path.

- After loading the user profile, CONTROL-M/Agent sets all environment variables from the roaming profile:
  - Logs into a different computer with the roaming user
  - Changes/adds the private environment variable
  - Logs out
  - Runs the CONTROL-M job on the original computer

- New environment variables or updated variables performed by the roaming user on any computer will be detected by the CONTROL-M job.

NOTE
To eliminate the need to assign user rights to every job owner on every Microsoft Windows computer running CONTROL-M/Agent, BMC Software recommends that you define a domain-level group for all job owners. You can name this group CONTROL-M Job Owners. Assign network access rights and the Logon as a batch job user right to this group.
Defining job owner and authentication settings for CONTROL-M/Agents and remote hosts

For each CONTROL-M/Agent and remote host, you must define the owners of the jobs that will run on it (that is, the job owners of those CONTROL-M jobs that list the agent or remote host computer in the Node ID field), and appropriate owner authentication parameters.

**NOTE**

For CONTROL-M/Agent, job owners can be defined only for owners of jobs running on CONTROL-M/Agent on Windows. These owners are relevant only when Logon_as_user=Y.

These definitions are saved in the CONTROL-M/Server database.

**NOTE**

If you are using the Key Authentication for the SSH connection method, you will be required to provide Key name and Passphrase authentication parameters. You generate these values using the CONTROL-M/Server ctmkeygen utility (described in the CONTROL-M Utility Guide). Be sure you have these values before performing this procedure.
To define or update agent or remote host job owner and authentication settings

1. In the CONTROL-M Configuration Manager, right click a CONTROL-M/Server and click Security => Owners Authentication Settings. This displays the list of job owners for the CONTROL-M/Server in the Owners Authentication Settings dialog box.

   ![Owners Authentication Settings](image)

   To filter the list, click Manual Load, enter the filter criteria at the bottom of the dialog box, and click Load. You can specify asterisks as wildcards in the filtering criteria.

2. To add a job owner for an agent or remote host:

   A. Click to display the New Owner Definition dialog box.

   B. Specify the owner and the host (Node ID). To make this owner the default owner of all agents or remote hosts, specify <All> in the Host field. Ensure that you include the angle brackets when you specify <All>.

   **NOTE**

   If the connection method will be WMI, the job owner must belong to the local Administrator group on the agent or remote host.
C In the Authentication Properties area, click the appropriate authentication method and fill in or select the authentication parameters as follows:

- For WMI connections, click **Use Password Authentication**, and then fill in the user name and password, and confirm the password. The user name should include the domain.

- For SSH connections, either
  - click **Use Password Authentication** and fill in and confirm the password
  - click **Use Key Authentication (SSH only)**, and fill in the Key Name and Passphrase values generated by the CONTROL-M/Server ctmkeygen utility. (For details about the ctmkeygen utility, see the utility description in the **CONTROL-M Utility Guide**.)

D Click **Test** to check that your settings are correct and workable.

E Click **OK**.

3 Optionally perform any of the following as needed in the Owners Authentication Settings dialog box:

- To delete a job owner for an agent or remote host, click 

- To modify the authentication properties for a job owner on an agent or remote host, click the line that lists the owner and host, modify the values in the Authentication Properties area, and click **Save**

- To modify an owner-host combination, delete the owner-host line, and then add new owner-host definition

4 Click **Test** to check that your settings are correct and workable.

5 Click **Close**.
Setting up CONTROL-M authorization security

Conceptual overview. .......................................................... 177
CONTROL-M/EM authorization security .................................. 179
CONTROL-M/Server authorization security ............................... 180
CONTROL-M/Agent security .................................................. 182
Recommended task summary ................................................. 184
Implementing CONTROL-M/EM authorization security ............. 184
  Creating and deleting group security definitions ..................... 185
  Defining which group profiles apply to a user ...................... 186
  Defining or modifying user or group authorization details .......... 186
  Ensuring owner verification during New Day processing job ordering . 197
  Authorizing non-administrators to manage application accounts .... 200
Enabling passage of global conditions from GCS to CONTROL-M/Servers ........................................... 202
Changing the default Global Conditions Server user name .......... 202
Implementing CONTROL-M/Server authorization security ............ 202
  Adding, deleting and modifying users and groups .................. 204
  Assigning authorizations to users and groups .................... 205
  Activating CONTROL-M/Server security ............................. 206
Implementing CONTROL-M/Agent and remote host authorization security .................................................. 207
  Implementing CONTROL-M/Agent job owner security (Windows only) ........................................... 207
  Implementing CONTROL-M/Agent remote host security .......... 208
  Authorizing which CONTROL-M/Server utilities a CONTROL-M/Agent can request ........................................ 209

Conceptual overview

With CONTROL-M, you can establish a high degree of data security without adversely affecting production.
Authorization security defines which data users are allowed to view and which operations (including data modification) that users can perform. At the CONTROL-M/EM and CONTROL-M/Server levels, you can define security for individual users and for groups.

A group is an authorization profile that is relevant to more than one user. Users can be associated with more than one group and obtain authorizations based on the group profiles with which the user is associated.

CONTROL-M/EM security authenticates users and validates authorizations when a request is sent through CONTROL-M/Enterprise Manager.

An additional level of security can be applied by CONTROL-M/Server when it receives a request from CONTROL-M/EM.

CONTROL-M/EM and CONTROL-M/Server each have a security definition repository; CONTROL-M/Agent does not have a security definition repository, but instead utilizes operating system security.

SSL security ensures both data privacy (unauthorized users cannot view the data) and data integrity (unauthorized updates cannot be performed) between the following connection points:

- CONTROL-M/EM clients and CONTROL-M/EM servers.
- CONTROL-M/EM server and CONTROL-M/Server (and CONTROL-M for z/OS)
- CONTROL-M/Server and CONTROL-M/Agent (and remote hosts)

When you are defining authorization security, mask characters are available for all options. Mask characters * and $ are translated during runtime security checking. (For example, if User1 is granted full Scheduling Table authorization for table ACC*, CONTROL-M allows User1 to update or order any table whose name starts with ACC.) Valid mask characters are as follows:

- * represents any number of characters (including none).
- $ represents a single character.

Mask character authorizations do not override full name authorizations. (For example, if User1 has only Read privileges for ACC999, CONTROL-M will not allow User1 to update or order table ACC999.)

Figure 15 on page 179 highlights the basic recommended workflow for setting up authorization security for CONTROL-M. This overview section explains concepts that are related to the workflow.
For specific tasks that correspond to each phase of the workflow, see Table 15 on page 184. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

**Figure 15  Recommended workflow for setting up authorization security**

---

**CONTROL-M/EM authorization security**

Using the CONTROL-M/EM authorization security feature, you specify

- entities (such as jobs, Viewpoints, calendars, and resources) that a user or group of users can access

- actions (such as view, modify, or delete) that a user or group of users can perform on those entities

To set up CONTROL-M/EM user and group authorizations, you use the Authorization window, which you can access from CONTROL-M/EM or CONTROL-M/Desktop.

When you associate a user with the authorization profiles of groups, either of two algorithms apply to the inheritance of those profiles:
■ When you define user privileges using the Privileges tab in the Authorization window, authorization inheritance works as follows:

— Specifying the DEFAULT access level for a privilege causes the user to inherit the authorization for that privilege from the group profile. If the user is associated with multiple groups, the user inherits the highest access level defined for that privilege in those groups.

— Specifying any other access level gives the user that level (group access levels for that privilege are ignored).

■ When you define the other authorizations (authorizations other than Privileges), the algorithm is a composite of the user and group authorizations. For each authorization, you specify an entity name and an authorization. For each entity defined for the user or related groups, the user inherits the highest authorization defined for that entity.

**CONTROL-M/Server authorization security**

For many situations, CONTROL-M/EM security, which is based on user id, is sufficient, and implementation of CONTROL-M/Server security is unnecessary.

However, an important use of CONTROL-M/Server security is to ensure that only appropriate, authorized end-users can run powerful utilities, such as ctmdefine, from jobs. CONTROL-M/Security can block access to the utilities if an end-user should not run such utilities.

CONTROL-M/Server security is recommended if

■ end users can access and run utilities from CONTROL-M/Server accounts

■ jobs running on the CONTROL-M/Agent or remote host computer can execute other jobs or command line utilities

■ you do not trust the security of the communication channel between CONTROL-M/EM and CONTROL-M/Server. (If you implement SSL security, which protects your data from unauthorized updates, there is no need to implement CONTROL-M/Server security.)

CONTROL-M/Server security allows you authorize under which account a job can run, based on the job’s owner, and which actions (for example, forcing another job or running a utility) the job owners are authorized to perform in the CONTROL-M/Server account.
CONTROL-M/Server authorization security applies to the Active environment. For example, if a job should run under the Root, or other account, you define that account as the owner.

**NOTE**

If needed, you can also define authorization security for applications by defining a Control Module account as the owner. For an Operating System job, you use operating system security.

These authorizations are used to perform security checks each time one of the following actions is attempted in CONTROL-M/Server:

- accessing a scheduling table (to add, delete, or modify a job definition)
- ordering a job
- selecting and submitting a job
- running a command that affects jobs in the Active environment (for example, Hold, Confirm, Rerun)
- maintaining CONTROL-M entities (for example, calendars and prerequisite conditions)

Security verifications for these actions are implemented according to specifications stored in a section of the CONTROL-M/Server database called the security database. CONTROL-M checks the security database to answer one of the following questions:

- Is the job owner authorized to perform the attempted action?
- Is the owner of an executing job authorized to order or force additional jobs that belong to that owner or other owners?

To set up authorizations and to maintain the CONTROL-M/Server security database, you use the CONTROL-M Configuration Manager. (Alternatively, you can use the ctmsec Security Maintenance utility.)

**Users and groups in CONTROL-M/Server authorization security**

When you assign a user to a group at the CONTROL-M/Server level, the following rules apply:

- If no authorizations are defined for the user, the user inherits the authorizations for the group.
- If authorizations are defined for a user, the user’s authorizations take precedence.
When defining an authorization for a user (for example, Scheduling Table), use of the (D)efault setting enables the specific authorization (for example, Read) defined for the group.

If all of a user’s authorizations for a specific CONTROL-M element (for example, Scheduling Table) are defined with a (D)efault setting, the user’s authorizations for that element can be deleted more efficiently.

Authorizations that are not specifically defined for a group (or for a user not belonging to a group) revert to the Full Security parameter setting. (The Full Security parameter is described in Table 81 on page 454.)

CONTROL-M/Server authorization security for applications

CONTROL-M provides the following levels of application security for users who are not explicitly defined in the CONTROL-M security database:

<table>
<thead>
<tr>
<th>Security level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restricted</td>
<td>A user who is not defined in the CONTROL-M security database has no authorizations and cannot perform any action that requires security authorization.</td>
</tr>
<tr>
<td>Unrestricted</td>
<td>A user who is not defined in the CONTROL-M security database has all CONTROL-M application authorizations. This level is the default.</td>
</tr>
</tbody>
</table>

Regardless of which level is implemented, the following requirements apply:

- If one or more authorizations have been assigned to a user in the security database, that user can perform only those actions.

- The owner of each job processing definition must be defined as a user on the agent computer. Otherwise, CONTROL-M/Agent will not execute the job.

The value of the CONTROL-M system parameter Full Security (described in Table 81 on page 454) determines the security level.

CONTROL-M/Agent security

CONTROL-M/Agents are the components that actually process the jobs. CONTROL-M/Agents use operating system security, which focuses on the owner who is defined for each job.
For Unix: Upon receiving a job execution request, CONTROL-M/Agent submits the job on behalf of the owner only if the owner is defined in the operating system security.

For Windows: Upon receiving a job execution request, CONTROL-M/Agent submits the job on behalf of the owner only if the owner is defined in the operating system security and the Logon_as_user=Y.
Recommended task summary

Table 15 lists specific tasks related to each phase of the workflow (Figure 15 on page 179). Subsequent sections provide step-by-step instructions.

Table 15  Task summary: setting up authorization security

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement CONTROL-M/EM authorization security</td>
<td>Creating and deleting group security definitions</td>
<td>185</td>
</tr>
<tr>
<td></td>
<td>Defining which group profiles apply to a user</td>
<td>186</td>
</tr>
<tr>
<td></td>
<td>Defining or modifying user or group authorization details</td>
<td>186</td>
</tr>
<tr>
<td></td>
<td>Ensuring owner verification during New Day processing job ordering</td>
<td>197</td>
</tr>
<tr>
<td></td>
<td>Authorizing non-administrators to manage application accounts</td>
<td>200</td>
</tr>
<tr>
<td>Enable passage of global conditions from</td>
<td>Enabling passage of global conditions from GCS to CONTROL-M/Servers</td>
<td>202</td>
</tr>
<tr>
<td>GCS to CONTROL-M/Servers</td>
<td>You can change the GCSERV default user name using the GCSCommUserId system</td>
<td>202</td>
</tr>
<tr>
<td></td>
<td>parameter. For more information, see Appendix B, “System parameters.”</td>
<td></td>
</tr>
<tr>
<td>Implement CONTROL-M/Server authorization</td>
<td>Adding, deleting and modifying users and groups</td>
<td>204</td>
</tr>
<tr>
<td>security</td>
<td>Assigning authorizations to users and groups</td>
<td>205</td>
</tr>
<tr>
<td></td>
<td>Activating CONTROL-M/Server security</td>
<td>206</td>
</tr>
<tr>
<td>Implement CONTROL-M/Agent and remote host</td>
<td>Implementing CONTROL-M/Agent job owner security (Windows only)</td>
<td>207</td>
</tr>
<tr>
<td>security</td>
<td>Implementing CONTROL-M/Agent remote host security</td>
<td>208</td>
</tr>
<tr>
<td></td>
<td>Authorizing which CONTROL-M/Server utilities a CONTROL-M/Agent can request</td>
<td>209</td>
</tr>
</tbody>
</table>

Implementing CONTROL-M/EM authorization security

This section provides instructions for defining CONTROL-M/EM authorizations. New authorizations or changes to existing authorizations will not take effect until the associated user logs off of all CONTROL-M/EM sessions.

You create users and define their authorizations from the User Authorizations window; and you create groups and define their authorizations from the Group Authorizations window.
Before you can define these authorizations, you must create the user or group.

For instructions on creating users and defining their logon authentication criteria, see “Defining users and their authentication criteria to CONTROL-M/EM” on page 166.

This section describes how to create groups and how to define user and group authorizations.

Creating and deleting group security definitions

When creating groups, you can create them “from scratch,” or you can copy an existing group (saving the details of an existing group under a new name).

NOTE

When you are copying an existing group, the users that belonged to the existing group are not associated with the new group.

To create a new group

1. From CONTROL-M/EM or CONTROL-M/Desktop, access the Authorizations window by choosing Tools => Authorizations.

2. In the Groups tab of the Authorizations window, proceed as follows:
   - To create a new group from scratch, click New.
   - To copy the details of an existing group, choose the group and click Copy.

3. In the New Name dialog box, enter the name of the group and click OK.
   The name of the new group is displayed in the Groups panel.

4. Define or modify the details of the group as needed.

   For instructions, see “Defining or modifying user or group authorization details” on page 186.

To delete a group

1. From CONTROL-M/EM or CONTROL-M/Desktop, access the Authorizations window by choosing Tools => Authorizations.

2. In the Groups tab of the Authorizations window, choose the group and click Delete.
Defining which group profiles apply to a user

3 In the confirmation window, click **OK**.

**Defining which group profiles apply to a user**

1 From CONTROL-M/EM or CONTROL-M/Desktop, access the Authorizations window by choosing **Tools => Authorizations**.

2 In the **Users** tab of the Authorizations window, choose the user and click **Update**.

3 In the **Member Of** tab in the User Authorization window, do the following:
   - To add the user to one or more groups, select the groups in the **Not A Member of** list and click **Add**.
   - To remove the user from one or more groups, select the groups in the **Member of** list and click **Remove**.

**Defining or modifying user or group authorization details**

You define or modify user or group details using the User Authorizations window or Group Authorizations window, respectively. These windows contain several tabs for defining different sets of authorizations.

1 From CONTROL-M/EM or CONTROL-M/Desktop, access the Authorizations window by choosing **Tools => Authorizations**.

2 To update user authorizations, complete these steps:
   - In the **Users** tab of the Authorizations window, choose the user and click **Update**.
   - In the User Authorization window, define or modify the authorizations in the appropriate tabs.

3 To update group authorizations, complete these steps:
   - In the **Groups** tab of the Authorizations window, choose the group and click **Update**.
   - In the Group Authorization window, define or modify the authorizations in the appropriate tabs (as explained in the following procedures).

4 When you finish defining the authorizations, click **OK**.
To define or modify the authorizations for users and groups, you perform the following tasks:

**NOTE**
The task of defining logon data (in the General tab of the User Authentication window) is described in the Security Authentication chapter.

- Defining general information about a group (for groups only)
- Defining which Active environment jobs the user or group can access and actions the user or group can perform
- Defining privileges and access to CONTROL-M components granted to a user or group
- Defining user or group access to and authorizations for scheduling tables
- Defining user or group access to jobs owned by other users
- Defining which conditions and resources a user or group can access
- Defining calendar access for a user or group

**Defining general information about a group (for groups only)**

Define or modify general information about a group in the fields of the General tab of the Group Authorization window (group name and description).

The General tab of the Group Authorization window lists the members of the group, but you cannot update these entries. To add or delete members from the Group, use the Member Of tab in the User Authorization window. For more information, see “Defining which group profiles apply to a user” on page 186.

**Defining which Active environment jobs the user or group can access and actions the user or group can perform**

The Jobs tab enables you to define which Active environment jobs the user or group members can access (display in a ViewPoint) and which actions the user or group can perform on those jobs.

In the Jobs tab:
1 Define a filter that determines which jobs the user or group can display in a ViewPoint, as follows:

A Click Filter to display the Job Filter Definition dialog box.

B Optionally, enter a description of the filter.

Each set of filtering criteria consists of a field to be checked, and a relational operator and value used when the field is checked (for example, Member Name LIKE e* will check the Member Name field for a name that begins with the letter e).

You determine whether to include or exclude jobs that match a set of criteria.

C To define sets of filtering criteria, perform the following as often as needed until the filter is completely defined:

1. In the Edit area, select a Field and relational operator, and specify the value. You can specify an asterisk as a wildcard.

2. Click Add by the Include or Exclude area, as appropriate.

3. If necessary, you can delete criteria from an Include or Exclude area.

---

**NOTE**

- Each line in the Include in or Exclude from Jobs Filter list can include multiple criteria. There is an AND relationship between all the criteria on a line. Only jobs that satisfy all the criteria on a line are included or excluded by the Jobs filter.

- There is an OR relationship between separate lines in the Include in or Exclude from Jobs Filter list. Jobs that fulfill the criteria on any one line are included or excluded by the Jobs filter.

---

2 Click the appropriate boxes to define the actions the user or group can perform. The following categories are available:

- Job-related information that the user or group can browse
- Job control actions the user or group can perform
- Job update actions the user or group can perform.
Defining or modifying user or group authorization details

Chapter 6 Setting up CONTROL-M authorization security

Defining or modifying user or group authorization details

Defining privileges and access to CONTROL-M components granted to a user or group

Using the Privileges tabs, you define access levels that determine what CONTROL-M components a user or group can access and what actions the user or group can perform on those components.

Table 16 lists the possible access levels that you can allow for the privileges you grant.

### Table 16 Privileges tab access levels (part 1 of 2)

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>None</td>
<td>Denies access to the component.</td>
</tr>
<tr>
<td>Browse</td>
<td>Can view and refresh the component.</td>
</tr>
<tr>
<td>Update</td>
<td>Permits adding and modifying CONTROL-M information.</td>
</tr>
</tbody>
</table>

---

**NOTE**

- Some job processing parameters cannot be used as selection criteria.
- The following job filtering fields are relevant to alerts and are used when you apply the filter definition to alerts: **Application**, **CTM Name** (CONTROL-M name), **Group**, **Job Name**, **Member Name**, and **Owner**.
- Users can see jobs permitted by User Authorization filtering criteria and jobs permitted by Group Authorization criteria for any group to which the user belongs. However, the jobs actions permitted by any of those filters apply only to the jobs permitted by that filter. Therefore, the user might be able to perform certain actions on some jobs but not other jobs.

---

**EXAMPLE**

User Bob has permission to see jobs starting with a*, and is authorized to perform Free and Hold actions with regard to those jobs.

User Bob belongs to the Tech Support group. Members of this group have permission to see jobs starting with b*, and are authorized to perform Rerun and Confirm actions with regard to those jobs.

User Bob also belongs to the DBA group. Members of this group have permission to see jobs starting with c*, and are authorized to use the Log and Documentation browse features and perform Confirm actions with regard to those jobs.

When Bob logs on to CONTROL-M/EM, he will see all jobs starting with the letter a, b, and c. On the group of jobs starting with the letter a he will be able to perform Hold and Free actions. On jobs starting with the letter b he can perform Rerun and Confirm actions. On jobs starting with the letter c he can view the Log and Documentation and perform Confirm actions.
Defining or modifying user or group authorization details

Table 16  Privileges tab access levels (part 2 of 2)

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Full</td>
<td>Permits adding, modifying, and deleting CONTROL-M information.</td>
</tr>
<tr>
<td>Default</td>
<td>[Valid for user authorizations. Not valid for group authorizations.] The user inherits the maximum access level granted by the groups to which the user belongs.</td>
</tr>
</tbody>
</table>

Table 17 lists the components for which you can grant privileges at the desired access level.

Table 17  Privileges and features (part 1 of 2)

<table>
<thead>
<tr>
<th>CONTROL-M/EM privilege</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Login</td>
<td>The ability to log on to the CONTROL-M Configuration Manager.</td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>The ability to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ create, update, delete, and get CONTROL-M/EM components</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ enable, disable, update, and manage CONTROL-M/Server components</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ create, update, delete, and get CONTROL-M/EM system parameters</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ view agent logs and get components</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ use CTL on a CONTROL-M/EM component</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ perform administrative tasks for CONTROL-M/Agents</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ get and set CONTROL-M debug level</td>
</tr>
<tr>
<td></td>
<td>Operation</td>
<td>The ability to manage components, including:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Start and stop CONTROL-M/EM components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Recycle CONTROL-M/EM components.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Set ignore status.</td>
</tr>
<tr>
<td></td>
<td>Database</td>
<td>The ability to</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ remove old data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ check the amount of space in the database</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ enlarge the database</td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/Server Security</td>
<td>The ability to create, update, view, and delete user and group CONTROL-M security records.</td>
</tr>
</tbody>
</table>
Defining or modifying user or group authorization details

Chapter 6 Setting up CONTROL-M authorization security

Using the Scheduling Tables tab, you can define

- which scheduling tables a user or group member can access
- level of access provided to the users or groups
- actions users or groups are authorized to perform on the tables

Table 18 summarizes the actions that you can authorize users and groups to perform on scheduling tables.

### Table 18  Scheduling table authorization (part 1 of 2)

<table>
<thead>
<tr>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Delete</td>
<td>Delete an entire Scheduling table or a job contained in the table.</td>
</tr>
<tr>
<td>Read</td>
<td>Download a Scheduling table from CONTROL-M/Server to CONTROL-M/EM.</td>
</tr>
</tbody>
</table>

### Table 17  Privileges and features (part 2 of 2)

<table>
<thead>
<tr>
<th>CONTROL-M/EM privilege</th>
<th>Feature</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitoring and Administration tools</td>
<td>Archived viewpoints</td>
<td>Actions that can be performed on archived viewpoints.</td>
</tr>
<tr>
<td></td>
<td>CLI</td>
<td>The ability to use the CLI utility. For more information, see the CONTROL-M Utility Guide.</td>
</tr>
<tr>
<td></td>
<td>Alerts</td>
<td>Specifies whether Alerts can be monitored and the actions that can be performed on them.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Note: Relevant parameters of the Jobs filter are also used to filter the Alert messages that are displayed.</td>
</tr>
<tr>
<td></td>
<td>BIM</td>
<td>The ability to access BMC Batch Impact Manager and its features.</td>
</tr>
<tr>
<td>ViewPoint Manager</td>
<td>Collections</td>
<td>The ability to perform actions on Collection definitions.</td>
</tr>
<tr>
<td></td>
<td>Hierarchies</td>
<td>The ability to perform actions on Hierarchy definitions.</td>
</tr>
<tr>
<td></td>
<td>Filters</td>
<td>The ability to perform actions on Filter definitions.</td>
</tr>
<tr>
<td></td>
<td>Viewpoints</td>
<td>The ability to perform actions on ViewPoint definitions.</td>
</tr>
</tbody>
</table>

**NOTE**

CONTROL-M/EM users with **Full** access to CONTROL-M/Server Attributes in the Privileges tab can add, modify, copy, or delete user and group authorizations. Users with **Browse** access can view authorizations.

Defining user or group access to and authorizations for scheduling tables

Using the Scheduling Tables tab, you can define

- which scheduling tables a user or group member can access
- level of access provided to the users or groups
- actions users or groups are authorized to perform on the tables

Table 18 summarizes the actions that you can authorize users and groups to perform on scheduling tables.
Defining or modifying user or group authorization details

Table 19 describes the access levels.

Table 19  Scheduling table access levels

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Permitted actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Viewing scheduling tables in CONTROL-M/Desktop. Default: Cannot order or force jobs. Can be modified to allow ordering and forcing jobs.</td>
</tr>
<tr>
<td>Update</td>
<td>Modifying and adding scheduling tables. Ordering and forcing jobs.</td>
</tr>
<tr>
<td>Full</td>
<td>Modifying, adding, and deleting scheduling tables. Ordering and forcing jobs.</td>
</tr>
</tbody>
</table>

**Ordering a scheduling table**

Authorization for an OrderTable action for a Scheduling table is checked in the following situations:

- When a user of CONTROL-M/EM attempts to order or force a Scheduling table or a job in the table, CONTROL-M/Server checks the user’s authorization for the action.

- When a job executing under CONTROL-M attempts to perform a Do Forcejob action on a Scheduling table or a job in the table, CONTROL-M/Server checks the authorization of the job’s Owner.

- When the Scheduling table is ordered by a User Daily job, CONTROL-M/Server checks the authorization of the User Daily job’s Owner.

- When a Scheduling table is ordered by the New Day procedure, CONTROL-M/Server checks the authorization of the CONTROL-M/Server account owner.

**NOTE**

In addition to the security checks described above, CONTROL-M checks authorization for each job in the Scheduling table, as described in Table 18 on page 191.
To allow a user or group to access and perform actions on a scheduling table

1. In the Scheduling Table tab, click **Add** to display the Scheduling Tables dialog box.

2. Provide the names of the CONTROL-M/Server, Library (for scheduling tables in CONTROL-M for z/OS only), scheduling tables. You can use pattern matching strings (and an * to denote all values).

3. Select the **Access Level** for these scheduling tables. Table 19 on page 192 describes the access levels.

4. Click **OK** to add the scheduling tables to the list in the **Scheduling Tables** panel.

5. Repeat this procedure to add access to other scheduling tables.

---

**NOTE**

When you define scheduling table access:

- The relationship between multiple values on a line is AND.
- The relationship between multiple lines is OR.

---

To modify or delete existing scheduling table access definitions

1. In the Scheduling Table tab, select the table.

2. Do either of the following, and when done, click **OK**:
   - Click **Update**, and in the Scheduling Tables dialog box, modify the current scheduling table access definition.
   - Click **Delete**.

---

**Defining user or group access to jobs owned by other users**

Using the Owner tab, you determine the specific operating system users or application accounts that can be specified as owners of a job. This determines which jobs users or groups can update and can run using XML utilities.

---

**NOTE**

These Owner definitions provide additional filtering criteria that supplement the criteria you defined using the Scheduling Table tab, and they apply only to users who have at least Update access granted in the Scheduling Tables tab. For more information, see “Defining user or group access to and authorizations for scheduling tables” on page 191.
1 In the Owner tab, specify the following:

A CONTROL-M/Server

B Owner (user ID) on whose behalf the user or group can execute the job.

C Node ID/Group. This field identifies the computers on which the user has authority to change or run jobs.

- The <local> Node ID/Group value should be used when the Node ID/Group field in the job editing form is left empty.

- The Node ID/Group field is not applied to jobs running on CONTROL-M for z/OS.

2 Click Add.

**Defining which conditions and resources a user or group can access**

The procedures for specifying which prerequisite conditions, control resources, quantitative resources, and global conditions that a user or group can access are almost identical, though each procedure uses a different tab and different dialog box.

**NOTE**

Prerequisite conditions, control resources, quantitative resources, and global conditions, are collectively referred to as conditions and resources in this section.

**To allow a user or group to access conditions or resources**

1 In the appropriate condition or resource tab, click Add to display the new condition or resource dialog box.

2 Provide the names of the CONTROL-M/Server and the condition or resource. You can use pattern matching strings (and an * to denote all values).

**NOTE**

For global conditions

- you do not provide a CONTROL-M/Server name
- you provide a global condition prefix

3 Select the **Access Level** for these scheduling tables. Table 20 describes the access levels.
Defining or modifying user or group authorization details

Chapter 6 Setting up CONTROL-M authorization security

1. Click **OK** to add the conditions or resources to the list in the condition or resource panel.

2. Repeat this procedure to add access to other conditions or resources.

--- **NOTE**

When you define conditions or resources access:

- The relationship between multiple values on a line is **AND**.
- The relationship between multiple lines is **OR**.

--- **EXAMPLE**

To authorize a user to modify prerequisite conditions that start with the letter C (for CTM1) or D (for CTM2):

1. Click **Add** in the **Prerequisite Conditions** panel.

2. In the New Prerequisite Condition dialog box, specify CTM1 in the **Control-M** text box, type **C* in the **Conditions** text box, and choose **Update** in the **Access Level** list box. Click **OK**.

3. Click **Add** again in the **Prerequisite Conditions** panel.

4. In the New Prerequisite Condition dialog box, specify CTM2 in the **Control-M** text box, type **D* in the **Conditions** text box, and choose **Update** in the **Access Level** list box. Click **OK**.

5. Click **OK** in the User Authorizations window.

---

**To modify existing condition or resource access definitions**

1. In the appropriate condition or resource tab, select the conditions or resources.

2. Click **Update**, and in the new conditions or resources dialog box, modify the current conditions or resources access definition.

3. Click **OK**.
**Defining or modifying user or group authorization details**

**To delete existing condition or resource access definitions**

1. In the appropriate condition or resource tab, select the conditions or resources.
2. Click **Delete**.
3. Click **OK**.

**Defining calendar access for a user or group**

You use the **Calendars** tab to specify which calendars a user or group can access.

**To allow a user or group to access a calendar**

1. In the Scheduling Table tab, click **Add** to display the New Calendars dialog box.
2. Provide the names of the CONTROL-M/Server and calendars. You can use pattern matching strings (and an * to denote all values).
3. Select the **Access Level** for these calendars. **Table 21** describes the access levels.
4. Click **OK** to add the calendars to the list in the **Calendars** panel.
5. Repeat this procedure to add access to other calendars.

---

**Table 21  Calendar access levels**

<table>
<thead>
<tr>
<th>Access Level</th>
<th>Permitted actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Browse</td>
<td>Permits viewing of specified calendars.</td>
</tr>
<tr>
<td>Update</td>
<td>Permits modifying specified calendars and adding new ones.</td>
</tr>
<tr>
<td>Full</td>
<td>Permits modifying and deleting specified calendars and adding new ones.</td>
</tr>
</tbody>
</table>

---

**NOTE**

When you define calendar access:

- The relationship between multiple values on a line is **AND**.
- The relationship between multiple lines is **OR**.

**To modify existing calendar access definitions**

1. In the Calendars tab, select the table.
2. Click **Update**, and in the New Calendars dialog box, modify the current calendar access definition.
Ensuring owner verification during New Day processing job ordering

Before every job submission, CONTROL-M verifies that the user ordering or forcing the job has appropriate authority. Typically, authorizations of the user ordering the job and the job owner are compared. For example, the security check determines if CONTROL-M/EM user Fred is allowed to order a job whose owner is root.

When a job is ordered during the New Day procedure or by a User Daily job, the Author parameter of the job is compared to the owner of the job. The Author parameter does not affect manual job order and job force requests.

Using AuthorSecurity to restrict Author modifications

The Author parameter contains the name of the CONTROL-M/EM user that performs a Write to CONTROL-M/EM from all CONTROL-M interfaces. Modifications to the Author parameter are restricted using the AuthorSecurity system parameter.

The following modes for restricting modification of the Author parameter are set using the AuthorSecurity system parameter:

“Mode 1: Permissive mode” on page 198
“Modes 2 and 3: Restrictive modes” on page 198

Special terms that are used in the description of this topic are defined in Table 22.
Ensuring owner verification during New Day processing job ordering

<table>
<thead>
<tr>
<th>Table 22</th>
<th>Terms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Term</td>
<td>Description</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>New jobs</th>
<th>Jobs that are</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>defined in CONTROL-M//Desktop during the current session</td>
</tr>
<tr>
<td></td>
<td>edited while CONTROL-M//Desktop is not connected to GUI server.</td>
</tr>
<tr>
<td></td>
<td>being written to CONTROL-M/EM the first time using a utility</td>
</tr>
<tr>
<td></td>
<td>edited while CONTROL-M/Desktop is connected to the GUI server but the job’s scheduling tables are not locked. Scheduling tables are unlocked using the Unlock option in the Scheduling Table Manager or the Disconnect from GUI Server option in the Communications menu in CONTROL-M/Desktop.</td>
</tr>
</tbody>
</table>

| Existing or other jobs | Jobs that were loaded from CONTROL-M/EM into CONTROL-M/Desktop and whose associated tables are locked. |

**Mode 1: Permissive mode**

This is the default mode. Editing the author is fully enabled. Users can retain the original author value when running utilities or performing a Write to CONTROL-M/EM or, alternatively, modify the author to another user.

**Modes 2 and 3: Restrictive modes**

Editing the author is either partially (mode 2) or fully (mode 3) disabled.

- For new jobs: The Author parameter is automatically set to the user who is running the utility or performing a Write to CONTROL-M/EM.

  **NOTE**
  
  If not currently connected to the GUI Server, the name is temporarily set to the *username* string. This name is reset to the current CONTROL-M/EM user when the user connects to the GUI server and the definition is written to CONTROL-M/EM.

- For existing jobs that have been changed and whose associated tables are locked:
  - In mode 2, the original Author parameter is retained.
  - In mode 3, the Author parameter is set to the user who is running the utility or performing a Write to CONTROL-M/EM.

  **NOTE**
  
  A prompt may be displayed indicating that the Author field will be automatically changed to the current user, depending on the setting of Resolve job’s Author Field conflict in the General panel of the Options dialog box in CONTROL-M/Desktop. The user can either accept the change, or cancel the entire Write to CONTROL-M/EM.

In both these modes, the Author parameter is displayed in the job editing form but cannot be modified.
In the Restrictive modes, a non-administrator user

- cannot update the Author field in the Mass Update window when performing mass updates in CONTROL-M/Desktop
- cannot assign a value to the Author field in the Template Editor window when defining CONTROL-M/Desktop templates

**NOTE**

Even when the AuthorSecurity system parameter is set to restrictive modes (2 or 3), an online CONTROL-M/EM administrator (meaning, one connected to a GUI Server) can modify the value of the Author parameter. Depending on the setting of *Resolve job’s Author Field conflict* in the General panel of the Options dialog box in CONTROL-M/Desktop, a prompt may be displayed before the value is changed.

### Other considerations

- After AuthorSecurity is modified, all CONTROL-M/Desktops must reconnect to the GUI Server (using the Communication menu) for the change to take effect.

- It is not necessary to recycle (stop and restart) the GUI server after changing the mode of the AuthorSecurity system parameter, but the user must disconnect and reconnect to CONTROL-M/Desktop.

- When a non-administrator performs a Write to CONTROL-M/EM, a message is displayed if an Author conflict exists. The user can choose one of these options:
  - OK – Accept the restrictions of the security mode.
  - Cancel – Cancel the entire Write to CONTROL-M/EM.

- If the administrator performs a Write to CONTROL-M/EM while in restrictive mode 2 or 3, a message is displayed if an Author conflict exists. The administrator can choose one of the following options:
  - Yes – Ignore the conflicts and save based on the Author that the administrator set.
  - No – Accept the security mode restrictions as if the administrator is a regular user.
  - Cancel – Cancel the entire Write to CONTROL-M/EM.

**NOTE**

The messages described above may not be displayed, depending on the *Resolve job’s Author Field conflict* setting in the General panel of the Options dialog box in CONTROL-M/Desktop. In this case, CONTROL-M/EM accepts the restrictions of the security mode and updates the Author for all conflicting jobs. For information about displaying confirmations, see the *CONTROL-M/Desktop User Guide*. 
Authorizing non-administrators to manage application accounts

By default, for users to be permitted to manage application (control module) accounts, they must have the Configuration box in the Privileges tab of the User Authorization window checked. However, placing a check in the Configuration box for users grants those users unlimited configuration privileges (they can configure everything).

The following procedure enables a CONTROL-M/EM administrator to define users or groups who can manage control module accounts, without granting them unlimited configuration privileges.

The permissions set using this procedure supersede the privileges defined in the User Authorization window.

To configure advanced security for control modules

1. Change the value of the restricted_cm_admin system parameter to 1.

   A. In the CONTROL-M Configuration Manager, select Tools -> System Parameters from the menu.

   B. Find the restricted_cm_admin system parameter and click Update.

   C. Change the value field to 1.

2. In a text editor, open the sample_cm_admin.xml file, which is located at `<emHome><instanceName>\ini` directory on the computer where the Configuration Management Server is running.

3. To give access to groups and users, enter values for the following tags. You can use expressions such as `a*` or `LIKE Bob` for any of the fields.

<table>
<thead>
<tr>
<th>Tag</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The name of the CONTROL-M/EM group or user to whom administrative rights for the control module are granted.</td>
</tr>
<tr>
<td>control_m</td>
<td>The CONTROL-M server with which the control module interfaces.</td>
</tr>
<tr>
<td>node_id</td>
<td>The name of the CONTROL-M agent node on which the control module is installed.</td>
</tr>
<tr>
<td>application_type</td>
<td>The type of control module.</td>
</tr>
</tbody>
</table>
NOTE

- To add an additional group or user, respectively, repeat step 3.
- The relationship between more than one filter in the file uses OR logic. Meaning, groups or users can manage control modules that answer any of the criteria in the list of filters.

4 Save the file as cm_admin.xml.

5 Run the following command:

   Ctl.exe -U EM_DBO -P EM_DBO_password -C CMS -name CMS -cmdstr “REFRESH_CM_ADMIN_AUTH”

   You must execute the above command every time the cm_admin.xml file is modified.

To disable advanced security for control modules

1 Perform the following to set the value of the restricted_cm_admin system parameter to 0.

   A In the CONTROL-M Configuration Manager, select Tools -> System Parameters from the menu.

   B Find the restricted_cm_admin system parameter and click Update.

   C Change the value field to 0.

2 Run the following command:

   Ctl.exe -U EM_DBO -P EM_DBO_password -C CMS -name CMS -cmdstr “REFRESH_CM_ADMIN_AUTH”
Enabling passage of global conditions from GCS to CONTROL-M/Servers

The CONTROL-M/EM Global Conditions server (GCS) distributes global conditions to data centers. (Global conditions are prerequisite conditions that can be propagated from one data center to another.) Prerequisite conditions can only be added or deleted by an authorized user.

To allow the GCS to add or delete global conditions on any CONTROL-M where CONTROL-M security is implemented, a special authorized user should be defined. On MVS systems, this user should be defined manually (as GCSERV, unless the default name was changed in CONTROL-M/EM) in CONTROL-M. For more information, see the chapter entitled “Installing IOA” in the INCONTROL for z/OS Installation Guide. On UNIX and Windows systems, a default authorized user already exists in CONTROL-M/Server, under the name GCSERV.

The GCSERV user name is also the default definition of an authorized user name in CONTROL-M/EM.

Changing the default Global Conditions Server user name

To change the default user name in CONTROL-M/EM

You can change the GCSERV default user name using the GCSCommUserId system parameter. For more information, see Appendix B, “System parameters.”

To change the default user name in CONTROL-M/Server

For detailed instructions, see “Implementing CONTROL-M/EM authorization security”.

Implementing CONTROL-M/Server authorization security

CONTROL-M/Server authorization security definitions are stored in the Security database.

To implement CONTROL-M/Server authorization security, you:
use the CONTROL-M/Server Security dialog box (Figure 16 on page 203), which you access from CONTROL-M Configuration Manager, to create security definitions. (Alternatively, you can use the CONTROL-M/Server ctmsec utility, described in the CONTROL-M Utility Guide.)

**NOTE**

- To implement CONTROL-M for z/OS authorization security, you must use the ctmsec utility; you cannot use the CONTROL-M Configuration Manager.

- To implement CONTROL-M/Server security from the CONTROL-M Configuration Manager, you must be authorized to use the CONTROL-M Configuration Manager.

Activate security by appropriately setting the Full Security system parameter.

**Figure 16  CONTROL-M/Server Security dialog box**
Adding, deleting and modifying users and groups

This section describes the following topics:

- Adding, deleting and modifying users and groups
- Assigning authorizations to users and groups
- Activating CONTROL-M/Server security
- Enabling passage of global conditions from GCS to CONTROL-M/Servers

Adding, deleting and modifying users and groups

Each CONTROL-M/EM user who performs actions affecting the CONTROL-M/Server database or jobs in the Active Jobs file must be defined in the CONTROL-M Security database. In addition, all users who can invoke CONTROL-M Security utilities must be defined in the CONTROL-M Security database.

To define users and groups (and to assign them privileges), you must have Full privileges.

To add a user or group


2. In the CONTROL-M/Server Security dialog box, click the down-arrow in the icon and select User or Group from the drop-down list.

3. In the dialog box, fill in the user or group details.

   **NOTE**
   
   To add a user to a group, the Group must already be defined.

4. Click OK.

To update or delete a user or group in the Security


2. In the CONTROL-M/Server Security dialog box, select the User or Group to modify or delete.

3. Perform either of the following:
Assigning authorizations to users and groups

When defining user or group authorizations, you must

- select the user or groups
- select the objects for which you authorizing that user or group
- select the authorizations that you are providing for those objects to the user or group

**NOTE**

For simplicity, the following steps will refer only to users, rather than users or groups. However, the steps apply to both users and group.


2. In the CONTROL-M/Server Security dialog box, select the user for which you are providing authorizations.

3. Define scheduling table authorizations for the user as follows:

   **A** Click the Scheduling Table tab.

   **B** To authorize the user for a scheduling table for which the user currently has not authorizations:

   1. Click the (New) icon below the tab name.

   2. Fill in the table name in the blank **Table** field.

   **C** For each possible action (delete, read, update, order), select whether you want to authorize (Yes/No/Default) the user for that action. Choose Default to apply the group authorization setting. If you select Default and the user does not belong to a group, the action will not be authorized (as if you selected No.)
Define authorizations that the job owner will have for the copies of the previously-defined scheduling tables that are placed in the Active Jobs file, as follows:

A Click the Authorized AJF tab.

B To authorize an owner that is not currently authorized for the user’s scheduling tables:

1. Click the (New) icon below the tab name.

2. Fill in the owner name in the blank Owner field.

C Specify the Node on which the owner will be authorized to perform actions on the scheduling tables in the Active Jobs file.

D Specify (Yes/No/Default) the actions (rerun, hold, confirm and so on) the owner will be permitted to perform on the tables in the AJF. Choose Default to apply the group authorization setting. If you select Default and the user does not belong to a group, the action will not be authorized (as if you selected No.)

Define authorizations that the user will have for the specific entities in the Active environment, as follows:

A Click the Entities tab.

B For each type of action (add, edit, delete) for each entity (calendar, condition, log, and so on), select whether you want to authorize (Yes/No/Default) the user to perform the action on the entity. Choose Default to apply the group authorization setting. If you select Default and the user does not belong to a group, the action will not be authorized (as if you selected No.)

6 To delete authorizations that you have defined, select the object in the appropriate tab, and click the (Delete) icon.

7 Click Apply to save the changes and leave the CONTROL-M/Server Security dialog box open. You can then select another user and repeat the process. (Or click OK to save the changes and close the dialog box).

Activating CONTROL-M/Server security

After defining CONTROL-M/Server security, you must activate it. You do this using the ctmsys utility. (In CONTROL-M for z/OS installations, activate CONTROL-M security by implementing Exit 7. For instructions, see the INCONTROL for z/OS Administrator Guide.)
Implementing CONTROL-M/Agent and remote host authorization security

To activate CONTROL-M/Server security

1 Display the CONTROL-M System Maintenance Utility Main Menu (ctmsys). For instructions on displaying the menu, see “Using the CONTROL-M System Maintenance Utility Main Menu” on page 47.

2 In the CONTROL-M System Maintenance Utility Main Menu, enter the number of the System Parameters option.

3 In the CONTROL-M System Parameters menu, if the Full Security system parameter is not set to Y, enter its option number to toggle it to Y.

4 Enter S to save the change.

Implementing CONTROL-M/Agent and remote host authorization security

To implement security for CONTROL-M agents and remote hosts, you must perform the following tasks:

- Implementing CONTROL-M/Agent job owner security (Windows only)
- Implementing CONTROL-M/Agent remote host security
- Authorizing which CONTROL-M/Server utilities a CONTROL-M/Agent can request

Implementing CONTROL-M/Agent job owner security (Windows only)

The following steps should be performed when using logging on as This account.

1 Log on to the CONTROL-M/Agent computer as a local administrator.

2 Choose Start => Settings => Control Panel => Administrative Tools => Local Security Policy.

3 In the displayed tree structure, select Local Policies.

4 In the displayed panel, double-click User Rights Assignments to display the list of user rights.
Implementing CONTROL-M/Agent remote host security

5 Double-click the user right you want to assign. The Local Security Policy Settings window for that user right is displayed.

A If the user who should have the selected user right is not listed in this window, click Add.

B In the bottom panel, enter the \domain\<user_name> of the user and click OK.

C When the specified user is displayed in the lower panel, click OK again.

6 Restart the agent services to make the user rights effective.

Implementing CONTROL-M/Agent remote host security

On an SSH remote host, the Job Owner must be an existing user in a remote host.

On a WMI remote host, the job owner must have the following authorizations:

■ The user needs to be Administrator on the remote host.

■ The user must have a write access to the SYSOUT directory on the remote host. To determine the SYSOUT directory of the remote host, do as the following:

   1. In the CONTROL-M Configuration Manager, right click the remote host and choose Properties.

   2. In the Remote Host Settings dialog box, select the appropriate CONTROL-M/Agents.

   The SYSOUT directory for WMI connection is listed at the bottom of the Connections area in the dialog box.

**NOTE**

Generally, WMI does not provide access to the network. To access the network, connect using a domain user, and grant DELEGATE impersonation level to the user and to any computer included in the chain of calls.
Authorizing which CONTROL-M/Server utilities a CONTROL-M/Agent can request

CONTROL-M/Agents might need to issue requests to CONTROL-M/Server to run a CONTROL-M/Server utility. For example:

- A job that runs on the agent may contain a command to run the ctmcreate CONTROL-M/Server utility.
- A user logs into the Agent account and manually runs the ctmcontb CONTROL-M/Server utility.

To prevent Agent users from submitting unauthorized commands and utility invocations to the Server, you define a separate list of allowable CONTROL-M/Server utilities for each agent.

The default CONTROL-M/Server utility list (listing all utilities) is located in the AGUTILS_PERMIT file in the CONTROL-M/Server data/AGDEFS directory.

To specify the list of utilities that an Agent can invoke

1. In the CONTROL-M/Server data/AGPERMIT_UTILS directory, create a file that has the same name as the Agent (in upper case letters).

2. In the file, list the CONTROL-M/Server utilities that are allowed to be run on the Agent. (You can copy names from the list in the AGUTILS_PERMIT file in the CONTROL-M/Server data/AGDEFS directory.)
Chapter 7 Implementing CONTROL-M security auditing

Conceptual overview

The Audit facility generates and stores a record in the CONTROL-M/EM database each time an audited activity is performed. You can use the Reporting facility to view audit records.

Figure 17 highlights the basic recommended workflow for implementing CONTROL-M auditing. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 23 on page 213. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.
Servers for auditing

The Global Alerts Server (GAS), GUI Server (GSR), and Configuration Management Server (CMS) handle audited activities separately:

- GAS records Alert activities.
- CMS records configuration and maintenance activities.
- GSR records scheduling activities.

If you change the value of the UserAuditContext system parameter while the GAS, GSR, or CMS is running, you must refresh the list of activities that each server handles.

Audit records

Audit records are stored in serial number order. They include the following information:

- sequential serial number
- timestamp indicating when the audited activity occurred
- name of the CONTROL-M/EM user
- host name or IP address from which the audited activity was performed
- name of the audited action (operation type)
- an indication of whether the authorization check succeeded
- separate fields for the attributes of each audited operation

For example, for Active Network activities, the following fields are included: data center name, scheduling table name, job name, memname, and order ID.
Recommended task summary

Table 23 lists specific tasks related to each phase of the workflow (Figure 17 on page 212). Subsequent sections provide step-by-step instructions.

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set up auditing</td>
<td>Enabling auditing</td>
<td>213</td>
</tr>
<tr>
<td></td>
<td>Setting which activities will be audited</td>
<td>214</td>
</tr>
<tr>
<td></td>
<td>Refreshing the list of activities handled by each server</td>
<td>215</td>
</tr>
<tr>
<td></td>
<td>Setting up or stopping automatic deletion of old audit records</td>
<td>215</td>
</tr>
<tr>
<td>View audit records</td>
<td>Viewing audit records</td>
<td>216</td>
</tr>
</tbody>
</table>

NOTE
For operations that change data values (such as updating quantitative resources or Zoom & Save), the value before the change is recorded in the Audit log.

Setting up auditing

This section explains how to use the UserAuditOn system parameter to enable auditing, and UserAuditContext to control which activities (for example, authentication, scheduling definition, or active job activities) to audit.

Enabling auditing

1 In the CONTROL-M Configuration Manager, choose Tools => System Parameters => CONTROL-M/EM System Parameters.

2 Double click the UserAuditOn system parameter (a CONTROL-M/EM system parameter of General type).

3 Set the value to 1 (default: 0, which disables auditing).

4 Click Save.
Setting which activities will be audited

1. In the CONTROL-M Configuration Manager, choose Tools => System Parameters => CONTROL-M/EM System Parameters.

2. Double click the UserAuditContext system parameter (a CONTROL-M/EM system parameter of General type).

   The default for UserAuditContext uses the following values:

   AUTH SCHED J_CONT J_INFO RES ALERT ACCOUNT CONFIG OPER CTMSEC DB_MAINT

3. To set an activity to be audited, include its value (as shown in Table 24 on page 214) in the UserAuditContext system parameter. To specify more than one value, separate the values with a blank space.

4. Click Save.

Table 24 Parameter values for activities to be audited

<table>
<thead>
<tr>
<th>Value</th>
<th>Activity</th>
</tr>
</thead>
<tbody>
<tr>
<td>ALL</td>
<td>all of the activities listed below</td>
</tr>
<tr>
<td>NONE</td>
<td>none of the activities listed below</td>
</tr>
<tr>
<td>AUTH</td>
<td>authentication (log on attempts, log offs, password actions)</td>
</tr>
<tr>
<td>SCHED</td>
<td>scheduling definition activities</td>
</tr>
<tr>
<td>J_CONT</td>
<td>active network activities (control requests)</td>
</tr>
<tr>
<td>J_INFO</td>
<td>active job information activities (log, sysout, statistics, and so on)</td>
</tr>
<tr>
<td>RES</td>
<td>resource activities (add, delete, or update resources and global prefixes)</td>
</tr>
<tr>
<td>ALERT</td>
<td>alerts</td>
</tr>
<tr>
<td>ACCOUNT</td>
<td>account management activities</td>
</tr>
<tr>
<td>CONFIG</td>
<td>configuration operations from CCM</td>
</tr>
<tr>
<td>OPER</td>
<td>start and stop components using the CCM</td>
</tr>
<tr>
<td>CTMSEC</td>
<td>CONTROL-M/Server security interface using the CCM</td>
</tr>
<tr>
<td>DB_MAINT</td>
<td>database maintenance operations using CCM</td>
</tr>
</tbody>
</table>

**NOTE**

CONTROL-M/EM clients, such as CONTROL-M/Desktop and CONTROL-M/EM GUI, have their own authorization checking mechanism. If an action does not pass a check at the client level, it is not sent to the CONTROL-M/EM server and a record for that action is not stored in the auditing table of the CONTROL-M/EM database.
Refreshing the list of activities handled by each server

If you change the values of the UserAuditOn or UserAuditContext system parameters while the GAS, GSR, or CMS is running, execute the following commands to refresh the list of activities handled by each server:

```
Ctl.exe -U EM_DBO -P EM_DBO_password -C GUI_Server [-M hostName | -name logicalNameGUIServer | -all] -cmdstr “REFRESH_AUDIT”

Ctl.exe -U EM_DBO -P EM_DBO_password -C GAS [-M hostName | -name logicalNameGAS | -all] -cmdstr “REFRESH_AUDIT”

Ctl.exe -U EM_DBO -P EM_DBO_password -C CMS [-M hostName | -name CMS | -all] -cmdstr “REFRESH_AUDIT”
```

Setting up or stopping automatic deletion of old audit records

By default, the GUI server automatically cleans up audit records from the CONTROL-M/EM database at an interval of every 360 minutes (on both UNIX and Windows).

Using the CONTROL-M/EM System Parameters dialog box, which you access from the CONTROL-M Configuration Manager, you can adjust the audit-related system parameters as necessary.

To set up or disable automatic audit record deletion

1. In the CONTROL-M Configuration Manager, choose Tools => System Parameters. The CONTROL-M/EM System Parameters window is displayed.

2. Scroll to the relevant audit system parameter (all belong to the general type, in the Type field) to see its currently defined value. The following is the list of audit system parameters and what they do:

   - AuditCleanupOn—when set to 1 (default), automatic audit log cleanup is enabled; when set to 0, automatic audit log cleanup is disabled

   - AuditCleanupIntervalMinutes—sets the cleanup interval in minutes (default: 360)

   - AuditHistoryDays—sets the number of days to retain audit information before deleting it from the CONTROL-M/EM database (default: 1)
Viewing audit records

- MaxAuditsToDelete—sets the maximum number of audit records to delete during each automatic cleanup operation (default: 200,000)

3 To modify a value of an audit system parameter

   A Select the parameter and click Update.
   
   B Adjust the value.
   
   C Click Save.

4 Execute the following command to refresh all audit-related system parameters:

```
ctl -U dboUser -P dboPassword -C CMS {-M hostName | -name CMSLogicalName | -all} -cmdstr "REFRESH_AUDIT"
```

5 When the next cleanup operation begins, verify that the cleanup is performed according to the new values for the system parameters.

Viewing audit records

To view the records generated when an audited activity occurs, use the Reporting facility as instructed in the CONTROL-M User Guide.
Setting up CONTROL-M firewall security

This chapter presents the following topics:

Conceptual overview ................................................................................................................ 217
  Communication between CONTROL-M/EM clients and servers ......................... 218
  Communication between CONTROL-M/Server and CONTROL-M/EM .......... 219
  Communication between agents and CONTROL-M/Server ............................... 219
Recommended task summary .............................................................................................. 221
Enabling communication between CONTROL-M/EM clients and servers ............ 222
Enabling communication between CONTROL-M/Server and CONTROL-M/EM 223
Enabling communication between agents and CONTROL-M/Server .................. 224

Conceptual overview

Because CONTROL-M components can be spread across multiple computers, firewall security at your site can disrupt the flow of communication between CONTROL-M components outside the firewall and those inside the firewall. Depending on your CONTROL-M and firewall configuration, the following flows might be impacted:

- flows from client components to CONTROL-M/EM server components
- flows between CONTROL-M/Servers and CONTROL-M/EM
- flows from CONTROL-M/Agent (or remote host) components to CONTROL-M/Server

To enable CONTROL-M components to communicate through firewalls, you must establish suitable port definitions. Figure 18 on page 218 highlights the basic recommended workflow. This overview section explains concepts that are related to the workflow.
Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

Figure 18  Recommended workflow for setting up firewall security

Communication between CONTROL-M/EM clients and servers

This is the most common communication flow issue because many client components operate outside the firewall and must communicate with CONTROL-M/EM servers through the firewall.

Before a client can initiate communication with a CONTROL-M/EM server, it must first retrieve the address of the server from the naming service. Once it has the address, it can communicate with the server.

To enable a client to communicate with a CONTROL-M/EM server, you must:

- open a port in the firewall and define that port to the Naming Service
- open a port in the firewall and define that port to the server

**NOTE**
This applies to CORBA servers (GSR, GAS, BIM, FORECAST and CMS). It does not apply to GCS server.

GUI clients (CONTROL-M/EM and CONTROL-M/Desktop) do not communicate directly with the BIM server. They go through the GSR server to the BIM server.
Some client actions (for example, opening a ViewPoint or uploading tables) require that the server return communication (callback) to the client. By default (bidirectional IIOP), the server can call back using the same port used by the client to communicate with the server. BMC Software recommends that you not change this default.

- If you change the default from bidirectional IIOP, and if callback is necessary, you must open a port in the firewall and define it to the client to enable the client to listen to communication from the server.

(Bidirectional IIOP is described in “Bidirectional IIOP” on page 389.

---

**NOTE**

Bidirectional communication is enabled only if both client and server are configured to use it.

---

**Communication between CONTROL-M/Server and CONTROL-M/EM**

Some sites have CONTROL-M/Servers operating off-site. For example, servers belonging to branch outlets might connect to the main branch. These CONTROL-M/Servers are often outside the firewall of the CONTROL-M/EM site. In addition, these CONTROL-M/Servers might have their own firewalls. Therefore, firewalls might interrupt the information flow between CONTROL-M/EM and CONTROL-M/Server in both directions.

---

**Communication between agents and CONTROL-M/Server**

CONTROL-M/Agents normally send information to their CONTROL-M/Server. (Remote hosts send information to CONTROL-M/Agent which sends this information to the CONTROL-M/Server. However, remote hosts do not open connections to Agents; therefore there should be no firewall problem.)

If CONTROL-M/Server is located behind a firewall on your internal network, and the CONTROL-M/Agents that communicate with this server are on the other side of your firewall (on your internal network or on an external network), the agent to server port is blocked. As a result, CONTROL-M/Server can connect to CONTROL-M/Agent, but CONTROL-M/Agent cannot connect to CONTROL-M/Server.
The recommended solution to this problem involves selecting the appropriate communication model. The following types of agent-to-server connection models are available:

- **transient connection**

  This type is the default model used with new and upgrade installations.

- **persistent connection model**

  This optional connectivity model between the server and agent is recommended for components on different sides of the firewall. It improves performance and avoids potential problems when establishing a connection.

These types of connection models are described below.

**Transient connection model**

In the transient connection model, CONTROL-M/Server initiates a connection with the CONTROL-M/Agent Listener process to submit jobs and other action requests. In contrast, the Agent Tracker and Agent Utilities only open a connection to CONTROL-M/Server when they need it. Once the purpose for opening these connections is finished, the connection terminates.

However, if CONTROL-M/Server sits behind a firewall, the Agent Tracker and Agent Utilities are not able to open a connection to the server. As a result, Agent Utilities cannot be run and job statuses are updated only upon server request, approximately once every 15 minutes.
Persistent connection model

In the persistent connection model, the connection between the server and agent is constant and can be initiated by both the server and agent. Upon startup of the agent, the Agent Router process is started and acts as a broker between the other agent components and the server.

The Agent Router process allows CONTROL-M/Server to maintain a constant connection with the agent. However, when CONTROL-M/Server sits behind a firewall, the Agent Router cannot initiate the connection with the server. Once the server creates the connection to the Agent Router, the Agent Tracker and Agent Utilities processes use this connection to communicate freely with the server.

Recommended task summary

The following sections provide step-by-step instructions on each phase of the workflow diagramed in Figure 18 on page 218:

- “Enabling communication between CONTROL-M/EM clients and servers” on page 222
- “Enabling communication between CONTROL-M/Server and CONTROL-M/EM” on page 223
- “Enabling communication between agents and CONTROL-M/Server” on page 224
Enabling communication between CONTROL-M/EM clients and servers

1 Open and define ports in the firewall, as follows:

A Open a port in the firewall and define it to the Naming Service (default Naming Service port: 13075), to enable the Naming Service to listen for communication from the client.

B Use the Ports panel of the Domain Configuration window (this window is often called the orbconfigure GUI) to open ports in the firewall and define them to the server components to enable the server to listen for communication from the client. For instructions, see “Assigning ports” on page 398.

NOTE
If you are not using Windows, you can use the orbadmin utility instead of the orbconfigure utility. For instructions on using the orbadmin utility, see the CONTROL-M Utility Guide.

BMC Software recommends the following when opening and defining ports:

- use the default communication policy (bidirectional IIOP between CORBA components and clients)

- open and define a range of ports for client applications such as the CONTROL-M/EM GUI, Desktop and CLI, so that more than one session can run simultaneously on the same machine

- assign a static port or a range of ports to each CONTROL-M/EM server application instead of using the default setting: random ports

2 If you choose to use non-bidirectional IIOP communication policy, open the assigned ports for incoming connections. In this case, all ports should be open for outgoing connections on the server’s side. (These ports are only used by server applications, and client applications that use callback objects but do not use bidirectional IIOP.)

3 For each relevant CONTROL-M/EM server component for which communication passes through a firewall, select Tools => System Parameters in the CONTROL-M Configuration Manager, and use the HostPort system parameter to assign the port to the server component (assign a unique name to the server component and specify the number of the port number to which the server component will listen).
If communication between the CONTROL-M Configuration Manager and a Configuration Agent supervising certain CONTROL-M/EM components passes through a firewall, use the HostPort parameter to assign a specific port to the Configuration Agent, and then open the port in the firewall.

4 Register the ports in your firewall. For information about how to register port numbers in your firewall, see the documentation provided with your firewall software.

---

**Enabling communication between CONTROL-M/Server and CONTROL-M/EM**

To enable communication between CONTROL-M/Server and a CONTROL-M/EM component, a port must be opened in the firewall and defined on the CONTROL-M/Server.

---

**NOTE**

When you define a port in CONTROL-M/Server, two ports are actually defined (each for communication flow in the opposite direction), and you must open both of them in the firewall.

- If your site uses Discovery (see “Defining a CONTROL-M/Server (automatic discovery method)” on page 57), the port is automatically defined, and you can open it using the CONTROL-M Configuration Manager. This section describes how to use the CONTROL-M Configuration Manager to open ports when you do not use Discovery.

**To open ports between CONTROL-M/Servers and CONTROL-M/EM to through a firewall when Discovery is enabled**

1 For each CONTROL-M/Server, select Tools => System Parameters => CONTROL-M/EM System Parameters in the CONTROL-M Configuration Manager.

2 In the HostPort system parameter, define the CONTROL-M/Server port as open for incoming communication.
Enabling communication between agents and CONTROL-M/Server

To enable CONTROL-M/Server to connect to an agent through a firewall, you should:

- open a port in the firewall as follows:
  - if the server is behind a firewall, open an Agent to Server port
  - if the agent is behind a firewall, open a Server to Agent port
- set the agent communication mode to persistent
- in the agent, modify the settings so that it does not attempt to connect to the server. Otherwise, the agent will keep attempting and failing to open a connection to the CONTROL-M/Server (through the firewall).

With a persistent connection, the connection between server and agent is constant and can be initiated by either the server or the agent.

To set the communication mode to persistent between the server and the agent

1. Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. Select the Parameter Customization Menu and press <Enter>.

3. Select the Parameters for Communicating with Specific Agent computers option and press <Enter>.

4. Specify the agent name and press <Enter>.

5. From the Parameters for Communicating with Specific Agent computers menu, select Persistent Connection and press <Enter>.


7. Enter S (Save) to save the modified parameters and to transfer the current connection configuration to the specified agent.

**NOTE**

When you save the changes, CONTROL-M/Server sets Persistent Connection with the new value and attempts to connect to the specific agent. When a connection is established with the agent, the new configuration is transferred to the agent. The updated agent is reset. This process can take a few minutes.
To set the agent so that it does not attempt to connect to the server

1 In the CONTROL-M Configuration Manager, right click the CONTROL-M/Agent and choose CONTROL-M/Agent System Parameters.

   The CONTROL-M/Agent System Parameters window displays the system parameters and values for the selected CONTROL-M/Agent.

2 Double click the Allow Comm Init parameter.

3 Set the value to N.

4 Click Save.
Configuring CONTROL-M for high availability

This chapter presents the following topics:

- Conceptual overview .......................................................... 228
- Methods of ensuring high availability .................................. 228
- Mirroring and failover ......................................................... 229
- Recommended task summary ................................................ 230
- Preparing to implement mirroring or failover ......................... 231
  - Reviewing prerequisites .................................................... 231
  - Gathering worksheet data ............................................... 232
  - Performing additional preparations .................................... 241
  - Preparing the failover CONTROL-M/Server .......................... 245
- Implementing database mirroring .......................................... 247
  - Building and initializing a new CONTROL-M mirror database .... 247
  - Changing over to the mirror database following primary database failure .... 249
  - Changing back to the primary database after fixing the problem .... 250
  - Disabling mirroring .......................................................... 250
- Implementing Failover ......................................................... 251
  - Initializing the failover system .......................................... 252
  - Changing over to the failover CONTROL-M/Server in an emergency .... 254
  - Changing back to the primary CONTROL-M/Server after fixing the problem .... 255
  - Disabling the failover system .......................................... 256
- Periodically synchronizing the primary and mirror database ......... 257
Conceptual overview

Ensuring high availability means ensuring that CONTROL-M is able to continue functioning and processing your production environment without interruption. This generally means having some kind of fallback mechanism in place that can replace failed components.

Methods of ensuring high availability

CONTROL-M supports a variety of high availability solutions at the following levels:

- application
- database
- server

The main methods of ensuring high availability are implementing any of the following

- CONTROL-M/Server Mirroring and failover—described in this chapter.
- Cluster and Disaster Recovery solutions
  
  Cluster implementation is characterized by the following:
  
  — CONTROL-M is installed on a shared disk
  
  — CONTROL-M components communicate using a virtual host name and virtual IP address
  
  — Cluster software is configured to automatically and immediately switch CONTROL-M to a secondary node in case of failure (whereas mirroring and failover require manual intervention to switch over)

  Disaster recovery is similar to clusters, except that the fallback mechanism is at a remote site, ensuring that if a disaster such as a fire disrupts the primary location, it is unlikely to disrupt the secondary location.

  Cluster and Disaster Recovery solution implementation is described in the Clusters topic in the CONTROL-M Installation Guide.

- Oracle DataGuard Support (3rd party database vendor solution)—allows replicating CONTROL-M database to a standby location. Similar to cluster implementation, when the primary site fails, a mirrored file system is brought online on the remote secondary site (using a designated storage device).
Its implementation with CONTROL-M described in the technical support bulletin posted on the BMC Customer support site at:


Figure 21 highlights the basic recommended workflow for configuring CONTROL-M for high availability. This overview section explains concepts that are related to the workflow.

**Figure 21  Recommended workflow for configuring CONTROL-M for high availability**

For specific tasks that correspond to each phase of the workflow, see Table 25 on page 231. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

**Mirroring and failover**

Mirroring involves setting up a secondary (mirror) CONTROL-M/Server database that maintains a mirror image of your primary database. If the primary database server fails or the primary database loses integrity, CONTROL-M/Server can continue by using the mirror database until the primary database becomes available again.

Failover takes high availability one step further than mirroring. With failover, you implement a secondary installation that includes a secondary (failover) CONTROL-M/Server in addition to a secondary database. This provides fallback not only in case of primary database disruption but in case of primary CONTROL-M/Server disruption.
The failover CONTROL-M/Server implementation utilizes the same agents and remote hosts as the primary CONTROL-M/Server installation.

To implement database mirroring or failover you must initialize (configure and define) the secondary components.

Once failover or mirroring has been implemented, if a disruption occurs, you must:

- manually shift processing over to the secondary system
- correct the problem on your primary system
- perform the necessary steps required to return processing to the primary system

**NOTE**

Once you have implemented database mirroring, CONTROL-M keeps the primary and secondary databases synchronized. However, if you run utilities to update the CONTROL-M database, you must perform database initialization again (synchronize the primary and secondary databases). For details, see “Periodically synchronizing the primary and mirror database” on page 257.

**Recommended task summary**

Table 25 lists specific tasks related to each phase of the workflow (Figure 21 on page 229). Subsequent sections provide step-by-step instructions.
Preparing to implement mirroring or failover

Before you can implement mirroring or failover, you must prepare for the implementation. This involves performing the following tasks:

- **Reviewing prerequisites** on page 231
- **Gathering worksheet data** on page 232
- **Performing additional preparations** on page 241

Be sure to complete the tasks in this section before implementing mirroring or failover.

### Reviewing prerequisites

Before proceeding, review the following requirements and guidelines, which are relevant to the tasks in this chapter:

---

**Table 25  Task summary: configuring CONTROL-M for high availability**

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Prepare to implement mirroring or failover</strong></td>
<td>Reviewing prerequisites</td>
<td>231</td>
</tr>
<tr>
<td></td>
<td>Gathering worksheet data</td>
<td>232</td>
</tr>
<tr>
<td></td>
<td>Performing additional preparations</td>
<td>241</td>
</tr>
<tr>
<td></td>
<td>Preparing the failover CONTROL-M/Server</td>
<td>245</td>
</tr>
<tr>
<td><strong>Implement database mirroring</strong></td>
<td>Building and initializing a new CONTROL-M mirror database</td>
<td>247</td>
</tr>
<tr>
<td></td>
<td>Changing over to the mirror database following primary database failure</td>
<td>249</td>
</tr>
<tr>
<td></td>
<td>Changing back to the primary database after fixing the problem</td>
<td>250</td>
</tr>
<tr>
<td><strong>Implement failover</strong></td>
<td>Initializing failover on the primary and secondary computers</td>
<td>252</td>
</tr>
<tr>
<td></td>
<td>Changing over to the failover CONTROL-M/Server in an emergency</td>
<td>254</td>
</tr>
<tr>
<td></td>
<td>Changing back to the primary CONTROL-M/Server after fixing the problem</td>
<td>255</td>
</tr>
<tr>
<td></td>
<td>Disabling the failover system</td>
<td>256</td>
</tr>
<tr>
<td><strong>Periodically synchronize the primary and mirror databases</strong></td>
<td>Periodically synchronizing the primary and mirror database</td>
<td>257</td>
</tr>
</tbody>
</table>
Gathering worksheet data

- Ensure that database and account names that you create conform to your database vendor’s naming conventions.
- Verify that the database server that you want to use for mirroring is running.
- *(Oracle databases only)* Ensure that the listener is running.
- *(PostgreSQL databases only)* Ensure that the PostgreSQL server is running.
- If you plan to build a mirror database from scratch, you will need the password of the database vendor’s system administrator.

Gathering worksheet data

You need to collect the following types of information to perform the following tasks:

- database parameters—to prepare a secondary (mirror) database server
- mirroring parameters—to initialize the mirror database
- environment variables—to initialize the failover server

This section provides worksheets to help you collect this information. Be sure to fill in the worksheets relevant to the type of database server.

Table 26 identifies by database server type and information type the relevant worksheet table number and page.

**Table 26 Relevant worksheet tables by database server type**

<table>
<thead>
<tr>
<th>Server type</th>
<th>Information to be gathered</th>
<th>See: table on page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase</td>
<td>Database parameters</td>
<td>Table 27 on page 233</td>
</tr>
<tr>
<td></td>
<td>Mirroring parameters (for copying)</td>
<td>Table 28 on page 233</td>
</tr>
<tr>
<td></td>
<td>Mirroring parameters (for building)</td>
<td>Table 29 on page 234</td>
</tr>
<tr>
<td></td>
<td>Environment variables</td>
<td>Table 30 on page 235</td>
</tr>
<tr>
<td>Oracle</td>
<td>Database parameters</td>
<td>Table 31 on page 236</td>
</tr>
<tr>
<td></td>
<td>Mirroring parameters</td>
<td>Table 32 on page 236</td>
</tr>
<tr>
<td></td>
<td>Environment variables</td>
<td>Table 33 on page 237</td>
</tr>
<tr>
<td>MSSQL</td>
<td>Database parameters</td>
<td>Table 34 on page 237</td>
</tr>
<tr>
<td></td>
<td>Mirroring parameters</td>
<td>Table 35 on page 238</td>
</tr>
<tr>
<td></td>
<td>Environment variables</td>
<td>Table 36 on page 238</td>
</tr>
<tr>
<td>PostgreSQL</td>
<td>Database parameters</td>
<td>Table 37 on page 239</td>
</tr>
<tr>
<td></td>
<td>Mirroring parameters</td>
<td>Table 38 on page 239</td>
</tr>
<tr>
<td></td>
<td>Environment variables</td>
<td>Table 39 on page 240</td>
</tr>
</tbody>
</table>
Gathering worksheet data

Gathering Sybase information

Worksheet for database parameters (Sybase)

You will need these values when you prepare the secondary (mirror) database server.

<table>
<thead>
<tr>
<th>Database</th>
<th>Parameters</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase</td>
<td>Sybase Host Name</td>
<td>host name of the computer that runs the Sybase SQL Server to be used for mirroring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Sybase Port Number</td>
<td>Sybase Port Number - TCP/IP query port number for the Sybase SQL Server to be used for mirroring</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Use the Sybase dsedit utility to find this value. For more information about the Sybase dsedit utility, see Sybase documentation.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>User connection</td>
<td>For more information, see the CONTROL-M/Server and CONTROL-M/Agent Installation Guide.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Memory</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Locks</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

a If you change the value of any Sybase parameter, the change will not be implemented until you restart Sybase SQL Server.

Worksheet for mirroring parameters—when copying a database (Sybase)

When you initialize the mirror database by copying, prepare the values in Table 28.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-M Mirror Database Owner (DBO)</td>
<td>Name of the CONTROL-M/Server Mirror database owner. This name is used by CONTROL-M when accessing the mirror database. When copying to an existing database, this user must already be defined on the database server.</td>
<td></td>
</tr>
<tr>
<td>DBO password</td>
<td>Password for the CONTROL-M/Server database user. The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the CONTROL-M/Server database.</td>
<td></td>
</tr>
<tr>
<td>Mirror Database (Data Portion) Size</td>
<td>Amount of space (in MB) to allocate for the data portion of the CONTROL-M/Server Mirror database. This value is taken from the current size of the primary database. It cannot be modified. Verify that the secondary database server can host a database of this size.</td>
<td></td>
</tr>
</tbody>
</table>
Worksheet for mirroring parameters—when building a database (Sybase)

You will need these values when you initialize (by building) the mirror database.

Table 28 Worksheet for mirroring parameters (when copying)—Sybase (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase Interface Directory</td>
<td>Directory in which the Sybase interface file is located.</td>
<td></td>
</tr>
<tr>
<td>Mirror Sybase Host Name</td>
<td>Name of the host computer for the mirror Sybase Database server.</td>
<td></td>
</tr>
<tr>
<td>Mirror Sybase Port Number</td>
<td>The communications port on which the secondary database server listens for queries.</td>
<td></td>
</tr>
<tr>
<td>Mirror Sybase server name</td>
<td>Name of the mirror database server. This entry is automatically added to the primary database’s interfaces file. This value should be unique.</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M Mirror database name</td>
<td>Name for the CONTROL-M/Server Mirror database. This name must be unique. When copying to an existing database, this database must already be defined on the database server.</td>
<td></td>
</tr>
</tbody>
</table>

Table 29 Worksheet for mirroring parameters (when building)—Sybase (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Owner Login</td>
<td>Name of the CONTROL-M Mirror database owner. This name is used by CONTROL-M when accessing the mirror database. When building a new mirror database, the initialization script creates this user on the database server.</td>
<td></td>
</tr>
<tr>
<td>Database Administrator Login</td>
<td>Name of the database administrator.</td>
<td></td>
</tr>
<tr>
<td>Database Administrator Password</td>
<td>Password of the database administrator.</td>
<td></td>
</tr>
<tr>
<td>Database Owner Password</td>
<td>Password for the CONTROL-M/Server Mirror database owner (6 to 30 characters, alphanumeric). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the mirror database.</td>
<td></td>
</tr>
<tr>
<td>Database Name</td>
<td>Name for the CONTROL-M/Server Mirror database. This name must be unique within the Sybase SQL server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ When building a new mirror database, the initialization script creates this database on the database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ When copying to an existing database, this database must already be defined on the database server.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 29  Worksheet for mirroring parameters (when building)—Sybase (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Size</td>
<td>Amount of space (in MB) to allocate for the data portion of the CONTROL-M/Server Mirror database. This value is taken from the current size of the primary database. It should not be modified. Verify that the secondary database server can host a database of this size. Verify that this value is the same as the primary database.</td>
<td></td>
</tr>
<tr>
<td>Sybase Interface Directory</td>
<td>Full path to the Sybase interfaces file on the primary system. This value is displayed and can be modified by changing the value of the Installed Sybase root directory parameter.</td>
<td></td>
</tr>
<tr>
<td>Installed Sybase server alias name</td>
<td>The Sybase alias name as listed in Sybase interfaces file.</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M Mirror Database Data Device Name</td>
<td>Name of the Sybase device that will be created for the data portion of the CONTROL-M/Server Mirror database.</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M Mirror Database Log Device Name</td>
<td>Name of the Sybase device that will be created for the log portion of the CONTROL-M/Server Mirror database.</td>
<td></td>
</tr>
<tr>
<td>Data Physical Device Path Name</td>
<td>Full path or physical device name where the mirror database will be located on the secondary database server. Specifying a pathname initiates a File-based installation. Specifying a device name initiates an installation to a Raw partition.</td>
<td></td>
</tr>
<tr>
<td>Log Physical Device Path Name</td>
<td>Full path or physical device name where the mirror database’s log database will be located on the secondary database server. Specifying a pathname initiates a File-based installation. Specifying a device name initiates an installation to a Raw partition.</td>
<td></td>
</tr>
</tbody>
</table>

### Worksheet for environment variables (Sybase)

You will need these values when initialize the failover server.

### Table 30  Worksheet for environment variables and alternative names—Sybase

<table>
<thead>
<tr>
<th>Field name</th>
<th>Equivalent name</th>
<th>To specify the value, run this command</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Owner Login</td>
<td>CONTROL-M Mirror Database Owner (DBO)</td>
<td>echo $CONTROLM_USER</td>
<td></td>
</tr>
<tr>
<td>Database Name</td>
<td>CONTROL-M Mirror database name</td>
<td>echo $CONTROLM_DATABASE</td>
<td></td>
</tr>
<tr>
<td>Sybase Server Query Port Number</td>
<td>Mirror Sybase Port number</td>
<td>sybedit (Sybase utility)</td>
<td></td>
</tr>
<tr>
<td>Sybase Server Host Name</td>
<td>Mirror Sybase Host name</td>
<td>sybedit (Sybase utility)</td>
<td></td>
</tr>
</tbody>
</table>
**Gathering Oracle information**

**Worksheet for database parameters (Oracle)**

You will need these values when you prepare the secondary (mirror) database server.

<table>
<thead>
<tr>
<th>Database</th>
<th>Parameters</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oraclea</td>
<td>Oracle SID</td>
<td>server ID of the secondary database server</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Host Name</td>
<td>host name of the computer that runs the Oracle SQL Server to be used for mirroring</td>
<td></td>
</tr>
<tr>
<td>Oracle</td>
<td>Oracle Port Number</td>
<td>TCP/IP query port number for the Oracle SQL Server used for mirroring</td>
<td></td>
</tr>
</tbody>
</table>

* To find the values for these Oracle parameters, run the following command on the secondary server: `echo $ORACLE_SID`. Based on the results, use the found entry to run the following command: `cat $TNS_ADMIN/listener.ora`. (If this command does not work, the default location is: `cat <oracleHome>/product/<version>/network/admin/listener.ora`.)

**Worksheet for mirroring parameters (Oracle)**

You will need these values when you initialize the mirror database.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-M Mirror Database Owner (DBO)</td>
<td>Name of the CONTROL-M/Server Mirror database owner. This name is used by CONTROL-M when accessing the mirror database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- When <em>building</em> a new mirror database, the initialization script creates this user on the database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- When <em>copying</em> to an existing database, this user must already be defined on the database server.</td>
<td></td>
</tr>
<tr>
<td>DBO password</td>
<td>Password for the CONTROL-M/Server database user. The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the CONTROL-M/Server database.</td>
<td></td>
</tr>
<tr>
<td>Mirror Oracle Host Name</td>
<td>The host computer name of an existing Oracle server.</td>
<td></td>
</tr>
<tr>
<td>Mirror Oracle Port Number</td>
<td>The communication port of the Oracle Database Server.</td>
<td></td>
</tr>
<tr>
<td>Mirror Oracle Instance Name (SID)</td>
<td>The Server ID of the Oracle Database Server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To find out this name use the following command on the mirror database server: <code>echo $ORACLE_SID</code></td>
<td></td>
</tr>
</tbody>
</table>
Gathering worksheet data

Chapter 9 Configuring CONTROL-M for high availability 237

Worksheet for environment variables (Oracle)

You will need these values when initialize the failover server.

Table 33  Worksheet for environment variables—Oracle

<table>
<thead>
<tr>
<th>Variable</th>
<th>To determine the value, do this</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-M Mirror Database owner (DBO)</td>
<td>Run the <code>echo $CONTROLM_USER</code> command</td>
<td>[value]</td>
</tr>
<tr>
<td>Mirror Oracle Host Name</td>
<td>Check the <code>tnsnames.ora</code> file. For more information about <code>tnsnames.ora</code>, see Oracle documentation.</td>
<td>[value]</td>
</tr>
<tr>
<td>Mirror Oracle Port Number</td>
<td>Check the <code>tnsnames.ora</code> file. For more information about <code>tnsnames.ora</code>, see Oracle documentation.</td>
<td>[value]</td>
</tr>
<tr>
<td>Mirror Oracle Instance name (SID)</td>
<td>Run the <code>echo $ORACLE_SID</code> command</td>
<td>[value]</td>
</tr>
</tbody>
</table>

Gathering MSSQL information

Worksheet for database parameters (MSSQL)

You will need these values when you prepare the secondary (mirror) database server.

Table 34  Worksheet for database parameter values—MSSQL

<table>
<thead>
<tr>
<th>Database</th>
<th>Parameters</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS SQL</td>
<td>MSSQL Host Name</td>
<td>host name of the computer that runs the MSSQL Server to be used for mirroring</td>
<td>[value]</td>
</tr>
</tbody>
</table>
Worksheet for mirroring parameters (MSSQL)

You will need these values when you initialize the mirror database.

Table 35 Worksheet for MSSQL Server mirroring parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror Database Server Name</td>
<td>Specify a name for the mirror Database Server.</td>
<td></td>
</tr>
<tr>
<td>Mirror CONTROL-M/Server Database</td>
<td>Name of the CONTROL-M/Server Database that will be a mirror of the primary database.</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M/Server Mirror DBO Username</td>
<td>Name of the database server administrator.</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M/Server Mirror DBO Password</td>
<td>Password for the CONTROL-M/Server database owner. The password must begin with a letter (A-Z, a-z) followed by 5 to 29 alpha-numeric characters (includes underscores). If the specified password is longer than 30 characters, only the first 30 are accepted. Default: password</td>
<td></td>
</tr>
<tr>
<td>Confirm DBO Password</td>
<td>Re-enter the Database Owner Password, confirming its correctness.</td>
<td></td>
</tr>
</tbody>
</table>

Worksheet for environment variables (MSSQL)

You will need these values when initialize the failover server.

Table 36 Worksheet for MSSQL environment variables—MSSQL

<table>
<thead>
<tr>
<th>Variable</th>
<th>To determine the value, check this registry name</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mirror Database Server Name</td>
<td>SQLSRVRNAME</td>
<td></td>
</tr>
<tr>
<td>Mirror CONTROL-M/Server Database</td>
<td>CONTROLM_DATABASE</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M/Server Mirror DBO User Name</td>
<td>DBO Owner</td>
<td></td>
</tr>
<tr>
<td>Database Owner Login</td>
<td>DBO Owner</td>
<td></td>
</tr>
</tbody>
</table>
Gathering PostgreSQL information

Worksheet for database parameters (PostgreSQL)

Table 37  Worksheet for database parameter values—PostgreSQL

<table>
<thead>
<tr>
<th>Database</th>
<th>Parameters</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PostgreSQL(^a)</td>
<td>Host Interface Name</td>
<td>host name of the computer that runs the PostgreSQL Server to be used for mirroring</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Port Number</td>
<td>PostgreSQL Port Number - TCP/IP query port number for the PostgreSQL Server to be used for mirroring</td>
<td></td>
</tr>
</tbody>
</table>

\(^a\) The value for the PostgreSQL port parameter is located in the `<PostgreSQL Home>/data/postgresql.conf` file, under the CONNECTIONS AND AUTHENTICATION section, on the line beginning with the word “port.” This is located on the computer on which the secondary (mirror) database server will be installed. In Windows, the details are located in `<CONTROL-M/Server home directory>/pgsql/etc/pg_service.conf`.

Worksheet for mirroring parameters (PostgreSQL)

You will need these values when you build the mirror database.

Table 38  Worksheet for mirroring parameters—PostgreSQL (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Interface Name</td>
<td>Name of the host computer for the mirror PostgreSQL database server.</td>
<td></td>
</tr>
<tr>
<td>Port Number</td>
<td>The communications port on which the mirror PostgreSQL database server listens for queries.</td>
<td></td>
</tr>
<tr>
<td>Database Owner Login</td>
<td>Name of the CONTROL-M/Server Mirror database owner. This name is used by CONTROL-M when accessing the mirror database. When building a new mirror database, the initialization script creates this user on the database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note: Do not use upper-case letters.</td>
<td></td>
</tr>
<tr>
<td>Database Owner Password</td>
<td>Password for the CONTROL-M Mirror database owner (6 to 30 characters, alphanumeric). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the mirror database.</td>
<td></td>
</tr>
<tr>
<td>Database Administrator Password</td>
<td>Password of the mirror PostgreSQL database server administrator. The characters you enter are not echoed for security reasons.</td>
<td></td>
</tr>
</tbody>
</table>
### Worksheet for environment variables (PostgreSQL)

**Table 38 Worksheet for mirroring parameters — PostgreSQL (part 2 of 2)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Name</strong></td>
<td>Name for the CONTROL-M/Server Mirror database. This name must be unique within the mirror PostgreSQL database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ When building a new mirror database, the initialization script creates this database on the database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ When copying to an existing database, this database must already be defined on the database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not use upper-case letters.</td>
<td></td>
</tr>
<tr>
<td><strong>Database Location</strong></td>
<td>Location of the CONTROL-M/Server Mirror database owner.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You must create this location prior to installing the CONTROL-M/Server mirror database. The location must be empty.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This is relevant only when the PostgreSQL database used for the mirror database is located on UNIX. The recommended location should be a new and empty directory under <code>&lt;owner user home directory&gt;/pgsql</code>.</td>
<td></td>
</tr>
<tr>
<td><strong>Existing Database</strong></td>
<td>Valid values:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>Y</strong> — This value indicates that the CONTROL-M/Server database is defined on a remote PostgreSQL database server.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ <strong>N</strong> — This value indicates that the CONTROL-M/Server database is defined on the local PostgreSQL database server.</td>
<td></td>
</tr>
</tbody>
</table>

**Table 39 Worksheet for environment variables and alternative names— PostgreSQL (part 1 of 2)**

<table>
<thead>
<tr>
<th>Field name</th>
<th>Equivalent name</th>
<th>To view the value</th>
<th>Your value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database Owner Login</td>
<td>CONTROL-M Mirror Database Owner (DBO)</td>
<td>In UNIX, run this command: echo <code>$CONTROL_MIRROR_USER</code></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>In Windows, go to this registry key: MIRROCircle Owner</td>
<td></td>
</tr>
</tbody>
</table>
Performing additional preparations

This section describes additional preparations and requirements by database server type. Be sure to perform the additional preparations before implementing mirroring or failover.

Additional preparations—Sybase server

1 Ensure that you do not change the values for the parameters listed in Table 27.

   If you change the value of any of these parameters, the change will not be implemented until you shut down and restart the Sybase SQL Server.

2 Prepare the additional details listed in Table 40.

Table 40 Additional required details—Sybase

<table>
<thead>
<tr>
<th>Details required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A database name and a database owner (DBO) name for the mirror database.</td>
<td>The database name can be the same as the database owner name, but the database name and database owner name must each be unique for a particular Sybase SQL Server. Therefore, when selecting names for the CONTROL-M/Server database (using an existing Sybase SQL Server), verify that the database name and database owner name are unique for the Sybase SQL Server.</td>
</tr>
</tbody>
</table>
Performing additional preparations

If you will be building a database, you must supply values for the database owner, database name, devices and file or partition paths:

- Specifying existing owner name, database name, and device assignments will erase and recreate these database elements.
- Specifying new, unique values for owner name, database name, and device assignments will build a new database on the server.

Every computer type uses a different character set for Sybase. If the character set for the primary database and mirror database are not the same, the character set for the primary database must be installed on the mirror Sybase SQL Server. Use the `sp_configure` command to configure the character set for the existing SQL Server.

### Additional preparations—Oracle server

1. The tablespace name and database owner name must each be unique for a particular Oracle SQL Server. However, the tablespace name and the DBO name can be identical to each other. Therefore, when selecting names for the CONTROL-M/Server mirror database, verify that the tablespace name and owner name are each unique for the particular Oracle SQL Server.

2. If you will be building a database, you must supply values for the database owner and tablespace name:

   - Specifying existing owner and tablespace will erase and recreate these database elements.
   - Specifying new, unique values for owner and tablespace name will build a new database on the server.

---

### Table 40  Additional required details—Sybase

<table>
<thead>
<tr>
<th>Details required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>UNIX system paths or raw partitions for the data and log files.</td>
<td>These paths must be unique.</td>
</tr>
<tr>
<td>Sybase device names for the data and log database devices.</td>
<td>These names must be unique for the database server. Use the Sybase <code>sp_helpdevice</code> command to view existing devices on the database server when building the database.</td>
</tr>
</tbody>
</table>
Additional preparations—MSSQL server

1  Prepare the additional details listed in Table 41.

Table 41  Additional required details—MSSQL

<table>
<thead>
<tr>
<th>Details required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A database name and a database owner (DBO) name for the mirror database.</td>
<td>The database name can be the same as the database owner name, but the database name and database owner name must each be unique for a particular MSSQL Server. Therefore, when selecting names for the CONTROL-M/Server database (using an existing MSSQL Server), verify that the database name and database owner name are unique for the MSSQL Server.</td>
</tr>
<tr>
<td>System path names for the data and log files.</td>
<td>These paths must be unique.</td>
</tr>
<tr>
<td>MSSQL device names for the data and log database devices.</td>
<td>These names must be unique for the database server.</td>
</tr>
</tbody>
</table>

2  If you will be building a database, you must supply values for the database owner, database name, devices and file or partition paths:

- Specifying existing owner name, database name, and device assignments will erase and recreate these database elements.
- Specifying new, unique values for owner name, database name, and device assignments will build a new database on the server.
- Any filenames you specify for a file-based installation must not exist on the mirror database server.

3  Every computer type uses a different character set for MSSQL. If the character set for the primary database and mirror database are not the same, the character set for the primary database must be installed on the mirror MSSQL Server.
Performing additional preparations

## Additional preparations—PostgreSQL server

1. Prepare the additional details listed in Table 42.

### Table 42  Additional required details—PostgreSQL

<table>
<thead>
<tr>
<th>Details required</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>A database name and a database owner (DBO) name for the mirror database.</td>
<td>The database name can be the same as the database owner name, but the database name and database owner name must each be unique for a particular PostgreSQL database server. Therefore, when selecting names for the CONTROL-M/Server database (using an existing PostgreSQL database server), verify that the database name and database owner name are unique for the PostgreSQL database server.</td>
</tr>
<tr>
<td>CONTROL-M/Server mirror database location</td>
<td>You must create this location prior to installing the CONTROL-M/Server mirror database. The location must be empty. Note: Only for PostgreSQL database server on UNIX.</td>
</tr>
</tbody>
</table>

2. If you will be building a database, you must supply values for the database owner, database name and database location.

   - Specifying existing owner name, database name, and database location will erase and recreate these database elements.

   - Specifying new, unique values for owner name, database name, and database location will build a new database on the server.

3. Every computer type uses a different character set for PostgreSQL. If the character set for the primary database and mirror database are not the same, the character set for the primary database must be installed on the mirror PostgreSQL Server.
Preparing the failover CONTROL-M/Server

Perform the steps in this section to install and verify the failover CONTROL-M/Server on the secondary computer.

The failover CONTROL-M/Server should be identical to the primary CONTROL-M/Server and use the same CONTROL-M/Agents and remote hosts.

For information that will help you prepare the failover database server, see the appropriate table:

- For Sybase—see Table 30 on page 235
- For Oracle—see Table 33 on page 237
- For MSSQL—see Table 36 on page 238
- For PostgreSQL—see Table 39 on page 240

The failover server can be configured to use either a dedicated or a non-dedicated database server. However, it should not use the same instance of the database server used by the primary environment.

To install the secondary failover CONTROL-M/Server

Use the standard installation procedure described in the CONTROL-M Installation Guide to install CONTROL-M/Server on the secondary, failover computer.

For instructions on configuring the secondary failover CONTROL-M/Server so that it can be seen from within CONTROL-M/EM, see “Defining CONTROL-M/EM components” on page 54.

To verify failover settings

1. Verify the following settings on the secondary failover CONTROL-M/Server:

   - The following file should be the same as the primary CONTROL-M/Server installations:
     - $HOME/ctm_server/data/TimeZone.dat
   - The configuration of the following directories should be the same as the primary CONTROL-M/Server installations:
     - $HOME/ctm_server/data/SSL
     - $HOME/ctm_server/data/Remedy
Preparing the failover CONTROL-M/Server

- **Agent-to-Server Port Number** should be the same as on the primary CONTROL-M/Server.

- **Server-to-Agent Port Number** should be the same as on the primary CONTROL-M/Server.

- The date should be the same on both computers.

- All CONTROL-M/Agents defined on the primary CONTROL-M/Server, must also be defined on the secondary CONTROL-M/Server.

- **CONTROL-M/Server Configuration Agent Port Number** should be the same as on the primary CONTROL-M/Server.

- Add the secondary server host name to the list of authorized hosts of each CONTROL-M/Agent.

- The **Database (Data Portion) Size** parameter should be assigned the same value as the current size of the primary database.

2 Verify that the secondary CONTROL-M/Server database conforms to the requirements for the mirror database.

For information that will help you ensure this, see the appropriate table:

- For Sybase—see Table 30 on page 235
- For Oracle—see Table 33 on page 237
- For MSSQL—see Table 36 on page 238
- For PostgreSQL—see Table 39 on page 240

3 Verify that the secondary CONTROL-M/Server is mapped to the same CONTROL-M/Agent remote host computers as the primary CONTROL-M/Server:

A On the primary CONTROL-M/Server computer, run the following command:

```
ctmhostmap -action list
```

A report is displayed, listing remote host computers in the primary CONTROL-M/Server.

B If you prepared the secondary database from a (non-primary) CONTROL-M/Server, enter the following commands on the host computer to shut down that Configuration Agent and CONTROL-M/Server:

```
shut_ca
shut_ctm
```
Implementing database mirroring

This section presents the following topics:

- Building and initializing a new CONTROL-M mirror database
- Changing over to the mirror database following primary database failure
- Changing back to the primary database after fixing the problem
- Disabling mirroring

Building and initializing a new CONTROL-M mirror database

Database mirroring can be initialized any time after CONTROL-M/Server has been installed.

**NOTE**

BMC recommends that the primary and mirror databases be hosted on separate servers.

The following are the general steps that you perform to initialize a mirror database.

1. If you haven’t already done so, prepare the secondary database server.

   You can prepare the secondary database server from the CD provided with the product, or from a CONTROL-M/Server that is not your primary CONTROL-M/Server. (For a third-party database, prepare it as you prepared the primary third-party database.)

C Run the following command on the secondary CONTROL-M/Server computer for each remote host on the displayed report:

```bash
ctm_agstat -AGSTAT <remoteHostName> R R
```

For each iteration, replace the `<remoteHostName>` variable with the name of a remote host from the report.
For information that will help you prepare the secondary server, see the appropriate table:

- For Sybase—see Table 27 on page 233
- For Oracle—see Table 31 on page 236
- For MSSQL—see Table 34 on page 237
- For PostgreSQL—see Table 38 on page 239

2 If you prepared the secondary database from a (non-primary) CONTROL-M/Server, enter the following commands on the host computer to shut down that Configuration Agent and CONTROL-M/Server:

```
shut_ca
shut_ctm
```

3 Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
shut_ca
shut_ctm
```

4 Build the mirror database by performing the following in the primary CONTROL-M/Server:

A Display the CONTROL-M Main Menu (ctm_menu).

For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Initialize Mirroring option.

D Either build the failover database from scratch by entering b (build), or copy an existing database to build your failover database by entering c (copy).

E At the prompts, provide the necessary information and confirmations, as follows:

- For Sybase—if you entered c (copy), see Table 28 on page 233
- For Sybase—if you entered b (build), see Table 29 on page 234
- For Oracle—see Table 32 on page 236
- For MSSQL—see Table 35 on page 238
- For PostgreSQL—see Table 38 on page 239
Changing over to the mirror database following primary database failure

If you are prompted whether to install, enter i (install) and confirm.

Perform any post-processing that the interactive utility instructs. (For example, if you are installing on Sybase and are instructed execute the ~/.cshrc command, do so.)

Check that mirroring is enabled by entering the number of the Check Mirroring Status option in the Database Mirroring Menu on the primary CONTROL-M/Server.

 Restart the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
start_ca
start_ctm
```

**NOTE**

All processing is executed on the primary and mirror database.

---

**Changing over to the mirror database following primary database failure**

In the event of failure of the primary database, change processing over to the mirroring database until you can fix the problem on the primary database.

1 Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
shut_ca
shut_ctm
```

2 Change over processing to the mirror database as follows:

A Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Use Mirror Database option.
Changing back to the primary database after fixing the problem

3 Restart the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```bash
start_ca
start_ctm
```

All processing is performed on the mirror database only. You should now fix the problem on the primary database.

Changing back to the primary database after fixing the problem

1 Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```bash
shut_ca
shut_ctm
```

2 Change processing back to the primary database as follows:

A Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Restore CONTROL-M Database from Mirror option.

3 Restart the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```bash
start_ca
start_ctm
```

The primary database is restored and all processing is performed on the primary and mirror database.

Disabling mirroring

If you decide that you do not want database mirroring to be performed, you can disable it as follows:
1 Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
shut_ca
shut_ctm
```

2 Disable processing on the mirror database as follows:

A Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Disable Mirroring option.

D Check that mirroring is disabled by entering the number of the Check Mirroring Status option in the Database Mirroring Menu on the primary CONTROL-M/Server.

3 Restart the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
start_ca
start_ctm
```

Database mirroring is disabled.

## Implementing Failover

This section presents the following topics:

- Initializing the failover system
- Changing over to the failover CONTROL-M/Server in an emergency
- Changing back to the primary CONTROL-M/Server after fixing the problem
- Disabling the failover system
Initializing the failover system

Initializing the failover system is the process of setting up and enabling the secondary server so that it will be ready to perform if a failure occurs. You do this by performing the following procedures:

1. “Preparing the failover CONTROL-M/Server” on page 245
2. “Initializing failover on the primary and secondary computers” on page 252

Initializing failover on the primary and secondary computers

1 If you have not already done so, perform “Preparing the failover CONTROL-M/Server” on page 245.

2 Shut down the failover (secondary) Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

   shut_ca
   shut_ctm

3 Ensure that mirroring is disabled on the failover (secondary) CONTROL-M/Server database as follows:

   A Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

   B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

   C In the Database Mirroring menu, enter the number for the Check Mirroring Status option, and verify that mirroring is disabled.

4 Initialize failover by entering the number of the Initialize Failover option in the Database Mirroring menu.

5 Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

   shut_ca
   shut_ctm

6 Ensure that mirroring is disabled on the primary CONTROL-M/Server database as follows:
A Display the CONTROL-M Main menu (ctm_menu).

For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number for the Check Mirroring Status option.

7 Initialize the mirroring database on the primary CONTROL-M/Server as follows:

A Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Initialize Mirroring option.

D Either build the failover database by entering b (build) (using the same exact parameters used in the database of the secondary CONTROL-M/Server), or copy an existing database to create your failover database by entering c (copy).

E At the prompts, provide the necessary information and confirmations.

For information that will help you respond to the prompts, see the appropriate table:

- For Sybase—if you entered c (copy), see Table 28 on page 233
- For Sybase—if you entered b (build), see Table 29 on page 234
- For Oracle—see Table 32 on page 236
- For MSSQL—see Table 35 on page 238
- For PostgreSQL—see Table 38 on page 239

F If you are prompted whether to install, enter i (install) and confirm.

G Perform any post-processing that the interactive utility instructs. (For example, if you are installing on Sybase and are instructed execute the ~/.cshrc command, do so.)

8 Check that mirroring is enabled by entering the number of the Check Mirroring Status option in the Database Mirroring Menu.
9 Restart the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

start_ca
start_ctm

**WARNING**
Do not start the failover (secondary) CONTROL-M/Server while the primary CONTROL-M/Server is running.

**NOTE**
When moving from primary to secondary server or from secondary to primary server, jobs that are in executing state on the default local agent are not recognized by the other server. If there are jobs without an owner, both the primary and the secondary server must have the same account name.

To avoid this situation from occurring, define a specific nodeid for a job.

**NOTE**
Parameters in the config.dat file are not copied from primary to secondary server or from secondary to primary server. For example, if SMTP communication parameters are not updated on the secondary database, all domail actions will fail.

---

**Changing over to the failover CONTROL-M/Server in an emergency**

In the event of failure of the primary CONTROL-M/Server, change processing over to the failover CONTROL-M/Server until you can fix the problem on the primary CONTROL-M/Server.

1 Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

shut_ca
shut_ctm

2 After ensuring that the primary CONTROL-M/Server is down, start failover processing by performing the following on the host computer of the failover CONTROL-M/Server:
Changing back to the primary CONTROL-M/Server after fixing the problem

A Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Start Failover option.

3 Start the failover (secondary) Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
start_ca
start_ctm
```

All processing is performed by the failover CONTROL-M/Server. You should now fix the problem on the primary CONTROL-M/Server.

Changing back to the primary CONTROL-M/Server after fixing the problem

1 Shut down the failover Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
shut_ca
shut_ctm
```

2 Stop failover processing by performing the following on the host computer of the failover CONTROL-M/Server:

A Display the CONTROL-M Main menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

B In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

C In the Database Mirroring menu, enter the number of the Stop Failover option.

3 Ensure that the primary Configuration Agent and CONTROL-M/Server are shut down by entering the following commands on their host computer:

```
shut_ca
shut_ctm
```
Disabling the failover system

4 Restore data to the primary CONTROL-M/Server database from the failover database by entering the number of the Restore CONTROL-M Database from Mirror option in the Database Mirroring menu.

5 Enter the following command on the primary CONTROL-M/Server computer for each remote host that is displayed in step A on page 246:

`ctm_agstat -AGSTAT <remoteHostName> R R`

Each time that you run this command, replace the `<remoteHostName>` variable with the name of a remote host from the list that was generated in step A on page 246.

6 Start the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
start_ca
start_ctm
```

All processing is performed by the primary CONTROL-M/Server on the primary and failover database.

Disabling the failover system

If you decide that you do not want failover implementation, you can disconnect it as follows:

1 Disable mirroring on the primary CONTROL-M/Server as follows:

A Shut down the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
shut_ca
shut_ctm
```

B Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

C In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

D In the Database Mirroring menu, enter the number of the Disable Mirroring option.

2 Disable mirroring on the failover CONTROL-M/Server as follows:
Periodically synchronizing the primary and mirror database

A Shut down the failover Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
shut_ca
shut_ctm
```

B Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

C In the CONTROL-M Main menu, enter the number for the Database Mirroring option.

D In the Database Mirroring menu, enter the number of the Disable Failover option.

3 Start the primary Configuration Agent and CONTROL-M/Server by entering the following commands on the host computer:

```
start_ca
start_ctm
```

All processing is performed by the primary CONTROL-M/Server on the primary database.

Periodically synchronizing the primary and mirror database

When database mirroring is enabled, all database updates from CONTROL-M/Server are sent simultaneously to both the primary and mirror CONTROL-M/Server database. However, if a CONTROL-M/Server administrative utility modifies the primary database, the mirror database will not automatically reflect these changes. Either the same or a similar utility must be run against the mirror database, or the mirror database must be re-initialized as described in “Building and initializing a new CONTROL-M mirror database” on page 247.

The following table lists CONTROL-M/Server utilities that affect the primary database. Also included is the action to perform to get the mirror database in sync. For more information about these utilities, see the CONTROL-M Utility Guide.
Table 43  Utilities affecting the primary database (part 1 of 2)

<table>
<thead>
<tr>
<th>ctm_menu Option</th>
<th>Database</th>
<th>Utility</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database Creation Menu</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Build Database</td>
<td>Sybase</td>
<td>build_db.sh</td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td></td>
<td>Oracle</td>
<td>make_db</td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td></td>
<td>MSSQL</td>
<td>build_db</td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td></td>
<td>PostgreSQL</td>
<td>build_db</td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td>Delete Database</td>
<td>Oracle</td>
<td></td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td></td>
<td>Sybase</td>
<td></td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td>Erase Database</td>
<td>All</td>
<td>ctm_clean_db</td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td><strong>Database Maintenance Menu</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restore Database</td>
<td>All</td>
<td>ctmdbrst</td>
<td>Initialize Mirroring</td>
</tr>
<tr>
<td>Add Backup Devices</td>
<td>Sybase</td>
<td>internal utility</td>
<td>No action necessary</td>
</tr>
<tr>
<td></td>
<td>MSSQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delete Backup Devices</td>
<td>Sybase</td>
<td>internal utility</td>
<td>No action necessary</td>
</tr>
<tr>
<td></td>
<td>MSSQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extend Database Size</td>
<td>Oracle</td>
<td>ctm_db_extend</td>
<td>Initialize mirroring</td>
</tr>
<tr>
<td></td>
<td>Sybase</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>MSSQL</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Extend Temporary Database Size</td>
<td>Sybase</td>
<td>ctm_tempdb_extend</td>
<td>Either run the utility on the backup server computer or see your Systems Administrator.</td>
</tr>
<tr>
<td><strong>Troubleshooting Menu</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Truncate Database Log</td>
<td>Sybase</td>
<td>ctm_cleanlog</td>
<td>Either run the utility on the backup server computer or see your Systems Administrator.</td>
</tr>
</tbody>
</table>
Table 43  Utilities affecting the primary database (part 2 of 2)

<table>
<thead>
<tr>
<th>ctm_menu Option</th>
<th>Database</th>
<th>Utility</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Restart New Day Procedure</td>
<td>All</td>
<td>internal utility</td>
<td>Initialize Mirroring.</td>
</tr>
<tr>
<td>Reset CONTROL-M Active Environment</td>
<td>All</td>
<td>clean_ajf</td>
<td>Initialize Mirroring.</td>
</tr>
<tr>
<td>Remote Host computers</td>
<td>All</td>
<td>ctmhostmap or CONTROL-M Configuration Manager</td>
<td>Run the following command on the secondary CONTROL-M/Server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ctm_agstat -AGSTAT &lt;remoteHostName&gt; R R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Replace the &lt;remoteHostName&gt; variable with the name of remote host that was added.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>update – modify the details of the specified remote host computer in the CONTROL-M/Server database</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Run the following command on the secondary CONTROL-M/Server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ctm_agstat -AGSTAT &lt;remoteHostName&gt; R R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Replace the &lt;remoteHostName&gt; variable with the name of remote host that was updated.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>delete – delete the details of the specified computer from the CONTROL-M/Server database</td>
</tr>
<tr>
<td>Remote Host compute</td>
<td>All</td>
<td>ctmhostmap or CONTROL-M Configuration Manager</td>
<td>Convert a CONTROL-M/Agent to a remote host</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Run the following command on the secondary CONTROL-M/Server:</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ctm_agstat -AGSTAT &lt;remoteHostName&gt; R R</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Replace the &lt;remoteHostName&gt; variable with the node that was updated.</td>
</tr>
</tbody>
</table>
Periodically synchronizing the primary and mirror database
Part 3 Maintaining and managing CONTROL-M

This part presents the following topics:

Chapter 10
Maintaining the CONTROL-M environment ............................... 263

Chapter 11
Maintaining databases and CONTROL-M data ........................... 281
Maintaining the CONTROL-M environment

This chapter presents the following topics:

- Conceptual overview .......................................................... 264
- CONTROL-M/EM server and CONTROL-M/Server component states .... 265
- CONTROL-M/Server management .......................................... 265
- Heartbeat monitor and Watchdog facility .................................. 266
- Remote host network disconnections ...................................... 267

Recommended task summary .................................................. 267

Starting and stopping CONTROL-M/EM server components and
CONTROL-M/Server ............................................................. 268
Starting and stopping CONTROL-M/Agent .................................... 269
  For UNIX ........................................................................ 269
  For Windows ...................................................................... 270
Recycling CONTROL-M/Agent .................................................... 271
Manually testing CONTROL-M/Server communication with Agents and remote
hosts .............................................................................. 272
Viewing CONTROL-M/EM component activation history .................. 272
Sending Control Shell commands .............................................. 273
Managing CONTROL-M/Servers ............................................... 274
  Setting whether a CONTROL-M/Server is managed or unmanaged from
  CONTROL-M/EM ............................................................. 274
  Disabling and enabling a CONTROL-M/Server .......................... 275
  Deleting a CONTROL-M/Server definition from CONTROL-M/EM .... 275
  Implementing Heartbeat Monitors and the Watchdog facility .......... 275
Managing CONTROL-M/Agents .................................................. 276
  Disabling a CONTROL-M/Agent ............................................ 276
  Setting debug on CONTROL-M/Agent .................................... 276
  Setting CONTROL-M/Agent system parameters ......................... 278
Figure 23 highlights the basic recommended workflow for maintaining the CONTROL-M environment. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 44 on page 268. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.

**Figure 23  Recommended workflow for maintaining the CONTROL-M environment**

- Start and stop components
  - Page 268
- Automate process start-up and shutdown (UNIX)
  - Page 269
- Manage CONTROL-M/Servers
  - Page 274
- Send Control Shell commands
  - Page 273
- Manually test communication
  - Page 272
CONTROL-M/EM server and CONTROL-M/Server component states

A component can be in any of the following states:

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up</td>
<td>The component is active (started).</td>
</tr>
<tr>
<td>Down</td>
<td>The component is not active (stopped).</td>
</tr>
<tr>
<td>Hanging</td>
<td>The component is not responding.</td>
</tr>
</tbody>
</table>

Using the CONTROL-M Configuration Manager, you can view and change component states.

**NOTE**

When a CONTROL-M/Server or its corresponding Configuration Agent is down, the subcomponents (CONTROL-M/Agent, CONTROL-M Configuration Manager, control modules, and remote hosts) are gray, indicating that their statuses are undetermined.

CONTROL-M/Server management

As part of CONTROL-M/Server management, you can do the following:

- Change the connection mode status of a CONTROL-M/Server to Managed or Unmanaged. For more information on Managed and Unmanaged CONTROL-M/Servers, see “CONTROL-M/Server definition and management” on page 51.

- Enable/Disable a CONTROL-M/Server—By default, CONTROL-M/Servers are enabled, which means that they can be monitored from within CONTROL-M/EM. You can disable a CONTROL-M/Server if it is unmanaged and inactive. This enables you to completely minimize the resources that CONTROL-M/EM allocates for the specific CONTROL-M/Server. When you disable a CONTROL-M/Server, it still appears in the CONTROL-M Configuration Manager by default, but is unavailable.

- Delete a CONTROL-M/Server—you can delete a definition of a CONTROL-M from CONTROL-M/EM. The CONTROL-M/Server will continue to exist, but it will no longer be visible within CONTROL-M/EM, and it will no longer be controlled from within the CONTROL-M Configuration Manager.
Heartbeat monitor and Watchdog facility

To check that TCP/IP communication between CONTROL-M/Server and CONTROL-M/EM is functional and responsive, CONTROL-M uses Heartbeat monitors.

CONTROL-M/EM, and each CONTROL-M/Server, contain a Heartbeat monitor.

A Heartbeat monitor can operate in either of two modes:

- **Active mode**—the Heartbeat monitor periodically initiates heartbeat checks by sending a heartbeat check message through a TCP/IP connection as follows:
  
  — A CONTROL-M/Server Heartbeat monitor sends a heartbeat check message to CONTROL-M/EM
  
  — The CONTROL-M/EM Heartbeat monitor sends a heartbeat check to a CONTROL-M/Servers.
  
  Active Heartbeat monitors can also respond to Heartbeat check messages.

- **Passive mode**—the Heartbeat does not initiate heartbeat check messages, but can respond to a heartbeat check message sent through a TCP/IP connection.

To automatically monitor essential CONTROL-M/Server processes and resources, CONTROL-M/Server contains a facility called Watchdog (WD) facility.

The Watchdog facility uses a Heartbeat monitor to check that all the primary CONTROL-M/Server processes are functioning. If any of these processes do not respond to the check, the Watchdog facility sends a message to an error handler. (The facility automatically logs messages to the CONTROL-M IOALOG and PROCLOG files.)

An error handler is an object that contains and performs instructions for handling errors about which it was notified. Generally, error handlers are scripts.

To monitor CONTROL-M/Server processes, the Watchdog facility can use the following built-in utilities (described in the CONTROL-M Utility Guide):

- **ctmdiskspace utility**—which checks the amount of free disk space on a specified device and sends an error message to the error handler if it is below a specified amount.

- **ctmdbspace utility**—which checks data and log usage in the CONTROL-M/Server database and sends an error message to the error handler if it is above a specified percentage.
To enable the Watchdog facility to run utilities and use scripts, you must enable certain user exits.

You can adjust the functioning of Heartbeat monitors and the Watchdog facility by modifying system parameters.

**Remote host network disconnections**

CONTROL-M/Agent requires an open connection to a remote host from the time of job submission until the end of the job. If a network disconnection occurs, CONTROL-M/Agent attempts to restore the connection. During the reconnection attempts, jobs running on the remote host, through the specified CONTROL-M/Agent, remain in executing status.

If the connection is restored, the status of jobs is updated to reflect their current status, either completed or still running. If the connection is not restored after the specified number of attempts, the jobs end with **NOT_OK** status.

The SYSOUT and exit code for jobs are stored in files on the remote host. The files reside in the user home directory of the job’s owner, in the directory specified by RJX_SYSOUT_DIR. For more information about RJX_SYSOUT_DIR, see “CONTROL-M/Agent parameters” on page 505.

- If network connections are restored, these files are deleted, by default, when the jobs end.
- If network connections were not restored, you can check these files to see if the jobs completed successfully or failed.

Following a remote host network disconnection, you should modify recovery configuration parameter settings. For more information, see “CONTROL-M/Agent parameters” on page 505.

**Recommended task summary**

Table 44 lists specific tasks related to each phase of the workflow (Figure 23 on page 264). Subsequent sections provide step-by-step instructions.
Starting and stopping CONTROL-M/EM server components and CONTROL-M/Server

This section provides instructions for changing the state of CONTROL-M/EM server components and CONTROL-M/Server. Only CONTROL-M/EM components and the running state of CONTROL-M/Server can be manipulated through the CONTROL-M Configuration Manager.

NOTE

The CONTROL-M Web Server cannot be started or stopped from the CONTROL-M Configuration Manager. It is a Windows service, and can only be started and stopped manually from the Windows Start menu. It is automatically restarted anytime you reboot the computer on which it resides. For details, see “Starting and stopping infrastructure processes in Windows” on page 36.

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start and stop components</td>
<td>Starting and stopping CONTROL-M/EM server components and CONTROL-M/Server</td>
<td>268</td>
</tr>
<tr>
<td></td>
<td>Starting and stopping CONTROL-M/Agent</td>
<td>269</td>
</tr>
<tr>
<td>Test CONTROL-M/Server communication with agents and remote hosts</td>
<td>Manually testing CONTROL-M/Server communication with Agents and remote hosts</td>
<td>272</td>
</tr>
<tr>
<td>View component activation history</td>
<td>Viewing CONTROL-M/EM component activation history</td>
<td>272</td>
</tr>
<tr>
<td>Send Control Shell commands</td>
<td>Sending Control Shell commands</td>
<td>273</td>
</tr>
<tr>
<td>Manage CONTROL-M/Servers</td>
<td>Setting whether a CONTROL-M/Server is managed or unmanaged from CONTROL-M/EM</td>
<td>274</td>
</tr>
<tr>
<td></td>
<td>Disabling and enabling a CONTROL-M/Server</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>Deleting a CONTROL-M/Server definition from CONTROL-M/EM</td>
<td>275</td>
</tr>
<tr>
<td></td>
<td>Implementing Heartbeat Monitors and the Watchdog facility</td>
<td>275</td>
</tr>
<tr>
<td>Manage CONTROL-M/Agents and remote hosts</td>
<td>Disabling a CONTROL-M/Agent</td>
<td>276</td>
</tr>
<tr>
<td></td>
<td>Setting debug on CONTROL-M/Agent</td>
<td>276</td>
</tr>
</tbody>
</table>
To change the state (start, stop, ignore, or recycle) of a CONTROL-M/EM server component or CONTROL-M/Server

1. In the CONTROL-M Configuration Manager, select one or more components and right-click.

   If you select multiple components, all of them must have a similar state.

2. Choose Desired State and then choose one of the following submenu options:
   - **Up**—bring the component up
   - **Down**—bring the component down
   - **Ignore**—instructs the appropriate Configuration Agent to ignore the running state of the component. This capability enables you to manipulate the running state of the component manually. For example, you might choose to ignore a component if you want to run it manually from the command line with a different debug level for a short period of time.
   - **Recycle**—stops the current instance and starts a new instance, using one action. You can choose Recycle only if the state of the selected component is Up.

3. If prompted for confirmation, confirm the action.

**NOTE**

You can also perform these operations by using the ccmcli utility. For more information, refer to the CONTROL-M Utility Guide.

---

Starting and stopping CONTROL-M/Agent

For UNIX

You can start the agent automatically (whenever the computer starts) or manually.

**To start CONTROL-M/Agent automatically**

After CONTROL-M/Agent is installed, copy the rc.agent_user startup script from ctm/scripts in the directory under which you installed CONTROL-M/Agent, and place it in the operating system’s startup script directory.
To start CONTROL-M/Agent manually

1 Log on to the agent computer as root.

2 Enter the following command from the agent directory:

   ctm/scripts/start-ag -u <agent_username> -p ALL :

To stop CONTROL-M/Agent manually

1 Log on to the agent computer as root.

2 Enter the following command from the agent directory:

   ctm/scripts/shut-ag -u <agent_username> -p ALL :

For information about recycling CONTROL-M/Agent using the CONTROL-M Configuration Manager, see “Recycling CONTROL-M/Agent” on page 271.

For Windows

To start CONTROL-M/Agent manually

1 In Microsoft Windows, select Start => Settings => Control Panel => Administrative Tools.

2 In the Administrative Tools window, click Services.

3 Select CONTROL-M/Agent and click Start.

To stop CONTROL-M/Agent manually

1 In Microsoft Windows, select Start => Settings => Control Panel => Administrative Tools.

2 In the Administrative Tools window, click Services.
3 Select CONTROL-M/Agent and click Stop.

For information about recycling CONTROL-M/Agent using the CONTROL-M Configuration Manager, see “Recycling CONTROL-M/Agent” on page 271.

Recycling CONTROL-M/Agent

Recycling stops the current instance of CONTROL-M/Agent and starts a new instance, using one action.

To recycle CONTROL-M/Agent

1 In the CONTROL-M Configuration Manager, select one or more components and right-click.

   If you select multiple components, all of them must have a similar state.

2 Choose Desired State => Recycle.

   You can choose Recycle only if the state of the selected component is Up.

3 If prompted for confirmation, confirm the action.

--- NOTE ---

Using CONTROL-M Configuration Manager, you can recycle a CONTROL-M/Agent (version 6.4.01 or later), but you cannot bring up, bring down, or ignore a CONTROL-M/Agent. The Desired State fields in the CONTROL-M Configuration Manager remain empty for CONTROL-M/Agents. For information on starting and stopping CONTROL-M/Agents, see “Starting and stopping CONTROL-M/Agent” on page 269.

---

By default, CONTROL-M/Agent is automatically started when the computer is turned on or rebooted. When CONTROL-M/Agent is in shutdown mode, the recycle is disabled.

You can manually stop and start CONTROL-M/Agent at any time. When CONTROL-M/Agent version 6.4.01 or higher is up, you can recycle it from CONTROL-M Configuration Manager.

To recycle (stop and restart) a CONTROL-M/Agent that is currently up

1 In the CONTROL-M Configuration Manager, right-click the agent.

2 Choose Recycle.
Manually testing CONTROL-M/Server communication with Agents and remote hosts

3 If prompted for confirmation, confirm the action.

NOTE
A confirmation message appears only if the CONTROL-M/Agent has jobs in Executing state. If you select Yes

- (For Unix) the jobs remain in Executing state and continue to run after the agent is restarted
- (For Windows) the jobs turn to Disappeared status and do not run after the agent is restarted

If CONTROL-M/Agent and CONTROL-M/Server have a persistent connection the message does not appear even though jobs remain in Executing state and continue to run when the CONTROL-M/Agent is restarted.

You can also perform these operations by using the ccmcli utility. For more information, refer to the CONTROL-M Utility Guide.

Manually testing CONTROL-M/Server communication with Agents and remote hosts

1 In the CONTROL-M Configuration Manager, right-click the CONTROL-M/Agent or remote host, and choose Ping.

A test is automatically performed on the communication channel between the CONTROL-M/Agent or remote host and its CONTROL-M/Server. When the check is complete, a dialog box displays the result.

Alternatively, you can test the CONTROL-M/Server communication with CONTROL-M/Agents and remote hosts using the ctmping utility. For more information, see the CONTROL-M Utility Guide.

Viewing CONTROL-M/EM component activation history

You can use the CONTROL-M Configuration Manager to examine the activation history CONTROL-M/EM components.

In the CONTROL-M Configuration Manager, select View => Agents Log.
Sending Control Shell commands

The Control Shell enables you to send commands to CONTROL-M/EM components and components of CONTROL-M for z/OS version 6.3.01 and later.

- The commands for CONTROL-M/EM components that you can run from the Control Shell are the same as those that you can run using the `-cmdstr` parameter in the CTL command line utility. For more information about this utility, see the section entitled CTL in the CONTROL-M Utility Guide.

- The commands for CONTROL-M for z/OS components are the same that you can run directly from CONTROL-M for z/OS.

To perform commands using the Control Shell

1. In the CONTROL-M Configuration Manager, right-click the required CONTROL-M/EM or CONTROL-M for z/OS component, and choose Control Shell.

2. To display the list of valid commands and requests for the selected component, click Usage. (The list is displayed in the Result box.)
Managing CONTROL-M/Servers

Managing CONTROL-M/Servers consists of the following tasks:

- Setting whether a CONTROL-M/Server is managed or unmanaged from CONTROL-M/EM
- Disabling and enabling a CONTROL-M/Server
- Deleting a CONTROL-M/Server definition from CONTROL-M/EM
- Implementing Heartbeat Monitors and the Watchdog facility

Setting whether a CONTROL-M/Server is managed or unmanaged from CONTROL-M/EM

CONTROL-M/EM can manage CONTROL-M/Server versions 6.3.01 or later. (For information about managed and unmanaged CONTROL-M/Servers, see “CONTROL-M/Server definition and management” on page 51.) If you migrated to CONTROL-M/Server 6.3.01 or later, the default setting is Unmanaged.

To set a CONTROL-M/Server version 6.3.01 or later to be managed (or unmanaged) by CONTROL-M/EM, in CONTROL-M Configuration Manager, right click the CONTROL-M/Server, and choose Set to Managed (or Set to Un-Managed).

**NOTE**  
CONTROL-M/Servers that are unmanaged have a current state of Unknown.

**WARNING**  
Do not use the Unmanaged option except for special cases where the CONTROL-M Configuration Manager is unable to connect to the CONTROL-M Configuration Agent.
Disabling and enabling a CONTROL-M/Server

You can disable a CONTROL-M/Server if the CONTROL-M/Server is unmanaged and inactive.

To disable (or enable) a CONTROL-M/Server, right click the CONTROL-M/Server and choose Enable or Disable.

**NOTE**
Depending on your CONTROL-M Configuration Manager setup, disabled CONTROL-M/Servers may still appear in the CONTROL-M Configuration Manager — with a status of Ignored.

Deleting a CONTROL-M/Server definition from CONTROL-M/EM

When you delete a CONTROL-M/Server definition from CONTROL-M/EM, the CONTROL-M/Server will continue to exist, but will no longer be visible within CONTROL-M/EM, nor controllable from the CONTROL-M Configuration Manager.

To delete a CONTROL-M/Server definition show

1. Back up and then delete all the scheduling tables from the CONTROL-M/Server.
2. In CONTROL-M Configuration Manager, right-click the CONTROL-M/Server and choose Delete.
3. Confirm the deletion.

Implementing Heartbeat Monitors and the Watchdog facility

Modifying system parameters

During installation, default values are set for Heartbeat Monitor and Watchdog facility system parameters.

BMC Software recommends that you not alter the defaults. However, if you choose to alter the defaults, the system parameters are described in Appendix B, “System parameters.”
Implementing exits

For implementing Watchdog facility exits, see “Watchdog facility exits” on page 528.

Managing CONTROL-M/Agents

Managing CONTROL-M/Agents consists of the following tasks:

- “Disabling a CONTROL-M/Agent”
- “Setting debug on CONTROL-M/Agent”
- “Setting debug on CONTROL-M/Agent”
- “Setting CONTROL-M/Agent system parameters”

Disabling a CONTROL-M/Agent

To stop CONTROL-M/Server from sending jobs to a specific CONTROL-M/Agent, you can disable the agent. This leaves the agent processes running even though CONTROL-M/Server will not send it jobs. Jobs assigned to the specific agent are held in Wait state, until the agent is re-enabled.

If the disabled agent is part of a node group, that agent will be skipped when jobs in the node group are assigned to an agent.

To disable a CONTROL-M/Agent, in the CONTROL-M Configuration Manager, right-click the required CONTROL-M/Agent, and choose Disable.

Setting debug on CONTROL-M/Agent

You can set debug levels on CONTROL-M/Agent version 6.4.01 and later using the CONTROL-M Configuration Manager.

NOTE

The CONTROL-M/Agent that is being modified must be available.
To set a debug level on CONTROL-M/Agent

1 In CONTROL-M Configuration Manager, right-click the required CONTROL-M/Agent.

2 From the pop-up menu, select CONTROL-M/Agent Debug.

The CONTROL-M/Agent Debug dialog box is displayed. You can also display this dialog box by choosing Tools => CONTROL-M/Agent Debug if there is at least one CONTROL-M/Agent version 6.4.01 and later that is using the CONTROL-M Configuration Manager.

Table 45 describes the fields in the CONTROL-M/Agent Debug dialog box.

---

### NOTE

Values are dimmed if you do not have authority to change them.

<table>
<thead>
<tr>
<th>Field name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONTROL-M/Server</strong></td>
<td>The name of the CONTROL-M/Server to which the agent is connected.</td>
</tr>
<tr>
<td></td>
<td>To change the CONTROL-M/Server, click the down-arrow and select from the list that is displayed. The agents that are displayed in the CONTROL-M/Agent field depend on which CONTROL-M/Server is chosen.</td>
</tr>
<tr>
<td><strong>CONTROL-M/Agent</strong></td>
<td>The name of the CONTROL-M/Agent that is being configured.</td>
</tr>
<tr>
<td></td>
<td>To change the CONTROL-M/Agent, click the down-arrow and select from the list that is displayed. The agents that are displayed depend on which CONTROL-M/Server is chosen in the CONTROL-M/Server field.</td>
</tr>
<tr>
<td><strong>Diagnostic level</strong></td>
<td>Select the required diagnostic level to generate diagnostic messages. The valid values are: 0–4. Level 0 generates no diagnostics. Level 4 generates maximum diagnostics.</td>
</tr>
<tr>
<td><strong>Communication trace</strong></td>
<td>Select the required communication trace level to debug communications between CONTROL-M/Agent and CONTROL-M/Server. The valid values are:</td>
</tr>
<tr>
<td></td>
<td>0 no</td>
</tr>
<tr>
<td></td>
<td>1 yes</td>
</tr>
</tbody>
</table>

3 Click **Apply** to accept all changes and for them to take immediate effect.
In the event of an error, the original diagnostics level and communication trace values are set in the corresponding combo boxes.

4 Click **OK** to accept all changes and for them to take immediate effect.

The CONTROL-M/Agent Debug dialog box is closed.

**Generating agent debug logs**

Set the diagnostic level and the communication trace and then rerun the required job to generate agent debug logs in the proclog sub-directory of CONTROL-M/Agent. For more information, see Chapter 12, “Diagnostics: conceptual information”.

**Setting CONTROL-M/Agent system parameters**

You can set or modify system parameters on CONTROL-M/Agent version 6.4.01 and later using the CONTROL-M Configuration Manager.

**NOTE**

The CONTROL-M/Agent that is being modified must be available.

**To modify system parameters on CONTROL-M/Agent**

1 In CONTROL-M Configuration Manager, right-click the required CONTROL-M/Agent.

2 From the pop-up menu, select **CONTROL-M/Agent System Parameters**.

The CONTROL-M/Agent System Parameter window is displayed. You can also display this window by choosing **Tools => System Parameters => CONTROL-M/Agent System Parameters** if there is at least one CONTROL-M/Agent version 6.4.01 and later that is using the CONTROL-M Configuration Manager.

3 In the CONTROL-M/Agent System Parameter window, double-click the required CONTROL-M/Agent.

The CONTROL-M/Agent - Update System Parameter dialog box is displayed. You can also display this dialog box by clicking the **Update/View System Parameter** icon in the CONTROL-M/Agent System Parameter window.

**Table 45** describes the fields in the CONTROL-M/Agent - Update System Parameter dialog box.
Setting CONTROL-M/Agent system parameters

Chapter 10 Maintaining the CONTROL-M environment

4 Click **Save** for the changes to take immediate effect and to close the CONTROL-M/Agent - Update System Parameter dialog box.

In the event of an error, CONTROL-M/Agent issues an appropriate message so that you can set an alternative value, if required.

5 In the CONTROL-M/Agent System Parameter window click **Close** to close this window.

**Restoring system parameters to their default values**

When reviewing agent system parameters in the CONTROL-M/Agent System Parameter window, lines that are bold indicate that the current values of these system parameters are different from the default values.
If a system parameter does not have a default value, "N/A" is displayed in the Default Value column.

To restore a system parameter to its default value, display the CONTROL-M/Agent - Update System Parameter dialog box and click Restore Default. This button is enabled only when the current value of the system parameter is different from the default value.
Maintaining databases and CONTROL-M data

This chapter presents the following topics:

- Conceptual overview ......................................................... 282
- CONTROL-M databases ...................................................... 284
- Database maintenance menus ............................................. 284
- CONTROL-M/EM database backup, archive, and restore ........ 284
- CONTROL-M/Server database backup, archive, rebuild, and restore .... 284
- Automatic and manual database cleanup ................................ 286
- Recommended task summary ............................................... 286
- Maintaining Databases ...................................................... 287
- Implementing CONTROL-M/Server database archiving, backup, and restore 291
  - Enabling archiving of a CONTROL-M/Server database (Oracle and PostgreSQL only) 291
  - Backing up a CONTROL-M/Server database ........................... 292
  - Adding a new CONTROL-M/Server backup device .................. 294
  - Restoring a CONTROL-M/Server database from a backup ........ 295
  - Rebuilding a CONTROL-M/Server database ......................... 297
- Managing the CONTROL-M/EM database .............................. 299
  - Exporting and importing CONTROL-M/EM data ..................... 299
  - Exporting and importing audit records ............................... 301
  - Exporting and importing CONTROL-M/Server security definitions .... 301
- Performing periodic CONTROL-M/EM database maintenance and cleanup .... 302
  - Checking available space in the CONTROL-M/EM database .......... 302
  - Extending the CONTROL-M/EM database .............................. 303
  - Cleaning up CONTROL-M/EM database error log files ............... 304
  - Removing old archived networks ..................................... 304
  - Removing old alerts .................................................... 305
  - Removing old job versions ............................................ 306
  - Removing exception alerts ............................................ 306
  - Deleting audit records ................................................ 307
- Performing periodic CONTROL-M/Server database maintenance and cleanup .... 308
  - Checking available space in the CONTROL-M/Server database .... 308
  - Extending the CONTROL-M/Server database .......................... 309

Chapter 11  Maintaining databases and CONTROL-M data  281
Conceptual overview

This chapter explains how to backup, restore, rebuild, and maintain your CONTROL-M databases. Figure 24 on page 283 highlights the basic recommended workflow. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 47 on page 287. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks. (For information about database utilities, refer to the CONTROL-M Utility Guide.)
Figure 24  Recommended workflow for maintaining and managing databases

1. Accessing the CONTROL-M/EM Database Maintenance menu
   - Page 288
2. Accessing the CONTROL-M/Server Database Maintenance menu
   - Page 289
3. (Oracle & PostgreSQL) Enable archiving of a Server database
   - Page 291
4. Create Server database backups
   - Page 292
5. Restore or rebuild a Server database
   - Page 286
6. Manage the Enterprise Manager database
   - Page 299
7. Perform periodic cleanup
   - Page 308
CONTROL-M databases

Each CONTROL-M/Server has its own database. Each Server database contains the job processing definitions (organized by scheduling tables) for which that Server is responsible. In addition to the Definitions file, the CONTROL-M/Server database also maintains an Active Jobs file, a Resources table and a Conditions table.

CONTROL-M/EM has its own database. This database allows you to control your entire batch production enterprise. The Definition file of the CONTROL-M/EM database contains a copy of all job processing definitions from all of your CONTROL-M/Server databases. This database also includes the Active Environment.

Database maintenance menus

Many of the database maintenance function that you perform are performed from database maintenance menus and submenus:

- For CONTROL-M/EM, you can access these from the Root menu.
- For CONTROL-M/Server, you can access these from the CONTROL-M Main Menu (ctm_menu).

CONTROL-M/EM database backup, archive, and restore

You perform backup of CONTROL-M/EM data, or archive of data such as audit data (Old Nets) by performing data export. Conversely, you restore backed up or archived CONTROL-M/EM data by performing data import. For details, see “Managing the CONTROL-M/EM database” on page 299.

CONTROL-M/Server database backup, archive, rebuild, and restore

Types of backups (*Oracle and PostgreSQL only*)

CONTROL-M/Server can perform *hot backups* or *cold backups*.
Hot backups

A hot backup continuously tracks changes to the database while CONTROL-M/Server is active. Following a crash (or other event), you can restore the database to the state it was in just before the crash.

The following considerations apply to hot backups:

- Hot backups are performed in archive mode, which is discussed in “Archive mode (Oracle and PostgreSQL only)” on page 285. Running the database in Archive mode requires extra disk space for control files.
- You must specify an existing directory when implementing hot backups.

Cold backups

A cold backup copies the contents of the database to a file when CONTROL-M/Server is shut down. The database can be restored up to the date/time of the last backup.

You can use cold backups to restore the database to the state it was in when the backup was performed. To perform a cold backup, archive mode must be disabled.

NOTE

- You can run the ctm_backup_bcp utility even when the database is in archive mode.
- Shut down CONTROL-M/Server before performing a cold backup.

Archive mode (Oracle and PostgreSQL only)

If you enable archive mode and your database logs become full, CONTROL-M/Server backs up the logs before overwriting them with new information. If the database subsequently crashes, you can use the archived logs to restore the database up until the most recent SQL transaction.

If you enable archive mode, you should plan to keep it enabled for long term use. If you enable and disabled it frequently, the archived log files will not provide useful information for database restoration.

NOTE

If archive mode is enabled, database transactions might be performed more slowly, and archive files will require more disk space.
**Database restore and rebuild**

If the data in your database becomes corrupt, you must restore the data from a backup. You can only restore data when the database structure is correct.

If the CONTROL-M/Server database structure (schema) becomes corrupt, you must rebuild the database. Following the rebuild, you must restore the data.

**NOTE**

When a cold restore is performed, the restore file must be exported from the database with the same encoding as the destination database.

If you rebuild the database with UTF8 encoding, you must manually configure the environment settings, to enable the CONTROL-M/Server components to support this encoding.

**Automatic and manual database cleanup**

Older and unneeded data is normally cleaned (deleted) from the database automatically according to system parameters that determine (for example) how long to retain records, how many records to retain, and how often to perform cleanup.

Manual database housekeeping and cleanup described in this chapter is intended for special situations where you might want to clean out more data than is cleaned out by the automatic clean up. For example, if disk space is low, you might want to remove a larger than normal portion of a particular type of data.

If you find that you are performing manual cleanups frequently, especially the same type of cleanup each time, you should consider adjusting the system parameters so that automatic cleanup more closely matches the cleanup pattern you desire.

**Recommended task summary**

Table 47 lists specific tasks related to each phase of the workflow (Figure 24 on page 283). Subsequent sections provide step-by-step instructions.
You can use the following methods to maintain the CONTROL-M/EM and CONTROL-M/Server databases.
To maintain CONTROL-M/EM databases

— use the interactive Database Maintenance menu that you access from the Root menu (described in this section).

— run the ecsutil from the command line (described in the CONTROL-M Utility Guide.)

To maintain CONTROL-M/Server databases, use the Database Maintenance menu that you access from the CONTROL-M Main Menu (described in this chapter).

To access the Database Maintenance menu for CONTROL-M/EM

1 Display the CONTROL-M/EM Root Menu (root_menu). For instructions on displaying the Root menu, see “Using the CONTROL-M/EM Root Menu” on page 46.

2 In the CONTROL-M/EM Root menu, enter the number for the Database Maintenance option.

Table 48 describes the options in the Database Maintenance Menu for CONTROL-M/EM.

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Export Database</td>
<td>Extracts the contents of the CONTROL-M/EM database to a compressed flat file or tape.</td>
</tr>
<tr>
<td>Import Database</td>
<td>Restores the CONTROL-M/EM database from a file or tape created using the Export Database option. Note: Stop all CONTROL-M/EM components before performing this operation.</td>
</tr>
<tr>
<td>Custom Export/Import</td>
<td>Displays the Export/Import Default Parameters menu that enables you to customize the parameters used for the Export Database and Import Database options. Note: Stop all CONTROL-M/EM components before performing this operation.</td>
</tr>
<tr>
<td>Extend Database Size</td>
<td>Enlarges the data portion of the CONTROL-M/EM database. Depending on the type of database server installed, this option runs the db_extend_sybase or db_extend_oracle utility. When the utility runs, you may be prompted for the following data: Password for the sa or SYSTEM user. Oracle: Name of the existing device you want to extend. Sybase: Name of a new device that you want to extend. Size in MB of the additional space to allocate. Full path for the device. Size (in MB) to which you want to extend the device.</td>
</tr>
</tbody>
</table>
Maintaining Databases

Chapter 11  Maintaining databases and CONTROL-M data  289

To access the Database Maintenance menu for CONTROL-M/Server

1 Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

Table 49 describes the options in the Database Maintenance Menu.

Table 48  Database Maintenance menu options—from the Root Menu (part 2 of 2)

<table>
<thead>
<tr>
<th>Menu option</th>
<th>Description</th>
<th>Applicable database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Erase Old Nets</td>
<td>Erases an old network.</td>
<td></td>
</tr>
<tr>
<td>Erase Audit Data</td>
<td>Erases audit records that were stored in the database.</td>
<td></td>
</tr>
<tr>
<td>Erase Exception</td>
<td>Erases exception alerts that were stored in the CONTROL-M/EM database.</td>
<td></td>
</tr>
<tr>
<td>Alerts</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify Interfaces</td>
<td>Activates the dsedit utility so that you can modify the Interfaces file.</td>
<td></td>
</tr>
<tr>
<td>File</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Modify Database</td>
<td>Modifies the CONTROL-M/EM database name. A prompt is displayed requesting</td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>the new name. This option is displayed only when Sybase Adaptive Server is</td>
<td></td>
</tr>
<tr>
<td></td>
<td>installed.</td>
<td></td>
</tr>
</tbody>
</table>

To access the Database Maintenance menu for CONTROL-M/Server

1 Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

Table 49 describes the options in the Database Maintenance Menu.

Table 49  Database Maintenance Menu options—from the Main menu (part 1 of 2)

<table>
<thead>
<tr>
<th>Menu item</th>
<th>Description</th>
<th>Applicable database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Archive mode</td>
<td>When database logs are full, they are written to a special backup destination before they are overwritten by new information.</td>
<td>Oracle and PostgreSQL</td>
</tr>
<tr>
<td>Backup Database</td>
<td>Backs up the CONTROL-M/Server database onto a backup device.</td>
<td>All</td>
</tr>
<tr>
<td>Restore Database</td>
<td>Restores the CONTROL-M/Server database from a backup device.</td>
<td>All</td>
</tr>
<tr>
<td>List All Devices</td>
<td>Display list of all devices.</td>
<td>Sybase and MSSQL</td>
</tr>
<tr>
<td>List Backup Device</td>
<td>Display a list of valid devices.</td>
<td>Sybase and MSSQL</td>
</tr>
<tr>
<td>Add Backup Device</td>
<td>Add a device to the list of devices.</td>
<td>Sybase and MSSQL</td>
</tr>
<tr>
<td>Drop Backup Device</td>
<td>Deletes a device from the list of backup devices.</td>
<td>Sybase and MSSQL</td>
</tr>
<tr>
<td>Extend Database Size</td>
<td>Extends the data segment of the database.</td>
<td>All</td>
</tr>
</tbody>
</table>
### Table 49  Database Maintenance Menu options—from the Main menu (part 2 of 2)

<table>
<thead>
<tr>
<th>Menu item</th>
<th>Description</th>
<th>Applicable database</th>
</tr>
</thead>
<tbody>
<tr>
<td>Extend Temporary Database (Tempdb) Size</td>
<td>Extends the temporary storage area of the database.</td>
<td>Sybase</td>
</tr>
<tr>
<td>Extend Database Log Size</td>
<td>Extends the log segment of the database.</td>
<td>Sybase and MSSQL</td>
</tr>
<tr>
<td>Extend TEMP Tablespace Size</td>
<td>Extends the tablespace of the database.</td>
<td>Oracle</td>
</tr>
<tr>
<td>Extend Rollback Tablespace Size</td>
<td>Extends the log segment of the database.</td>
<td>Oracle</td>
</tr>
<tr>
<td>Show Database Parameters</td>
<td>Displays the CONTROL-M/Server database parameters</td>
<td>All</td>
</tr>
<tr>
<td>Check Database</td>
<td>Displays the size of the CONTROL-M/Server database and availability of space, and verifies database integrity.</td>
<td>All</td>
</tr>
<tr>
<td>Quit</td>
<td>Quits the Database Maintenance menu and returns to the CONTROL-M Main menu.</td>
<td>All</td>
</tr>
</tbody>
</table>
Implementing CONTROL-M/Server database archiving, backup, and restore

Enabling archiving of a CONTROL-M/Server database (*Oracle and PostgreSQL only*)

Use this optional procedure if you want to archive database log files when they become full. If a database crash occurs, you can use the archived files to restore the database up until the most recent SQL transaction.

**NOTE**

Archiving, using the Archive Mode option described below, is only possible when CONTROL-M is running with a dedicated database server.

The CONTROL-M/Server automatically shuts down during this procedure.

Hot backups require that archive mode be enabled, but the backup procedure automatically sets archive mode if it was not previously set. For more information about hot backups, see “Types of backups (Oracle and PostgreSQL only)” on page 284.

To enable archiving of a CONTROL-M/Server database (*Oracle and PostgreSQL only*)

1. Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. In the CONTROL-M Main menu, enter the number for the *Database Maintenance* option.

3. In the *Database Maintenance* menu, enter the number for the *Archive Mode* option.

4. At the prompt for the destination directory, enter the name of the destination for archived log files.

5. When you are done, enter q to quit.
Backing up a CONTROL-M/Server database

BMC recommends that you back up your CONTROL-M/Server databases onto backup devices daily. This section explains how to back up a CONTROL-M/Server database onto a backup device. You can complete this procedure while the database is running.

**NOTE**
Performing this procedure has the same effect as running the ctmdbbck utility. For more information, see the CONTROL-M Utility Guide.

To back up a Sybase or MSSQL database

1. Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.
2. In the CONTROL-M Main Menu, enter the number for the **Database Maintenance** option.
3. In the **Database Maintenance** menu, enter the number for the **List Backup Devices** option, and write down the name of the device that you want to use.

**NOTE**
If the device you want is not listed, you can add it as instructed in “Adding a new CONTROL-M/Server backup device” on page 294.

4. Return to the **Database Maintenance** menu, and enter the number of the **Backup Database** option.
5. Enter the name of the backup device you wrote down in step 3.

The backup device must be either a valid device defined in the SQL database, or the full path name of a file to be created by the backup procedure.

A Sybase database has several backup devices, frequently called "tapedump1", tapedump2, and so on, if you use tapes rather than disk files.

6. Respond to the subsequent prompts that are displayed.
7. When you are done, enter q to quit.

The CONTROL-M/Server database is backed up onto a backup device.
To back up an Oracle and PostgreSQL databases

1 Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

3 In the Database Maintenance menu, enter the number for the Backup Database option.

   For Oracle: The following prompt is displayed:

   Enter a destination directory name [<ctm_home_dir>]:

   For PostgreSQL: The following prompt is displayed:

   Enter a destination file name [<ctm_home_dir>]:

4 Press Enter to accept the default directory, or enter the name of a different directory where you want the backup to be saved.

   The backup procedure assigns its own file name.

   ■ If Archive mode is not active at your site, a cold backup (described in “Types of backups (Oracle and PostgreSQL only)” on page 284) is automatically performed.
   ■ If Archive mode is active, the following prompt is displayed:

   Enter your choice for backup mode (Hot or Cold) [H/C]:

5 Select either H for hot backup or C for cold backup, and press Enter.

   The following prompt is displayed:

   Specify archiving process destination directory:

6 Enter the directory in which the archive process will store its control files.

   The backup procedure begins. Informational messages report the progress of the backup.

7 When you are done, enter q to quit.

8 If you selected a cold backup in step 5 on page 293, when the backup is complete, start CONTROL-M/Server.
Adding a new CONTROL-M/Server backup device

1 Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

3 In the Database Maintenance menu, enter the number for the Add Backup Device option.

Interactive prompts similar to the following are displayed:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter &lt;dev_logical_name&gt; :</td>
<td>cont</td>
</tr>
<tr>
<td>Enter {disk</td>
<td>tape} :</td>
</tr>
<tr>
<td>Enter &lt;file_full_path_name</td>
<td>device_name&gt; :</td>
</tr>
</tbody>
</table>

Table 50 describes the variables in this prompt.

Table 50 Logical device description

<table>
<thead>
<tr>
<th>Variable</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;dev_logical_name&gt;</td>
<td>logical name of the device</td>
</tr>
<tr>
<td>{disk</td>
<td>tape}</td>
</tr>
<tr>
<td></td>
<td>If you specify disk, you must specify the file full path name.</td>
</tr>
<tr>
<td></td>
<td>If you specify tape, you must specify the device name.</td>
</tr>
<tr>
<td>&lt;file_full_path_name</td>
<td>device_name&gt;</td>
</tr>
</tbody>
</table>

4 Enter the required parameters for the new device.

5 When you are done, enter q to quit.

Example

When prompted, specify the following values for the Add Backup Devices option in the Database Maintenance Menu:

<table>
<thead>
<tr>
<th>Prompt</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter &lt;dev_logical_name&gt; :</td>
<td>cont</td>
</tr>
<tr>
<td>Enter {disk</td>
<td>tape} :</td>
</tr>
<tr>
<td>Enter &lt;device_name&gt; :</td>
<td>cont_dev</td>
</tr>
</tbody>
</table>
The following messages are displayed:

<table>
<thead>
<tr>
<th>Creating Tape device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>'Tape' device added.</td>
</tr>
<tr>
<td>(return status = 0)</td>
</tr>
</tbody>
</table>

**NOTE**
You can drop or delete a backup device by choosing Drop Backup Device from the Database Maintenance Menu and providing the device’s logical name.

---

**Restoring a CONTROL-M/Server database from a backup**

This section provides the following procedures for restoring the Server database. Use the procedure that corresponds to your situation:

- restoring a Sybase or MSSQL database due to database failure
- restoring Sybase or MSSQL data due to data corruption
- restoring an Oracle or PostgreSQL database
- reverting back if a hot restore fails for a PostgreSQL database

**NOTE**
Performing this procedure has the same effect as running the ctmdbrst utility. For more information, see the CONTROL-M Utility Guide.

---

**To restore a Sybase or MSSQL database from a backup device**

1. Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

3. In the Database Maintenance menu, enter the number for the Restore Database option.

4. Follow the displayed prompts.

The backup device must be a valid device defined in the database, or the full path name of a backup file to be used as input for the ctmdbrst utility.
If you do not know the name of the backup device, display the list of backup devices by entering the number of the List Backup Devices option in the Database Maintenance menu, and then note the name of the device.

5 When you are done, enter q to quit.

To restore an Oracle or PostgreSQL database

**NOTE**

- This restore procedure assumes that CONTROL-M/Server and the Oracle database server are down as the result of a crash. If this is not the case, the restore procedure will fail.

- If you want to perform a restore from a Cold backup and Archive mode is active, deactivate Archive mode (using option 1 of the Database Maintenance menu) before performing the steps described below.

1 Shut down CONTROL-M/Server, and make sure there are no other users or processes connected to the SQL Server.

2 Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

3 In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

4 In the Database Maintenance menu, enter the number for the Restore Database option.

The following prompt is displayed:

Enter a destination directory name [ctm_home_dir]:

5 Press Enter to accept the default directory, or type the name of the directory in which the backup was saved.

6 When you are done, enter q to quit.

CONTROL-M performs the restore as follows:

- If Archive mode is not active, a restore is automatically performed using information from the most recent Cold backup.

- If Archive mode is active, a restore is automatically performed using information from the most recent Hot backup.
Rebuilding a CONTROL-M/Server database

---

**WARNING**

If you try to restore a dedicated Oracle database using the ctmdbrst utility without previously having backed up the database, the database will become unavailable. To access the database, enter the following procedure from the CONTROL-M/Server home directory command line:

```sql
sqlplus /nolog
connect / as sysdba
alter database mount;
alter database open;
exit
```

*(For PostgreSQL only)* - If a hot restore process failed, it is possible to revert back to the file system as it existed before the restore process began. For details, see the following instructions.

---

**NOTE**

The hot restore process uses the `$HOME/pgsql/data/pg_xlog` directory to recover the database up until the point of failure. If this directory was damaged during the failure, the database can only be recovered up until the last database log switch.

---

**To recover from a hot restore failure *(for PostgreSQL)***

1. Stop any PostgreSQL processes currently running on the computer.

2. Go to the `pgsql` parent directory. On UNIX for example, this directory is the user `$HOME` directory.

3. Check if `pgsql_old_<current_date>` exists. If so, it means that the restore process renamed the old (now corrupted) directory.

4. Rename it to `pgsql`.

5. Start the PostgreSQL server.

---

**Rebuilding a CONTROL-M/Server database**

If the CONTROL-M/Server database structure (schema) becomes corrupt, you must rebuild the database and then restore the data.

**Before you begin**

Before rebuilding the database, back up the database data. *(For instructions, see “Backing up a CONTROL-M/Server database” on page 292.)* You will use this backup to restore the data at the end of the rebuild process.
Also, verify that the following requirements are met:

- CONTROL-M/Server and CONTROL-M/Server Configuration Agent are not running.
- The SQL database is running. For more information, see “Starting and stopping CONTROL-M/EM server components and CONTROL-M/Server” on page 268.
- No CONTROL-M/Server utilities are connected to the SQL Server.

**To rebuild the database**

1. Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. In the CONTROL-M Main menu, enter the number for the **Database Creation** option.

3. In the **Database Creation** menu, enter the number for the **Build Database** option.

4. Follow the prompts online, and specify or change the parameters as required.
   
   Default values are provided for most of the parameters. Modify them as required. For more information on the parameters, see Appendix B, “System parameters.”

   **NOTE**

   When rebuilding the database, working in an existing mode, the full path names of the log and data devices must be different from the original path names.

5. In the **Main Menu**, enter the number of the **Database Maintenance** option.

6. In the **Database Maintenance**, enter the number of the **Restore Database** option to load the data into the new database.

7. Follow the displayed prompts.

   The backup device must be a valid device defined in the database, or the full path name of a backup file to be used as input for the ctmdbrst utility.

   If you do not know the name of the backup device, display the list of backup devices by entering the number of the **List Backup Devices** option in the **Database Maintenance** menu, and then note the name of the device.

8. When you are done, enter `q` to quit.
Managing the CONTROL-M/EM database

Managing the CONTROL-M/EM database can involve the following tasks:

- Exporting and importing CONTROL-M/EM data
- Exporting and importing audit records
- Exporting and importing CONTROL-M/Server security definitions

Exporting and importing CONTROL-M/EM data

You perform backup and restore CONTROL-M/EM data, archive and restore of audit data, and so on, by performing data export and import.

To export CONTROL-M/EM data

1. Display the CONTROL-M/EM Root Menu (root_menu). For instructions on displaying the Root menu, see “Using the CONTROL-M/EM Root Menu” on page 46.

2. In the CONTROL-M/EM Root Menu, enter the number for the Database Maintenance option.

3. In the Database Maintenance menu, enter the number for the Export Database option.

4. Specify the name of the file to which the database should be exported.

   The database is exported to a file that you specify. The file is called `export_file_name.Z`.

5. Enter q to exit the Database Maintenance menu and the Root menu.

To import previously exported CONTROL-M/EM data

1. Display the CONTROL-M/EM Root Menu (root_menu). For instructions on displaying the Root menu, see “Using the CONTROL-M/EM Root Menu” on page 46.

2. In the CONTROL-M/EM Root Menu, enter the number for the Database Maintenance option.

3. In the Database Maintenance menu, enter the number for the Import Database option.
You are prompted for location of the export_file_name file that was created during the procedure “Export the existing CONTROL-M/EM database” on page 154.

4 Enter the path and name for the export_file_name file. Do not include the .Z extension.

When the procedure is complete, the Database Maintenance menu is displayed.

5 Enter q to exit the Database Maintenance menu and the Root menu.

---

**WARNING**

If you quit the Root menu or its submenus while performing the database import, you must perform “Rebuilding the database schema following import interruption” on page 300.

---

**Rebuilding the database schema following import interruption**

---

**NOTE**

You should only perform this procedure if an interruption occurred to the procedure: “To import previously exported CONTROL-M/EM data” on page 299.

---

1 Enter the following command to build the database schema:

```
ecs util -U ecs_admin_username -P password -build_schema
```

2 Enter the following command to uncompress the export_file_name file you created during the procedure “Exporting and importing CONTROL-M/EM data” on page 299:

```
uncompress export_file_name.Z
```

3 Ensure that there are no files under the $HOME/tmp/ecs_export directory.

4 When the file is uncompressed, enter the following command:

```
tar xvf export_file_name
```

5 Import the database data to the new database using the following command:

```
ecs util -U ecs_admin_username -P password -import -type all -dir $HOME/tmp/ecs_export/
```
6 Verify that the import was successful by accessing the data in CONTROL-M/Desktop.

7 Remove the $HOME/tmp/ecs_export directory.

The Build Database procedure is complete.

Exporting and importing audit records

To export audit records

Invoke the util utility with -export and -type audit, using the following syntax:

```
util -U DBO_name -P DBO_password -export -type audit
```

To import audit records

--- NOTE ---

The command described in this procedure deletes old audit records. To save old audit records, invoke the util utility with -export and -type audit as described in “Exporting and importing audit records.”

```
util -U DBO_name -P DBO_password -import -replace -type audit
```

Exporting and importing CONTROL-M/Server security definitions

You can use the ctmsec batch utility to export and import CONTROL-M Security Definition tables. The file that is generated by the ctmsec command is an executable file containing API functions that will redefine all the security entries when the script is run. The generated file can be modified and imported to any CONTROL-M installation.

For more information, see the description of the ctmsec utility in the CONTROL-M Utility Guide.
Performing periodic CONTROL-M/EM database maintenance and cleanup

Periodic CONTROL-M/EM database cleanup can involve the following tasks:

- Checking available space in the CONTROL-M/EM database
- Extending the CONTROL-M/EM database
- Cleaning up CONTROL-M/EM database error log files
- Removing old archived networks
- Removing old alerts
- Removing old job versions
- Removing exception alerts
- Deleting audit records

Checking available space in the CONTROL-M/EM database

1. In the CONTROL-M Configuration Manager, choose Database => Check space.

2. If you are using an Oracle database, specify the database administrator password and the user name.

   The CONTROL-M/EM Database dialog box is displayed, showing the size and free space of the database.

   **NOTE**

   If the available space falls below 20%, either extend the database or reduce the existing data.
   - For instructions on extending the database, see page 303.
   - To reduce the data, cleanup the database error log files. For instructions, see page 304.

   **NOTE**

   Alternatively, you can check the available space in the database from the Root menu. For instructions on activating the Root menu, see page 46.
Extending the CONTROL-M/EM database

1. In the CONTROL-M Configuration Manager, choose **Database => Extend Database**.

2. Specify the database administrator password and the user name.

   The CONTROL-M/EM Extend Database dialog box is displayed.

3. Extend the database as follows, depending on the database type:

   **For Sybase and MSSQL databases:**
   - A. Specify whether to extend the Data or Log segment of the database.
   - B. Specify the new size (in MB) for the segment that you are extending.
   - C. Specify the path and assign a file name for the segment you are extending.

   **NOTE**

   Ensure that a file with that name does not yet exist.

   **For Oracle databases:**
   - A. Specify the name of the table space that you are extending.
   - B. Specify the new size (in MB) for the segment that you are extending.
   - C. Click **Extend Existing File**.
   - D. Specify the path and file name for the segment you are extending.

4. Click **OK** to implement the new or extended database segment.

   **NOTE**

   Alternatively, you can extend the database from the Root menu. For instructions on activating the Root menu, see page 46.
Cleaning up CONTROL-M/EM database error log files

The database server writes a message to an error log file when the server is started or shut down, and when a database error occurs. This file is not automatically truncated. If not manually truncated, the file will utilize a large amount of disk space. The file created is called an error log for Sybase and MSSQL, and an alert log for Oracle. [UNIX only]

Whether responsibility of maintaining the error log file goes to the CONTROL-M administrator or the database administrator depends on whether your site is using the dedicated database server provided with the installation, or an existing database server.

- When your site uses a dedicated database server provided during installation, it is the responsibility of the CONTROL-M administrator to truncate this file on a regular basis. The location of this file depends on the database type.

<table>
<thead>
<tr>
<th>Table 51 Location of the dedicated database message log</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Database</strong></td>
</tr>
<tr>
<td>Sybase</td>
</tr>
<tr>
<td>Oracle</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

- If you use an existing database server, it is the responsibility of the database administrator to truncate this file on a regular basis.

Removing old archived networks

An archived Net (network) is a recording of job changes (data, conditions, and resources) that occur in the Active Jobs file on any given day. For more information, see the chapter on viewing and playing archived data in the CONTROL-M User Guide.

You can delete old archived Nets as follows:
Removing old alerts

The number of handled alerts kept in the Gateway is set according to the **NrHandledAlarms** system parameter. Handled alerts in excess of this number are automatically deleted.

The number of days alerts are kept in the database is set according to the **MaxDaysAlertRetained** system parameter. Alerts older than the specified days are automatically deleted, regardless of their status.

Should you want to delete additional alerts manually (for example, if disk space is low), you can perform the following steps. (Alternatively, you can delete the using the ccmcli utility. For details, see the **CONTROL-M Utility Guide**.)

1. In the CONTROL-M Configuration Manager, right-click the Global Alerts server and choose **Remove Old Alerts**.

2. In the **Date** field, choose the desired date and click **OK**, to delete all alerts posted on or before the specified date from the **CONTROL-M/EM** database.
Removing old job versions

You can using the ccmcli utility to manually remove old job versions.

Enter the following line command:

```
ccmcli -u <user> -p <password> -cmd erase_jobs_history -keep_days nn -s <configServer>
```

where `nn` is the number of days to keep job history. Job version that have been kept for more days will be deleted.

Output of the utility will list the number of old versions before the cleanup and number of old versions remaining after the cleanup.

Removing exception alerts

Exception alerts differ from regular alerts in that:

- Regular alerts relate to job processing problems and are intended for the end user.
- Exception alerts identify problems with component infrastructure, and are intended for the administrator for diagnostics purposes.

**NOTE**

To enable the deletions to take effect, refresh the Global Alerts Server server from the Control Shell, as follows:

1. In the CONTROL-M Configuration Manager, right-click the Global Alerts Server, and choose **Control Shell**.
2. Enter the **REFRESH** command into the **Specify...** field.
3. Click **Apply**.
You can clean up old exception alerts as follows:

**UNIX**

1. Display the CONTROL-M/EM Root Menu (root_menu). For instructions on displaying the Root menu, see “Using the CONTROL-M/EM Root Menu” on page 46.

2. In the CONTROL-M/EM Root Menu, enter the number for the Database Maintenance option.

3. In the Database Maintenance menu, enter the number for the Erase Exception Alerts option.

4. Enter q to exit the Database Maintenance menu and the Root menu.

**Windows**

1. Run the following script: `purge_xalerts.bat`

2. Enter the numbers of days to retain the exception alerts.

3. Confirm whether the exception alerts should be removed after the number of days entered.

4. Enter your username and password to set the number of days.

**Deleting audit records**

You can delete audit records the Audit_activities table of the database using either of the following methods:

- interactively from the root_menu (Unix only)
- using a script (Unix or Windows)

**To delete audit records interactively from the root_menu (Unix only)**

1. Display the CONTROL-M/EM Root Menu (root_menu). For instructions on displaying the Root menu, see “Using the CONTROL-M/EM Root Menu” on page 46.

2. In the CONTROL-M/EM Root Menu, enter the number for the Database Maintenance option.
Performing periodic CONTROL-M/Server database maintenance and cleanup

In the Database Maintenance menu, enter the number for the **Erase Audit Data** option.

Enter `q` to exit the Database Maintenance menu and the Root menu.

**To delete audit records using a script (Unix or Windows)**

1. Log on to the CONTROL-M/EM host computer as a CONTROL-M/EM administrator.

2. Enter the following command. If you do not specify `-U` and `-P`, you will be prompted to enter the DBO user name and password.

   ```
   erase_audit_data [-date yyyymmdd] [-U EM_DBO_name] [-P EM_DBO_password]
   ```

   Records written before the specified date are deleted.

### Performing periodic CONTROL-M/Server database maintenance and cleanup

Periodic CONTROL-M/EM database cleanup can involve the following tasks:

- Checking available space in the CONTROL-M/Server database
- Extending the CONTROL-M/Server database
- Cleaning up old prerequisite conditions
- Cleaning up CONTROL-M/Server database error log files
- Cleaning up the CONTROL-M/Server proclog directory
- Increasing the size of the CONTROL-M/Server master database log

### Checking available space in the CONTROL-M/Server database

1. Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2. In the CONTROL-M Main menu, enter the number for the **Database Creation** option.

3. In the **Database Creation** menu, enter the number for the **Check Database** option.

4. When you are done, enter `q` to quit.
To ensure that the CONTROL-M/Server database is automatically and regularly checked for available space

1 Define a Command-type job that will run at the desired frequency.

2 Ensure that the job issues the `ctmdbused` command.

Possible messages generated by this utility relating to the amount of available space in the CONTROL-M/Server database are:

- When the database is 90% or more full:
  ATTENTION : Not enough DB free space
- When the database is 50% or more full:
  WARNING : DB is more than half full
- When the database is 90% or more full:
  ATTENTION : Log segment is almost full

3 Define On Statement/Code statements in this or another job to detect these messages, and Do Shout messages to be issued if the above warnings are issued. For example

   on "*ATTENTION*" DoShout <destination> urgency <R|U|V> <message>

Extending the CONTROL-M/Server database

Using the Database Maintenance menu options, you can extend the size of the following segments of the CONTROL-M/Server database: data, temp and log. The menu options are available regardless of whether CONTROL-M/Server is active or shut down. However, some methods are available only for certain types of databases (for example, Oracle or Sybase).

1 Display the CONTROL-M Main Menu (`ctm_menu`). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number for the Database Maintenance option.

3 To extend the data segment

   A In the Database Maintenance menu, enter the number for the Extend Database Size option.

   B At the prompt, specify a size value or press <Enter> to accept the default.

   C Specify a full path name or press <Enter> to accept the default.
Cleaning up old prerequisite conditions

4 To extend the temporary area (not required for MSSQL)

A Perform one of the following:

■ For Oracle: In the Database Maintenance menu, enter the number for the Extend TEMP Tablespace Size option.

■ For Sybase: In the Database Maintenance menu, enter the number for the Extend Temporary Database Size option.

B At the prompt, specify a size value that is approximately 10% of the data segment size, or press <Enter> to accept the default.

C Specify a full path name or press <Enter> to accept the default.

5 To extend the log segment

A Perform one of the following:

■ For Oracle: In the Database Maintenance menu, enter the number for the Extend Rollback Tablespace Size option.

■ For Sybase or MSSQL: In the Database Maintenance menu, enter the number for the Extend Database Log Size option.

B At the prompt, specify a size value that is approximately 1/3 of the data segment size, or press <Enter> to accept the default.

C Specify a full path name or press <Enter> to accept the default.

If, after you have issued the extension request, you get a warning about an unsafe virtual device, or non-guaranteed recovery, disregard it.

6 When you are done, enter q to quit.

Cleaning up old prerequisite conditions

Retaining a large number of prerequisite conditions in the database beyond the amount of time that they should be retained can slow down performance during download of the Active environment from the CONTROL-M/Server. Cleanup of prerequisite conditions is normally done as part of New Day processing (for more information, see “Automatic prerequisite condition cleanup” on page 86).

If regular cleanup of prerequisite conditions is insufficient, you can manually clean them by running the ctmcontb utility on the relevant CONTROL-M/Servers. (To clean up conditions from for CONTROL-M for z/OS, run the IOAC_RES utility.) You can also delete conditions from the CONTROL-M/EM GUI.
Cleaning up CONTROL-M/Server database error log files

The database server writes a message to an error log file when the server is started or shut down, and when a database error occurs. This file is not automatically truncated. If not manually truncated, the file will utilize a large amount of disk space. The file created is called an error log for Sybase and MSSQL, and an alert log for Oracle. [UNIX only]

Whether responsibility of maintaining the error log file goes to the CONTROL-M administrator or the database administrator depends on whether your site is using the dedicated database server provided with the installation, or an existing database server.

■ When your site uses a dedicated database server provided during installation, it is the responsibility of the CONTROL-M administrator to truncate this file on a regular basis. The location of this file depends on the database type.

WARNING

■ Using the ctmcontb utility to clean up a large number of prerequisite conditions from the originating CONTROL-M/Server (and therefore all CONTROL-M/Servers to which they were added) can degrade performance.

■ If you run ctmcontb on the CONTROL-M/Server where the prerequisite condition originated, the prerequisite condition is deleted not only on that server but on all CONTROL-M/Servers where the prerequisite condition was sent.

■ To prevent undesired mass deletion of prerequisite conditions during this type of cleanup which might cause excessive traffic, ensure that you defined appropriate values for the following distribution system parameters for the prerequisite conditions:

— LimitGCDistribActivate
— LimitGCDistribMaxDays
— LimitGCDistribExcludeDates

BMC Software recommends that the LimitGCDistribMaxDays value (number of days) be set to less than the number of days that conditions are retained according to site housekeeping policy.

For more information, see the CONTROL-M Utility Guide.
Cleaning up the CONTROL-M/Server proclog directory

CONTROL-M/Server writes process log trace files to the proclog directory.

Each time CONTROL-M/Server is started,

- the new logs are saved to one of the following locations:
  - On UNIX: $CONTROLM_SERVER/proclog
  - On Windows: <ctm_installation>\proclog

- the proclog file from the previous session is saved to one of the following locations:
  - On UNIX: $CONTROLM_SERVER/proclog.sav
  - On Windows: <ctm_installation>\proclog.sav

The higher the trace level, the larger the log files. If CONTROL-M/Server entities operate for a long time using a trace level greater than zero, these log files utilize a large amount of disk space.

Log retention is determined by the following parameters in Table 53.

---

### Table 52 Location of the dedicated database message log

<table>
<thead>
<tr>
<th>Database</th>
<th>Dedicated database message log location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sybase</td>
<td>$SYBASE/ASE-12_5/data/errorlog</td>
</tr>
</tbody>
</table>
| Oracle   | Alerts are saved in files with the extension .log  
          | $ORACLE_BASE/admin/$ORACLE_SID/bdump/alert$ORACLE_SID.log  
          | Trace log files are saved in files with the extension .trc  
          | $ORACLE_BASE/admin/$ORACLE_SID/bdump/$ORACRR_SID_*_.trc |

- If you use an existing database server, it is the responsibility of the database administrator to truncate this file on a regular basis.
Cleaning up the CONTROL-M/Server proclog directory

Chapter 11 Maintaining databases and CONTROL-M data

The CONTROL-M/Server administrator should delete these log files when they are no longer needed.

To cleanup the proclog directory

1 Display the CONTROL-M Main Menu (ctm_menu). For instructions on displaying the Main menu, see “Using the CONTROL-M/Server Main Menu” on page 47.

2 In the CONTROL-M Main menu, enter the number for the Troubleshooting option.

3 In the Troubleshooting menu, enter the number of the Erase Proclog Files option.

This option erases the contents of the current process log file either for all active CONTROL-M/Server processes or for any specific active process.

4 Specify the 2-character code for a specific process, or ALL for all current process log files. For more information, see “Troubleshooting menu analyzing options” on page 367.

Table 53 proclog utility parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS_DIAG_LIMIT_LOG_VERSIONS</td>
<td>Number of generations of diagnostic log information to keep for a process or a thread.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ -1 (no limit to the number of files)</td>
</tr>
<tr>
<td></td>
<td>■ 1–2^31</td>
</tr>
<tr>
<td>Default: -1</td>
<td>(In the shipped config.dat, the default value is overridden by 10.)</td>
</tr>
<tr>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
<tr>
<td>OS_DIAG_LIMIT_LOG_FILE_SIZE</td>
<td>Maximum size (MB) of diagnostic log files for a process or a thread.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ -1 (no filesize limit)</td>
</tr>
<tr>
<td></td>
<td>■ 1–2^31</td>
</tr>
<tr>
<td>Default: -1</td>
<td>(In the shipped config.dat, the default value is overridden by 10.)</td>
</tr>
<tr>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
</tbody>
</table>
Increasing the size of the CONTROL-M/Server master database log

**NOTE**
This problem might in rare instances occur in CONTROL-M/Server versions prior to 6.3.01, on Sybase only.

The master database log might become full if the `trunc log on chkpt` option is not enabled. If this problem occurs, the Sybase error_log displays the following message:

```
Cannot allocate space for object 'syslogs' in database 'master'
because the 'logsegment' segment is full or has no free extents.
```

You can resolve this problem using any of the following methods, as appropriate.

**To fix this particular occurrence (a short-term solution)**

1. Log on to Sybase using the `sa` user.
2. Enter the command, which dumps unnecessary information from the log:
   
   ```
   dump tran master with no_log
   ```

**To add more space to the log (a longer-term solution if the master log often gets full)**

1. Log on to Sybase using the `sa` user.
2. Enter the command:
   
   ```
   alter database master log on 
   master=<increase>
   ```

   The `<increase>` variable is the number of 2K blocks to be added to the master database.

**To enable automatic log truncation (an ongoing solution that prevents the problem but results in automatic loss of log data)**

1. Log on to Sybase using the `sa` user.
2. Enter the following commands to set the `trunc log on chkpt` option for the master database, which will truncate the log as needed, so that it will never become full.
spConfigure "allow updates", 1
update master..sysdatabases set status = 8 where dbid = 1
spConfigure "allow updates", 0
checkpoint
Increasing the size of the CONTROL-M/Server master database log
Diagnostics and troubleshooting

This part presents the following topics:

Chapter 12
Diagnostics: conceptual information ........................................ 319

Chapter 13
Activating diagnostics .............................................................. 329

Chapter 14
Collecting diagnostic data ....................................................... 343

Chapter 15
Processes of elimination and analysis ......................................... 345
Diagnostics: conceptual information

This section comprises diagnostics and troubleshooting in CONTROL-M. Various fundamental diagnostic tasks are discussed in context, with examples of some of the expected circumstances surrounding the issues. In many cases, troubleshooting information relates to very specific issues that are particular to you and your site requirements. For this reason, you can always search the CONTROL-M Knowledge Base, accessible through the BMC website, under the heading “Support”.

Diagnostics requires a very systematic and methodological approach. In order to determine the cause of a problem, and thereby fix it, you must first eliminate all possible causes for any symptom that shows up in your CONTROL-M environment.

Various situations require various diagnostic activities. One of these is that the information gathered by default by a product is sufficient for analysis (First Failure Data Capture). A second is that each time an action is performed, it fails. This requires that you gather diagnostic information about the circumstances that occurred in your system before, during and after the symptom displayed. To do this, you must set certain diagnostic parameters and configurations to run, and then recreate the situation where the symptom occurred. A third situation is where a problem recurs but on a sporadic basis, with no clear pattern or the possibility to recreate it. This requires that a diagnostic be activated (one which will not over-burden the system) and left to run in the background for a few days.

This chapter comprises the following sections:

- “Basic diagnostic mechanisms” on page 320
- “Basic diagnostic capability in CONTROL-M” on page 322
- “Common symptoms, causes and best practices” on page 322
Basic diagnostic mechanisms

For each CONTROL-M/EM component, there is a specific custom diagnostic level. The target of diagnostics is to provide out-of-the-box diagnostic functionality which allows First Failure Data capture (FFDC) (in the majority of cases) and does not impair the performance of the product.

There are several basic diagnostic mechanisms used when running diagnostic actions.

- “Source Level Debugging,” see below
- “Communication Traces” on page 321
- “Exception Alerts” on page 321

Source Level Debugging

Source level debugging are messages that are provided at a source code function level. These messages are intended for deeper and more extensive analysis, usually by high-level specialists of CONTROL-M and BMC Software.

An example of source level debugging is the “Diag” mechanism, which is used by the majority of the CONTROL-M/EM component servers (GUI Server, Global Alerts Server and so on).

Another dimension of source level debugging is the ability to choose to where the information gathered is written. Basic source level debugging (persistent) is written to a log file. Extended source level debugging (dynamic) means that you write a diagnostic message into the memory of the process, using the advanced level memory buffer. This gives you FFDC, and can provide invaluable insight into the reasoning behind service, component or functional failure.

There are both advantages and disadvantages to each method, and you should make your choice according to the specific issue and based on the nature of your environment and your requirements.

Information captured in a log file covers the events that occurred over a longer period of time, and can therefore provide more chronological details. Using the memory buffer gives you a more detailed level of information, regarding when the problem occurred, how it occurred, where it occurred and so on. However, the memory buffer option is more limited in space, and information is cyclically overwritten, as often as the configuration dictates.
Communication Traces

Communication Traces can be either log or trace files, which provide a comprehensively detailed exchange of data between two or more servers. Said data is structured in a specific manner, in order to give as much information as possible about the occurrences between the servers. Examples of communication trace activities include the Global Conditions Server log, or the.

Exception Alerts

This feature alerts you to system failures and enables you to handle these exception alerts as necessary. Exception alerts (X-Alerts) are provided for the following types of failures:

- database
- communications network
- application errors and failures in CONTROL-M/EM background processes, such as CONTROL-M/EM Server processes, that could impair production. An example of such a background process error might be the failure of the Global Condition Server to deliver a global condition to one or more of its target data centers.

Using system parameters, you can configure the exception handling mechanism by determining

- the amount of time exceptions are kept in the database table
- whether to send exceptions to a script file or as an SNMP trap
Basic diagnostic capability in CONTROL-M

A certain level of diagnostics are automatically set as part of the default CONTROL-M configuration. These are largely those that concern user operations which fail and display indications of said failure; usually generating an error message, indicating the source of the symptom.

For more information about the types of issues that can be diagnosed prior to contacting BMC Customer Support, please see Chapter 15, “Processes of elimination and analysis.”

Documented in that chapter are several examples of common issues that can occur, and procedures that follow a straightforward, methodological approach to ascertaining the root cause behind them. In this way, a seemingly random or unconnected symptom that displays as an error within your CONTROL-M environment can be either easily dealt with, or the information gathered and packaged to facilitate a clear channel of communication between you and BMC Customer Support.

Common symptoms, causes and best practices

Issues sometimes arise that require a deeper level of diagnostic activity, and a closer, and more in-depth analysis. This kind of situation typically requires that you work in conjunction with BMC Customer Support to resolve the issue successfully.

Following is a table designed to help you identify some of the more common issues of this nature. These examples range across the broader sphere of the various components and sub-components which constitute your CONTROL-M environment.

While the issues described in this table are considered “common”, they are all also complex and severe enough to require that you work in conjunction with BMC Customer Support to achieve a successful resolution.

---

**NOTE**

Issues can often be caused or be connected to more than one CONTROL-M component.
<table>
<thead>
<tr>
<th>Scenario</th>
<th>Diagnostic to activate</th>
<th>Collecting diagnostic data</th>
<th>For more information...</th>
</tr>
</thead>
</table>
| The Active Table download from CONTROL-M/Server to CONTROL-M/EM did not complete successfully, and the Gateway status toggles between **Downloading** and **Disconnect**. | Stop the Gateway, and specify the following communication trace setting in the Additional Parameters field:  
  ■ -dbg 3 -T 5  
Turn on the CD and CO processes diagnostic functionalities, and re-perform the download. This generates the CD and CO debug logs in the proclog sub-directory of CONTROL-M/Server.  
Recreate the situation.                                                                 | After the failure is reproduced, run the Health Check utility to collect the Gateway diagnostic files, using the following command line arguments:  
  ■ -F EM  
After the failure is reproduced, run the Health Check utility to collect the Gateway server diagnostic files. Use the following command line arguments:  
  ■ -F EM -F ENV | For information about activating diagnostics, see “Activating CONTROL-M/EM diagnostics” on page 329.  
For information about collection of data using the Health Check utility, see “CONTROL-M data for BMC support (Health Check utility)” on page 343. |
| Definition problems, performance problems and user actions related problems. For example, clicking the **Hold** command and the job fails to hold. | Issue the following commands to the Gateway using the CONTROL-M Configuration Manager Control Shell:  
  ■ TRACE_CTM on  
  ■ TRACE_CLIENT on  
  ■ dbg lvl co 4  
After the failure is reproduced, run the Health Check utility to collect the Gateway server diagnostic files. Use the following command line arguments:  
  ■ -F EM -F ENV | For information about activating diagnostics, see “Activating CONTROL-M/EM diagnostics” on page 329.  
For information about collection of data using the Health Check utility, see “CONTROL-M data for BMC support (Health Check utility)” on page 343. |
### Table 54  Examples of diagnostic scenarios and solutions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Diagnostic to activate</th>
<th>Collecting diagnostic data</th>
<th>For more information...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuration Management Server cannot establish connection with</td>
<td>Perform the basic</td>
<td>After the failure is reproduced, run the Health Check utility to collect the</td>
<td>For information about the processes of elimination, see Chapter 15, “Processes of</td>
</tr>
<tr>
<td>CONTROL-M/Server.</td>
<td>processes of elimination. If these produce no result, do the following:</td>
<td>Configuration Management Server diagnostic files using the following command line</td>
<td>elimination and analysis.”</td>
</tr>
<tr>
<td></td>
<td>1. Access the</td>
<td>arguments:</td>
<td>For information about activating diagnostics, see “Activating source level debugging</td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/EM System</td>
<td>■ -dbg 3</td>
<td>diagnostics” on page 330</td>
</tr>
<tr>
<td></td>
<td>Parameters windows from the CONTROL-M Configuration Manager, and update the CMSGateAdditionalParams</td>
<td>■ -F EM</td>
<td>For information about collection of data using the Health Check utility, see</td>
</tr>
<tr>
<td></td>
<td>system parameter with the following extra value:</td>
<td>■ -F EM</td>
<td>“CONTROL-M data for BMC support (Health Check utility)” on page 343.</td>
</tr>
<tr>
<td></td>
<td>-dbg 3. (Note that there is a space before this value.)</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2. In CONTROL-M/EM,</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>recycle the</td>
<td>■ DIAGL CORBA_incoming 5 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration</td>
<td>After the failure is reproduced, run the Health Check utility to collect the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Management Server (see</td>
<td>Configuration Management Server diagnostic files using the following command line</td>
<td></td>
</tr>
<tr>
<td></td>
<td>“Starting and stopping</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/EM server</td>
<td>■ DIAGL CORBA_incoming 6 6</td>
<td></td>
</tr>
<tr>
<td></td>
<td>components and</td>
<td>■ XMLDUMP on</td>
<td></td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/Server” on</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>page 268).</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>3. Issue the following</td>
<td>■ DIAGL CORBA_incoming 5 5</td>
<td></td>
</tr>
<tr>
<td></td>
<td>command using the ctl</td>
<td>After the failure is reproduced, run the Health Check utility to collect the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>utility:</td>
<td>Configuration Management Server diagnostic files using the following command line</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ DIAGL CORBA_incoming</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 6</td>
<td>■ XMLDUMP on</td>
<td></td>
</tr>
<tr>
<td>Requests-related problems in the Configuration Management Server</td>
<td>Issue the following</td>
<td>After the failure is reproduced, run the Health Check utility to collect the</td>
<td>For information about activating diagnostics, see “Activating source level debugging</td>
</tr>
<tr>
<td></td>
<td>commands using the ctl</td>
<td>Configuration Management Server diagnostic files using the following command line</td>
<td>diagnostics” on page 330</td>
</tr>
<tr>
<td></td>
<td>utility:</td>
<td>■ DIAGL CORBA_incoming 6 6</td>
<td>For information about collection of data using the Health Check utility, see</td>
</tr>
<tr>
<td></td>
<td>■ DIAGL CORBA_incoming</td>
<td>■ XMLDUMP on</td>
<td>“CONTROL-M data for BMC support (Health Check utility)” on page 343.</td>
</tr>
<tr>
<td></td>
<td>6 6</td>
<td>■ -F EM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>XMLDUMP on</td>
<td>■ -F EM</td>
<td></td>
</tr>
</tbody>
</table>
### Table 54  Examples of diagnostic scenarios and solutions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Diagnostic to activate</th>
<th>Collecting diagnostic data</th>
<th>For more information...</th>
</tr>
</thead>
</table>
| The user fails to perform a definition action, for example, to write a scheduling table from CONTROL-M/EM. (The action is reproducible.) | Issue the following commands to the GUI server via the CONTROL-M Configuration Manager Control Shell:  
  ■ DIAGL  
  ■ CORBA_INCOMING 5  
  ■ DIAGL ecsdefdb 5  
**Note:** To restore diagnostic levels to the normal or default level: Issue the following commands to the GUI server via the CCM control shell:  
  ■ DIAGL  
  ■ CORBA_INCOMING 3 5  
  ■ DIAGL ecsdefdb 2 4 | After the failure is reproduced, run the Health Check utility to collect the GUI Server diagnostic files using the following command line arguments:  
  ■ -F EM  
It is also worth noting the following:  
  ■ which user failed to perform the action  
  ■ when the failure occurred  
  ■ which entities were involved (for example, the scheduling table name) | For information about activating diagnostics, see “Activating source level debugging diagnostics” on page 330  
For information about collection of data using the Health Check utility, see “CONTROL-M data for BMC support (Health Check utility)” on page 343. |
| The CONTROL-M/EM clients (CONTROL-M/Desktop, CONTROL-M/EM GUI) “hang”, but the GUI server seems to be up and running. | **Note:** There is no specific diagnostic to be activated in this situation, and all the following information concerns the collection of data from built-in diagnostics.  
Issue the following commands to the GUI server via the CONTROL-M Configuration Manager Control Shell:  
  ■ PGUI (output should be collected)  
  ■ PVIEW (output should be collected)  
  ■ PSTACK  
  ■ BUFFPRN <file path on GUI server machine>  
**Note:** No action required to return diagnostic levels to normal or default level. | For Solaris HP/Itanium & Linux, collect the output of the following command:  
  ■ pstack <GUI server process id>  
**For AIX**, collect the output of the following commands:  
  ■ procstack <GUI server process id>  
  ■ proffiles <GUI server process id>  
Run the health check utility to collect the GUI server diagnostics files.  
Collect the file that you specified in the BUFFPRN command in the previous phase. | For information about activating diagnostics, see “Activating source level debugging diagnostics” on page 330  
For information about collection of data using the Health Check utility, see “CONTROL-M data for BMC support (Health Check utility)” on page 343. |
### Table 54  Examples of diagnostic scenarios and solutions

<table>
<thead>
<tr>
<th>Scenario</th>
<th>Diagnostic to activate</th>
<th>Collecting diagnostic data</th>
<th>For more information...</th>
</tr>
</thead>
</table>
| The scheduling criteria of a certain job has been matched but the job was not submitted. | Turn on the SL process diagnostic functionality. This generates the SL debug log in the proclog sub-directory of CONTROL-M/Server | After the failure is reproduced, run the Health Check utility to collect the Configuration Management Server diagnostic files. It is also worth noting the following:  
  ■ which user failed to perform the action  
  ■ when the failure occurred  
  ■ which entities were involved (for example, the scheduling table name) | For information about activating diagnostics, see “Activating CONTROL-M/EM diagnostics” on page 329. “CONTROL-M data for BMC support (Health Check utility)” on page 343. |
| The New day process started on time, but took much longer to finish than planned. | At the point when the next New Day is scheduled to begin, turn on the CD process diagnostic functionality. This generates the CD debug log in the proclog sub-directory of CONTROL-M/Server. | After the failure is reproduced, run the Health Check utility to collect the Configuration Management Server diagnostic files. It is also worth noting the following:  
  ■ which user failed to perform the action  
  ■ when the failure occurred  
  ■ which entities were involved (for example, the scheduling table name) | For information about activating diagnostics, see “Activating CONTROL-M/EM diagnostics” on page 329. For information about collection of data using the Health Check utility, see x-ref |
| A job hangs in executing status, despite the job process having completed. | Use the Agent Debug functionality in the CONTROL-M Configuration Manager, set the Agent diagnostic level to 4 and trace level to 1. Then, re-run the failing job. This generates the Agent debug logs in the proclog sub-directory of the CONTROL-M/Agent. | After the failure is reproduced, run the Health Check utility to collect the Agent diagnostic files. It is also worth noting which job failed:  
  ■ Order ID  
  ■ Run ID | For information about collection of data using the Health Check utility, see x-ref |
Checking the connection between CONTROL-M/EM and CONTROL-M/Server

In the System Parameter dialog in the CONTROL-M Configuration Manager, double-click CmsGateAdditionalParams, and add the following in the Value field after take_over:

- -dbg 3 -1dbg 1

You must now recycle the Configuration Server.

For more information about this, see “Starting and stopping CONTROL-M/EM server components and CONTROL-M/Server” on page 268

---

**NOTE**

For information regarding BMC Batch Impact Manager, or BMC Forecast, please refer to the BMC CONTROL-M BSM Administrator Guide.
Activating diagnostics

This chapter describes the diagnostic procedures that exist within the framework and architecture of CONTROL-M. These have been divided into sections according to CONTROL-M or CONTROL-M/EM component. However some of the issues that arise, and the subsequent diagnostic activity spans more than one component.

For the majority of the procedure and diagnostic capability described in this chapter, BMC Software recommends that you consult BMC Customer Support prior to activating any of the procedures.

For details of pre-diagnostic activities and procedures that check the cause of a problem using a process of elimination, prior to running actual diagnostic utilities, see Chapter 15, “Processes of elimination and analysis.”

The diagnostic procedures in this chapter have been categorized under the main components of CONTROL-M:

- “Activating CONTROL-M/EM diagnostics” on page 329
- “Activating diagnostics for CONTROL-M/Server” on page 339
- “Activating diagnostics for CONTROL-M/Agent” on page 340

Activating CONTROL-M/EM diagnostics

Two forms of diagnostic functionality can be activated: source level debugging and communication traces. The following sections deal with how to set levels and activate diagnostics according to the method of diagnostic functionality, which in turn is usually specific to the component for which diagnostics are required:

- “Activating source level debugging diagnostics” on page 330
- “Activating Communication Trace Diagnostics” on page 337
Activating source level debugging diagnostics

Certain components use both source level debugging and communication traces. These are detailed in the following sections.

**NOTE**

BMC Software recommends that you use the diagnostic facilities either as a precursor to working with BMC Customer Support, or in conjunction with them.

---

**Activating source level debugging diagnostics**

Source level debugging diagnostics in CONTROL-M/EM is activated per component for the following CONTROL-M/EM components:

- GUI Server
- Global Alerts Server
- Gateway (see also “Activating Communication Trace Diagnostics” on page 337)
- CONTROL-M Configuration Management Server
- CONTROL-M/EM Configuration Agent
- BMC Batch Impact Manager
- CONTROL-M Forecast
- Global Conditions Server (see “Diagnostics and the Global Conditions Server” on page 335)

Source level debugging diagnostic settings can be modified on both a persistent and a dynamic basis. It is advisable to modify using settings both methods. This means that changes can take effect immediately, without having to restart your system. In this way you do not lose production time, and when the system does restart, the settings will still be in effect.

Persistent (long term) changes are made by modifying the parameters in the component initialization (.ini) file. These remain set unless the file is altered. Information can then be recorded regarding events that occur over a period of time. Dynamic (immediate) changes are made by selecting a specific component from within the CONTROL-M Configuration Manager, and modifying the diagnostic settings accordingly.
The information collected when the DIAG diagnostics facility runs is collected in a log file. You can then look through the log file for any unusual activity that can help pinpoint the source of a problem.

For more information, see “Log files: Analyzing” on page 371.

Available diagnostic levels and advanced memory buffer

Diagnostic levels for CONTROL-M/EM range between 0 and 7. The default is 2.

The higher the level set, the more system resources are required. This can result in an environment functioning slower than usual.

This issue is resolved by the advanced memory buffer, which is set at level 4 by default, and prevents excessive slow-down in production.

Setting dynamic source level debugging diagnostics

To set dynamic source level debugging diagnostics, you must access the Control Shell window for a specific component, and modify the component settings accordingly.

**NOTE**

You should ensure that you also modify the persistent settings for the component. For more information, see “Setting persistent source level debugging diagnostics” on page 332.

For more information about the Control Shell and its functionality, see “Implementing job version management” on page 105.

To access the Control Shell (modifying dynamic diagnostic settings)

1. Open the CONTROL-M Configuration Manager.
2. Select the required component, and right-click.
3. Choose Control Shell.
4. In the “Specify...” field, enter one of the following diagnostic commands:
Setting persistent source level debugging diagnostics

To set persistent source level debugging diagnostics, you must access the initialization (.ini) file of a specific component, and modify the component settings accordingly.

**To access the .ini file**

1. Navigate to the following location:

   `<em_root>/ini/<component_name> DiagLvls.ini`

   The parameters that can be specified for setting persistent diagnostic levels are described in Table 56.

2. Modify the parameters accordingly, and save the file.

   **NOTE**
   
   Certain parameters can be modified dynamically, using the Control Shell. These are indicated clearly in Table 56. For more information, see “Setting dynamic source level debugging diagnostics” on page 331.

   A sample .ini file is displayed. See “Sample gsr_DiagLvls.ini file” on page 335.

---

**Table 55  Diagnostic commands using the Control Shell**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DIAGON</td>
<td>Starts the DIAG functionality running.</td>
</tr>
<tr>
<td>DIAGOFF</td>
<td>Stops the DIAG functionality running.</td>
</tr>
<tr>
<td>DIAGL</td>
<td>Set the debug level. For more information, see “Available diagnostic levels and advanced memory buffer” on page 331.</td>
</tr>
</tbody>
</table>
Table 56 Persistent diagnostic record file (.ini file) parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IsCyclic</td>
<td>Indicates whether the file is cyclic. Optional.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 (non-cyclic)</td>
</tr>
<tr>
<td></td>
<td>■ 1 (cyclic)</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td>NumOfFiles</td>
<td>Maximum number of cyclic files to create. Mandatory only if IsCyclic = 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter can also be modified dynamically.</td>
</tr>
<tr>
<td>NumOfMessages</td>
<td>Maximum messages in each cyclical file. Mandatory only if IsCyclic = 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter can also be modified dynamically.</td>
</tr>
<tr>
<td>*default</td>
<td>Debug level of the DIAG debug trace for the component.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0 (minimum messages) -7 (all messages).</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter can also be modified dynamically.</td>
</tr>
<tr>
<td>filename debug_level</td>
<td>Debug level is specified with the syntax: filename debug_level</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> filename is supplied by BMC Software Customer Support.</td>
</tr>
<tr>
<td></td>
<td>For example, gas_srv 5</td>
</tr>
<tr>
<td>MinimumDbgLvl</td>
<td>Message levels for messages sent to the log file and the memory buffer.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0 (no messages) - 7 (all messages)</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> MinimumDbgLvl 4 7 will set level 4 for the log file and 7 for</td>
</tr>
<tr>
<td></td>
<td>the memory buffer.</td>
</tr>
<tr>
<td>MemBufferSize</td>
<td>Buffer size in kilobytes.</td>
</tr>
<tr>
<td>size</td>
<td><strong>Valid values:</strong> 20 - 1000</td>
</tr>
<tr>
<td></td>
<td>The ctl utility can change the buffer size for the GUI Server and Global</td>
</tr>
<tr>
<td></td>
<td>Alerts Server during run time.</td>
</tr>
<tr>
<td>IsBufer</td>
<td>Specifies if the memory buffer is used or disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 – memory buffer is disabled</td>
</tr>
<tr>
<td></td>
<td>■ 1 – memory buffer is used</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
</tbody>
</table>
Table 56  Persistent diagnostic record file (.ini file) parameters (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| IsPIDUsed          | Specifies if the DIAG file name contains a Process ID (PID).  
                      **Valid values:**  
                      ■ 0 – PID is not included in the file name  
                      ■ 1 – PID is included in the file name  
                      **Default:** 0                                                                      |
| PrintLevelMaps     | Specifies if the list of DIAG levels for the process or component should be printed.  
                      **Valid values:**  
                      ■ 0 – levels should not be printed  
                      ■ 1 – levels should be printed  
                      **Default:** 0                                                                      |
| FlushBufferSize    | Number of bytes the buffer holds before it is flushed (that is, before DIAG messages are automatically written to file).  
                      **Default:** 0 - causes each DIAG message to be flushed immediately.                 |
| DiagStacksOn       | On and off toggle switch that controls whether an application stack trace is accumulated.  
                      **Valid values:**  
                      ■ 0 (off)  
                      ■ 1 (on)  |
| “Context”          | `@<context_name> <debug level>`  
                      Example: `@20 2`  
                      **Note:** Not for modification.                                                       |
| IgnoreMinimum      | **Default:** 0                                                                                                                                |
| ApplyCleanup       | Enables the clean up of old log files.  
                      **Default:** 0                                                                 |
| RetainDays         | Number of days a log file should exist before automatic deletion, according to the last modified date.  
                      **Default:** 3  |
| Enable             | Enables diagnostic functionality (on/off).  
                      **Note:** Equivalent to the dynamic settings DIAGON and DIAGOFF.  
                      **Default:** 1  |
Sample gsr_DiagLvlsls.ini file

```
MinimumDbgLvl 2 4
IsCyclic 1
NumOffFiles 5
NumOfMessages 25000
IsBuffer 1
MemBufferSize 5120
IsPIDUsed 1
PrintLevelMaps 1
DiagStacksOn 1
NumOfFormalObjects 100
@20 2 5
```

Diagnostics and the Global Conditions Server

This section describes:

- Setting cyclic GCS logging files on a dynamic and persistent basis
- Setting GCS source level debug diagnostics on a dynamic and persistent basis

**Setting cyclic logging files dynamically**

To set cyclic logging files on a dynamic basis, you must access the Control Shell window for GCS, and modify the settings accordingly.

For information about accessing the Control Shell, see “Setting dynamic source level debugging diagnostics” on page 331. For more information about the Control Shell and its functionality, see “Implementing job version management” on page 105.

**Setting cyclic logging files persistently**

For information about setting cyclic log files, and activating persistent settings for the GCS permanent log (GCS_LOG file), see Table 73 on page 431 in Appendix B, “System parameters.”

For more information about the GCS_LOG files, see “GCS_LOG files” on page 372.

**Setting dynamic source level debug diagnostics for the GCS (GCS_DIAG)**

To set cyclic diagnostic files on a dynamic basis, you must access the Control Shell window for GCS, and modify the settings accordingly.

For information about accessing the Control Shell, see “Setting dynamic source level debugging diagnostics” on page 331. For more information about the Control Shell and its functionality, see “Implementing job version management” on page 105.
Setting persistent source level debug diagnostics for the GCS (GCS_DIAG)

Setting persistent diagnostics for the Global Conditions Server differs from other CONTROL-M/EM components only because the file in which the settings are modified is the Defaults.rsc file, as opposed to an .ini file. The Defaults.rsc file is located:

- On UNIX: home_directory/site/resource/
- On Windows: home_directory\Gtwgcs\appl\site\resource

Table 57 displays the diagnostic parameters that determine the nature of the diagnostic messages displayed and collected in the GCS diagnostic files (GCS_DIAG). When set to default levels, only messages documenting more severe errors are displayed in the file. As soon as the settings are modified to a higher diagnostic level, more messages are displayed, encompassing a broader variety and severity of errors.

<table>
<thead>
<tr>
<th>Diagnostic parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **diag_module_lvl** ![integer2] integer1 | Determines the level of messages that are collected in the GCS_DIAG file. ![integer1]: The level of messages collected in the GCS_DIAG file. ![integer2]: Determines the module ID for which the diagnostics should be applied.  
**Note:** If no value is specified for ![integer2], the level defined in the ![integer1] value is applied for all modules.  
**Valid values (for ![integer1]):**  
- 0 – No messages  
- 1 – Error or exception messages (default)  
- 2 - 4 – Each higher level collects the messages from all of the lower levels. |
| **db_diag_lvl** | Determines the message levels for database diagnostic messages related to the Global Conditions server that are collected in the GCS_DIAG file.  
**Valid values:**  
- 0 – No database message collection (except those collected by db_diag).  
- 1 - 5 – Each higher level collects the messages from all of the lower levels.  
**Default:** 0 |
| **diag_size** | Maximum number of record lines in the GCS_DIAG file, where ![integer] indicates the number of rows permitted per file.  
**Default:** 25,000  
**Note:** Specifying 0 indicates no limitation on size. |
| **max_diags** | Maximum number of diagnostic files to be managed cyclically, where ![integer] indicates the required quantity of diagnostic files.  
**Default:** 10  
**Note:** Specifying 0 indicates no limitation on size. |
Activating Communication Trace Diagnostics

With communication trace diagnostics, the method in which they are read by the application does not use an initialization file. Rather parameters can be added to the command invocation, and once they have been added, become a permanent part of said invocation.

Communication trace diagnostics can be activated for the following components:

- Global Conditions Server
- Gateway

To set communication trace diagnostics

1. From the CONTROL-M Configuration Manager, right-click the required component, and select the Control Shell.

2. Click the **Usage** button.

   The list of available commands is displayed. These commands are described in Table 58.

3. Copy and paste the required command into the "Specify..." field, and click **OK**.

Table 58 Communication trace diagnostic commands (part 1 of 2)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CHANGE_LOG</td>
<td>Closes the current gateway log file and opens a new one.</td>
</tr>
<tr>
<td>TRACE_DISABLE_ALL</td>
<td>Stops all debug printing.</td>
</tr>
<tr>
<td>TRACE_DB</td>
<td>Sets the debug level. Valid values: 0 - 9. 0 turns off debugging.</td>
</tr>
<tr>
<td>TRACE_CTM on</td>
<td>Starts output of host debug messages.</td>
</tr>
<tr>
<td>TRACE_CTM off</td>
<td>Stops output of host debug messages.</td>
</tr>
<tr>
<td>TRACE_TRUNC on</td>
<td>Starts truncating messages. The header and one row of data remain.</td>
</tr>
<tr>
<td>TRACE_TRUNC off</td>
<td>Stops truncating messages.</td>
</tr>
<tr>
<td>TRACE_KLIVE on</td>
<td>Starts debugging “keep alive” messages.</td>
</tr>
<tr>
<td>TRACE_KLIVE off</td>
<td>Stops debugging “keep alive” messages.</td>
</tr>
</tbody>
</table>
### Table 58  Communication trace diagnostic commands (part 2 of 2)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TRACE_JOB_MESSAGE on</td>
<td>Starts dumping job messages about active job downloads, active job updates, and scheduling table uploads. Default: This option is active.</td>
</tr>
<tr>
<td>TRACE_JOB_MESSAGE off</td>
<td>Stops dumping job messages.</td>
</tr>
<tr>
<td>TRACE_LINK_CTM on</td>
<td>Starts a debug trace for the host link.</td>
</tr>
<tr>
<td>TRACE_LINK_CTM off</td>
<td>Stops a debug trace for the host link.</td>
</tr>
<tr>
<td>TRACE_LINK_CLIENT on</td>
<td>Starts a debug trace for the GUI link.</td>
</tr>
<tr>
<td>TRACE_LINK_CLIENT off</td>
<td>Stops a debug trace for the GUI link.</td>
</tr>
<tr>
<td>TRACE_CLIENT on</td>
<td>Starts a debug trace for the GUI.</td>
</tr>
<tr>
<td>TRACE_CLIENT off</td>
<td>Stops a debug trace for the GUI.</td>
</tr>
</tbody>
</table>
Activating diagnostics for CONTROL-M/Server

Activating diagnostic functionality for CONTROL-M/Server is done using the CONTROL-M Configuration Manager, as described in the following procedure.

**NOTE**

BMC Software recommends that you use the diagnostic facilities either as a precursor to working with BMC Customer Support, or in conjunction with them.

To activate CONTROL-M/Server diagnostics

1. From the CONTROL-M Configuration Manager, right-click the required CONTROL-M/Server.

2. Select **CONTROL-M/Server Debug** from the menu displayed. The CONTROL-M/Server Debug window is displayed (see Figure 25).

**Figure 25  CONTROL-M/Server Debug window**

![CONTROL-M/Server Debug window](image)

Displayed in this window are all the CONTROL-M/Server processes.

3. Specify a debug level for each process, and click **OK**.
Activating diagnostics for CONTROL-M/Agent

Activating diagnostic functionality for CONTROL-M/Agent is done using the CONTROL-M Configuration Manager, as described in the following procedure.

To activate CONTROL-M/Agent diagnostics

1. From the CONTROL-M Configuration Manager, right-click the required CONTROL-M/Agent.

2. Select CONTROL-M/Agent Debug from the menu displayed. The CONTROL-M/Agent Debug window is displayed (see Figure 26).

Figure 26  CONTROL-M/Agent Debug window

3. Select the required CONTROL-M/Server and CONTROL-M/Agent in the appropriate fields.

4. Set the diagnostic level as required.

---

**NOTE**

Valid values range from 0 to 5, where 0 indicates no diagnostic activity, and 5 indicates the highest level of diagnostic functionality.

---

**NOTE**

Valid values range from 0 to 4, where 0 indicates no diagnostic activity, and 4 indicates the highest level of diagnostic functionality.
5 Set the communication trace level, as required.

--- NOTE ---
The trace level can be set to ON by setting the value to 1 and can be set to OFF by setting the value to 0.

6 Click OK.
Collecting diagnostic data

This section describes the method for collecting diagnostic data for CONTROL-M/EM, CONTROL-M/Agent, CONTROL-M/Server, and related applications. Diagnostic information collected using such methods can assist in troubleshooting using the extensive data and information collected.

A section is also included on a specific utility used to collect information regarding CONTROL-M/Agent specifically. For more information, see “CONTROL-M/Agent data for BMC support (Agent Check utility)” on page 344.

NOTE

Once collected, the diagnostic information can then be analyzed. For more information about this, see Chapter 15, “Processes of elimination and analysis.”

CONTROL-M data for BMC support (Health Check utility)

The Health Check utility is used to collect diagnostic data for CONTROL-M/Enterprise Manager, CONTROL-M/Server, CONTROL-M/Agent BMC Batch Impact Manager, and CONTROL-M/Forecast.

Diagnostic data can also be collected for additional CONTROL-M applications, including the CONTROL-M/Control Modules and the BMC CONTROL-M Business Process Integration Suite.

The CONTROL-M Health Check utility scans and collects system information about the CONTROL-M environment and its various components. This information is used to troubleshoot and correct problems. The information gathered is packaged in a compressed hierarchical format that allows for analysis of the collected information. The hierarchy is important in determining the nature of the collected data.
The Health Check information is gathered based on either Categories or Profiles.

- Categories are different types of information from various parts of your system.
- Profiles are used to group categories according to a common denominator.

The Health Check utility should always be used in conjunction with BMC Customer Support.

For information about configuring, using and executing the Health Check utility, see the CONTROL-M Utility Guide.

**CONTROL-M/Agent data for BMC support (Agent Check utility)**

The CONTROL-M Agent Check Utility (ACU) is an additional tool that collects information and diagnostic data about the CONTROL-M Agent installation, execution state, and target environment. The data collected by the ACU is designed to assist CONTROL-M/Agent administrators and BMC Software technical support engineers to troubleshoot, fine-tune, and maintain the CONTROL-M/Agent.

With this tool, you can send generated reports to interested parties using e-mail or FTP to BMC Software (ftp://ftp.bmc.com/incoming). You can print the report to a hierarchical XML file, or save the report as a text file. In addition, you can set the agent debug level and download the most recent agent and CM patches.

This utility is located at /<agentDirectory>/ctm/exe/ and can be run from either the command line or as a Java application. For more information, see the CONTROL-M Utility Guide.
Processes of elimination and analysis

Prior to engaging in the more complex methods of diagnostic activity which require you to work in conjunction with BMC Customer Support, there are certain tasks that you can perform yourself, where applicable. These are described in this chapter.

You are also encouraged to find more information about problems with or questions about a BMC products at the Customer Support website at http://www.bmc.com/support_home. You can search the Knowledge Base for existing product resolutions, documentation, and FAQs. You can also view or download product documents, find answers to frequently asked questions, and download products and maintenance. If you do not have access to the web and you are in the United States or Canada, contact Customer Support at 800 537 1813. Outside the United States or Canada, contact your local BMC office or agent.

**NOTE**

If the procedures for processes of elimination do not reveal a solution to or clear source of whatever issue you are experiencing, please contact BMC Customer Support.

Also described in this chapter are the following:

- “Troubleshooting by process of elimination” on page 346
- “Checking CONTROL-M/EM communication” on page 347
- “Analyzing diagnostic data for CONTROL-M/Server” on page 367
- “Log files: Analyzing” on page 371
- “Working with Exception Alerts” on page 375
Troubleshooting by process of elimination

When unexpected issues arise, there are certain checks that should be performed in order to establish that the cause cannot be remedied relatively simply. This section describes some of the more common checks that can be executed prior to contacting BMC Customer Support. Some of these checks use a process of elimination to attempt to determine the cause of a problem.

Also discussed are basic diagnostic procedures that can be performed so that the resulting log files can indicate to BMC Customer Support upon initial contact what the nature and scope of the problem could be.

The following topics are included in this section:

- “Checking communication status between CONTROL-M/EM and CONTROL-M/Server” on page 346
- “Checking CONTROL-M/EM communication” on page 347

Checking communication status between CONTROL-M/EM and CONTROL-M/Server

This diagnostic procedure is for occurrences when it appears that there is no communication between CONTROL-M/EM server and CONTROL-M/Server. This symptom is likely to be displayed in the CONTROL-M Configuration Manager as CONTROL-M Configuration Agent Not Available.

Before engaging in more complex and script-specific diagnostic activities when checking the communication status between CONTROL-M/EM and CONTROL-M/Server, Table 59 describes certain basic functions that should be inspected first.

Table 59  Checks to make when CONTROL-M Configuration Agent Not Available

<table>
<thead>
<tr>
<th>Status check</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Check host and Configuration Agent port number</td>
<td>Ensure that the configuration specifications of the <strong>host name</strong> and <strong>Configuration Agent port number</strong> are identical in both the specific CONTROL-M iteration, and in the CONTROL-M/EM server. Check that the Configuration Agent is up and running.</td>
</tr>
<tr>
<td>Use netstat –na</td>
<td>Check the status of the Configuration Agent port.</td>
</tr>
<tr>
<td></td>
<td>Also check that CONTROL-M/Server is “listening” to the Configuration Agent port.</td>
</tr>
</tbody>
</table>

Once you have established that the above functions are configured correctly, the need to investigate further is justified.
Checking CONTROL-M/EM communication

Use the following procedures to check CONTROL-M/EM communication.

Communication trace debugging in the Gateway

If issues arise with the Gateway component of CONTROL-M/EM, there can be many symptoms which could indicate various issues. Nearly all of these symptoms will display as an error in the CONTROL-M/EM active environment. Setting a communication trace debug, and recreating the situation is the best advised way in which to determine the nature of the problem and the best course of action (usually, in conjunction with BMC Customer Support).

The Gateway is running but is not synchronized with CONTROL-M/Server

This generally displays as communication status “down” in the CONTROL-M Configuration Manager.

1. From the CONTROL-M Configuration Manager, right-click the specific Gateway, and select Control Shell.

2. Specify TRACE_LINK_CTM on, and click Apply.

3. Specify TRACE_CTM on, and click Apply.

4. Recreate the situation where the problem was first noticed.

**NOTE**

To end the communication trace, specify TRACE_DISABLE_ALL.

Gateway appears to be stuck downloading

There are constant “downloading, download failed” error messages that repeat cyclically.

1. From the CONTROL-M Configuration Manager, right-click the specific Gateway, and select Control Shell.

2. Specify TRACE_LINK_CTM on, and click Apply.

3. Recreate the situation where the problem was first noticed.
Checking CONTROL-M/EM communication

**NOTE**
To end the communication trace, specify `TRACE_DISABLE_ALL`.

---

**Gateway “bounces”**

The Gateway status changes from Up to Down and back again, frequently.

**NOTE**
Due to the apparent instability of the Gateway, you cannot use the Control Shell functionality.

1. Double-click the Gateway in CONTROL-M Configuration Manager.
2. In the displayed CONTROL-M Component window, enter the following command in the Additional Parameters field:

   ```
   -dbg 3
   ```
3. Recreate the situation where the problem was first noticed.

---

**User actions take an unusually long time**

This causes a timeout to occur. Such actions can include such issues as not seeing updates after a certain action has been performed, or an upload (or download) not succeeding or taking longer than usual.

1. From the CONTROL-M Configuration Manager, right-click the specific Gateway, and select Control Shell.
2. Specify `TRACE_LINK_CTM on`, and click Apply.
3. Specify `TRACE_CLIENT on`, and click Apply.
4. Recreate the situation where the problem was first noticed.

**NOTE**
To end the communication trace, specify `TRACE_DISABLE_ALL`.

---
After setting these traces and recreating the situation, you should run the Health Check utility to collect the relevant data. For more information, see Chapter 14, “Collecting diagnostic data.”

GUI Server: Processes of elimination

The following topics describe some common issues that occur, and the processes of elimination that should be observed before taking diagnostic activity to the next level.

The GUI Server does not “come up” when it should

Possibility 1: The CONTROL-M/EM Configuration Agent fails to respond

NOTE

This issue can also occur with components other than the GUI Server.

1 In the CONTROL-M Configuration Manager, select the row that displays the CONTROL-M/EM Configuration Agent details.

2 Check the text of your selection in the Message column.

   A message similar to the following is displayed:

   EM Configuration Agent Not Available

3 To make the CONTROL-M/EM Configuration Agent Available, use one of the following commands and then try to bring the GUI Server up again.

   ■ In Windows, start the CONTROL-M/EM Configuration Agent Service.
   ■ On UNIX, use the check_config_agent command.

4 If the GUI Server now comes up, no further diagnostics is required. Otherwise, proceed to the next possibility.

Possibility 2: The Database is not responding

There will be a clear indication in the CONTROL-M Configuration Manager, if this is the case.
GUI Server: Processes of elimination

1 Examine the Database status, displayed at the bottom left corner of the CONTROL-M Configuration Manager window.

2 If it is **Unavailable**, make it **Available**.

   Follow the procedure applicable to your database to make it Available.

3 If the GUI Server now comes up, no further diagnostics required. Otherwise, proceed to the next possibility.

**Possibility 3: The CONTROL-M/EM Configuration Agent is available but has exceeded its retry limit for this component**

   **NOTE**
   
   This issue can also occur with components other than the GUI Server.

1 On the GUI server, change the **Desired State** from **Up** to **Ignore**.

2 Wait for two or three minutes.

3 Change the **Desired State** back to **Up**.

4 If the GUI Server now comes up, no further diagnostics required. Otherwise, proceed to the next possibility.

**Possibility 4: The Naming Service is unavailable or not responding**

1 Check that:

   - In Windows, the **TAO NT Naming Service** is started. If not, start this service.
   - On UNIX, run the `check_ns_daemon` script to check if the Naming Service is up. If not, bring the Naming Service up by using the `start_ns_daemon` script.

2 If the GUI Server now comes up, no further diagnostics required. Otherwise, contact BMC Customer Support for directions on the best way to diagnose, and analyze this problem.

   **NOTE**
   
   This issue can also occur with components other than the GUI Server.


User cannot log on

Possibility 1: The Naming Service is down

An error message is displayed that indicates either an incorrect configuration, or that the database is down.

1. Fix the configuration, or bring the Naming Service back up.
   - In Windows, start the TAO NT Naming Service.
   - On UNIX, run the check_ns_daemon script to check if the Naming Service is up. If not, bring the Naming Service up by using the start_ns_daemon script.

2. If you can now log on, no further diagnostics required. Otherwise, proceed to the next possibility.

Possibility 2: The GUI Server is down

An error message is displayed indicating possible reasons why the GUI Server is down.

1. Ensure that you bring the GUI Server back up.

2. If you can now log on, no further diagnostics required. Otherwise, proceed to the next possibility.

   NOTE

See also “The GUI Server does not “come up” when it should” on page 349.

Possibility 3: The database server is down

This is indicated in the bottom left corner of the CONTROL-M Configuration Manager.

This could be an isolated problem between the GUI Server and the database.

1. Check the GUI Server log for the most recent instance of the wording vendorMessage, and for any messages displayed immediately after an “equals” symbol (“=”). Contact your Database Administrator with this information.

   After your Database Administrator has resolved the issues arising from these messages, continue with step 2.
NOTE
It is advisable to run both the PINGDB and CHECKDB scripts, as they will enable more information about the situation to be available.

2 If you can now log on, no further diagnostics required. Otherwise, contact BMC Customer Support for directions on the best way to diagnose, and analyze this problem.

Global Conditions Server: processes of elimination

The basic problems that arise in the Global Conditions Server are either that a condition does not exist where it should, or that a condition exists where it should not.

Check the GCS_LOG file

1 This file is an out-of-the-box diagnostic tool that exists in CONTROL-M/EM.

Use this file to determine whether this is a single or multiple condition issue.

Table 60 lists reasons that indicate a single condition issue.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Toggling conditions</td>
<td>If the word TOGGLED is displayed in the GCS_LOG file in relation to the global condition is question, it means that the issue has arisen as a result of toggling behavior, which in turn might indicate that there is a problem. Contact BMC Customer Support with this information.</td>
</tr>
<tr>
<td>Incorrectly defined conditions</td>
<td>There are two possible indications of this.</td>
</tr>
<tr>
<td></td>
<td>Check to see if the condition was received from the source, but not sent to the target.</td>
</tr>
<tr>
<td></td>
<td>Or check to see if the expected condition is absent completely from the file.</td>
</tr>
<tr>
<td></td>
<td>This can also indicate other things, for example, a problem with the Gateway.</td>
</tr>
<tr>
<td>Heavy condition distribution activity</td>
<td>If there is an unusual flow of messages in the GCS_LOG file; for example, a non-systematic flow with large numbers of timestamps that are very close together in chronology, or a large number of messages with the word REJECTED included, or evidence that the same conditions were sent over and over again.</td>
</tr>
<tr>
<td></td>
<td>This might indicate that specific conditions are affected, or that all conditions are affected.</td>
</tr>
</tbody>
</table>
Table 61 lists reasons that indicate a multiple condition issue.

<table>
<thead>
<tr>
<th>Reason</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Heavy condition distribution activity</td>
<td>If there is an unusual flow of messages in the GCS_LOG file; for example, a non-systematic flow with large numbers of timestamps that are very close together in chronology, or a large number of messages with the word REJECTED included, or evidence that the same conditions were sent over and over again.</td>
</tr>
<tr>
<td>Communication problems between the GCS and the Gateway</td>
<td>If conditions do not appear (as either Received or Sent) in the GCS_LOG file (meaning that no lines for the conditions are showing up in the file), or lines of conditions repeat themselves without a successful report, or no line contains the word CONFIRMED.</td>
</tr>
<tr>
<td>Problematic conditions clean-up policy</td>
<td>This typically happens near the time when the New Day is scheduled to start, and is indicated by a sequence of large numbers of conditions (possibly with old dates assigned to them).</td>
</tr>
</tbody>
</table>

2. If the GCS_LOG file does not identify the problem, run the GCS_DIAG diagnostic procedure, and recreate the situation. Also, contact BMC Customer Support for directions on the best way to diagnose, and analyze this problem.

3. If after this you have still not identified the problem or how to treat it, you have two further options, which you can do in conjunction with BMC Customer Support

- Run the Health Check utility and recreate the situation.
- Advance the diagnostic settings for the GCS and relevant Gateways, then run the Health Check utility and recreate the situation.

**Naming Service and Firewall functionality**

Use the following to troubleshoot aspects of the Naming Service and Firewall functionality. level.

**Naming Service problems**

Table 62 describes troubleshooting aspects related to Naming Service problems.
### Table 62  Troubleshooting aspects related to Naming Service problems (part 1 of 2)

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
</tr>
</thead>
</table>
| Invalid repository directory         | If the repository directory (-u parameter) is invalid or cannot be created (due to insufficient permissions or space, and so on), the Naming Service fails to start and the following error message is displayed:  

Invalid persistence directory  
Failed to start the Naming Service. |
| How to reset the Naming repository   | Stop all CONTROL-M/EM components that depend on the Naming Service by using the `orbadmin ns stop` command.  
Delete all files under the `$HOME/var` directory (default repository path), run the `orbadmin ns start` command and start CONTROL/EM components. |
| Invalid process ID file name         | If the Naming Service is run with a `-p` parameter for process ID file name but the path given is invalid or cannot be created (due to insufficient permissions or space, and so on), the Naming Service starts and no error message is displayed but a pid file is not created.  
In this case, the `orbadmin ns stop` command does not work (UNIX only) because the process ID of the Naming Service is unknown. |
| Naming Service listening port is not free | If the listening port for the Naming Service is not free, the Naming Service fails to start and the following error message is displayed:  

```
EXCEPTION, TAO_Naming_Server::init  
system exception, ID  
'IDL:omg.org/CORBA/BAD_PARAM:1.0'  
TAO exception, minor code = 62 (endpoint initialization failure in Acceptor Registry; low 7 bits of errno: 98 Unknown error), completed = NO  
```

Failed to start the Naming Service. |
Invalid listening port for the naming service

If the listening port for the naming service is invalid (such as 1234567), the Naming Service fails to start and the following error message is displayed:

```
EXCEPTION, TAO_Naming_Server::init
system exception, ID
'IDL:omg.org/CORBA/BAD_PARAM:1.0'
TAO exception, minor code = d (endpoint initialization failure in Acceptor Registry: EACCES), completed = NO
```

Failed to start the Naming Service.

Invalid IIOP reference: -ORBListenEndpoints parameter

If the IIOP reference (-ORBListenEndpoints parameter) for the Naming Service has an unknown host name or invalid IP address, the Naming Service fails to start and the following error message is displayed:

```
EXCEPTION, TAO_Naming_Server::init
system exception, ID
'IDL:omg.org/CORBA/BAD_PARAM:1.0'
TAO exception, minor code = d (endpoint initialization failure in Acceptor Registry: EACCES), completed = NO
```

Failed to start the Naming Service.

**CORBA server problems**

Table 62 describes troubleshooting aspects related to CORBA server problems.
### Table 63  Troubleshooting aspects related to CORBA server problems (part 1 of 2)

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
</tr>
</thead>
</table>
| The reuse_addr flag in -ORBListenEndpoints | In CONTROL-M/EM 6.3.01 and later, CORBA servers on UNIX that are configured to use a specific listening port, start only if that port is free. If the listening port is now marked by the operating system as any of the following, the CORBA server does not start:  
  - TIME_WAIT  
  - FIN_WAIT_2  
  - CLOSE_WAIT  
  
  **Note:** Use the `netstat -na` command to see the status of the port.  
  
  This behavior is controlled by the reuse_addr flag, which is set in the -ORBListenEndpoint parameter.  
  
  **Example**  
  
  A valid endpoint value of a CORBA server which is set to listen on port 4444 is:  
  
  ```-iiop://:4444/reuse_addr=0```  
  
  This is to stop the effect of a CORBA server (on UNIX) appearing to be working when connected to an occupied listening port, when in fact no communication with it is possible. |
Table 63 Troubleshooting aspects related to CORBA server problems (part 2 of 2)

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
</tr>
</thead>
</table>
| svc.conf file (-ORBSvcConf parameter) cannot be found | If the svc.conf file (-ORBSvcConf parameter) cannot be found, the Naming Service fails to start and the following error message is displayed:  

```
TAO (4928|1) Service Configurator unable to open file svc.conf
(4928|1) Unable to initialize the Service Configurator: Invalid argument
(4928|1) EXCEPTION. TAO_Naming_Service::init  
```

system exception, ID

```
'IDL:omg.org/CORBA/INITIALIZE:1.0'
```

TAO exception, minor code = 0 (ORB Core initialization failed; unspecified errno), completed = NO Failed to start the Naming Service.

**Workaround:** Provide the correct filename or directory path.

| javaw.exe - Entry Point Not Found | When running orbconfigure.vbs, the following message is generated if the correct version of dbghelp.dll is not in the d:\winnt\system32 directory:  

```
The procedure entry point SymFromAddr could not be located in the dynamic link library dbghelp.dll
```

This happens even if %NDS_ECS_ROOT% (or Product_Install_Dir)/bin is in the PATH environment variable. The search order for loading libraries is:

- working directory
- system32
- PATH

Do not replace dbghelp.dll in the system32 directory.

**Workaround:** Run orbconfigure from a directory that has the correct dbghelp.dll.

How to verify that a CORBA server is listening on port X

1. Use the NamingViewer utility to find the desired object’s IOR reference.
2 Enter the command:

```
catio name_of_file_containing_IOR_or_IOR_itself
```

You will obtain information about the object's reference, including the port number. Use this procedure to ensure an application is actually listening on the port you specified in the orbconfigure GUI Ports panel. If the port is not the one you specified, the process probably was not recycled after the port was assigned.

**ViewPoint is not able to load when connecting through a VPN**

Network connection problems can result in one of the following:

- The CONTROL-M/EM GUI appears to open a ViewPoint, but it is unable to establish a connection with the GUI Server.
- CONTROL-M/Desktop does not respond to callback actions, such as uploading tables, ordering jobs, and so on.
- When you run the CLI and Sweep utilities, the operations are completed, but the utilities do not respond.

**Problem**

The GUI Server attempts to communicate with the CONTROL-M/EM GUI using an IP address that is not accessible and therefore the callback action fails.

Initially, the CONTROL-M/EM GUI sends an IP address it wants the GUI Server to use when talking back to it in the IOR (IOR is a CORBA term). This is a random IP address received from the operating system.

However, if the computer on which the CONTROL-M/EM GUI is installed has either multiple network adapters or uses VPN or NAT, the IP address that the CONTROL-M/EM GUI gives the GUI Server might not be the correct one, and as a result, the callback action fails.

The failed callback action cannot be resolved by using the CONTROL-M/EM GUI host name instead of the GUI Server's because the CONTROL-M/EM GUI host name might not be resolved successfully (for example, when using VPN), and it will not be sent to the GUI Server as expected. The GUI Server's host name, however, is always accessible to a CONTROL-M/EM GUI, therefore, the valid host name (the GUI Server) is used instead.
Previously, you had to identify what the correct IP address is and then configure the CONTROL-M/EM GUI to publish that IP address. The IP address can change regularly and, since there might be more than one IP address from which to choose, it is difficult to know which is the correct one.

Once you identify the correct IP address, the change is made using the orbadmin utility or the orbconfigure application, causing the CONTROL-M/EM GUI to advertise a known and accessible address.

**When communication between the CONTROL-M/EM GUI and the GUI Server is not bidirectional**

Use the following procedure to tell the client application which IP address to prefer to publish by specifying the preferred subnet mask. Using this method, you do not have to specify the exact IP address generated dynamically, which might change upon every VPN connection.

Once you have the subnet mask, you can specify the $IP variable, which the application replaces during runtime using the specified subnet mask.

1. Identify the subnet mask of the dynamic IP addresses generated by the VPN adapter or additional interface.

   A. Connect to the network or VPN and note the IP address.

   B. Disconnect and reconnect to the network or VPN and note the IP address.

   **EXAMPLE**

   If the first time you connected the IP address was 192.68.12.6 and the second time you connected the IP address was 192.68.12.24, your subnet mask is 192.68.12.0

2. Add the -PreferIPMask parameter to the config.xml file, using the following orbadmin command:

   orbadmin variable create -scope default -value 192.68.12.0 -PreferIPMask

   Adding this variable to the default scope enables the other scopes to inherit the information.

3. Edit the -ORBListenEndpoints parameter, using the following orbadmin command:

   orbadmin variable modify -scope GUI -value iiop:///hostname_in_or=$IP -ORBListenEndpoints
NOTE

You can define the -ORBListenEndpoints parameter in the default scope instead of each individual scope (similar to the -PreferIPMask), but you must make sure to remove the -ORBListenEndpoints parameter from the other scopes (GUI, CLI, sweep, and Desktop) so as not to overwrite the value in the default scope.

The $IP variable receives its value according to the -PreferIPMask parameter. The application publishes the first IP address that matches the subnet specified in -PreferIPMask.

NOTE

If no IP address matches the specified subnet or the -PreferIPMask parameter is not defined, $IP is set to the default IP address associated with the computer’s hostname.

This way there is no need to modify the configuration when you are not using the VPN or other network adapter.

CONTROL-M/EM support for computer aliases (/etc/hosts)

Mapping aliases in local files, such as %windir%\system32\drivers\etc\hosts on Windows, is usually not sufficient. The local alias is valid only for the computer where it was defined.

In the CORBA implementation used in CONTROL-M/EM, both the client and server exchange their host names and try to access each other using them. If another computer tries to access the computer with the alias, the call fails.

For some cases, adding the alias to every single computer’s /etc/hosts file helps. In other cases, network concerns make this impossible. In this case, the preferable solution is to define an alias on DNS/NIS, and then configure CONTROL-M/EM with this alias. If this is not desirable, you can switch to using IP addresses instead.

Client cannot connect to Server with IOR IP address 127.0.0.1

When determining the endpoint for a server, CORBA chooses an interface from the interfaces available to the system and encodes its address in the IOR. If CORBA chooses 127.0.0.1 (the local loop back) as the endpoint address, then it could not find any other suitable interfaces. Because this address is only visible to the local platform, no other platform can connect to the local platform using that address.

If a dynamic interface is available to the system, you might need to explicitly specify that CORBA should use that interface in the first page (listening interface) of the orbconfigure GUI.
Firewall configuration requirements

If problems with empty ViewPoints or TCP/IP connections persist, the firewall might not be configured properly.

- The incoming ports selected in the Naming Service panel of the Domain Configuration window must be open and the TCP/IP protocol must be allowed.
- If not using bidirectional communications, all Outgoing ports above 1024 must allow TCP/IP communication on the server’s side.
- Generic firewall rules should not supersede the rules mentioned above.

Troubleshoot firewall problems by looking at the messages in the firewall log. The firewall should log traffic incoming to and outgoing from the suspect computer. Consult the firewall vendor’s manual.

Normally, it is possible to determine:

- Whether the firewall is denying access to a valid port. Review the firewall rules and correct the problem.
- Whether CONTROL-M/EM is not communicating over the correct ports. To try to understand why:
  - Examine the domain configuration file (config.xml) and check that the correct ports are assigned there.
  - Stop CONTROL-M/EM components and the Naming Service. Restart and retry. CONTROL-M/EM applications should have been recycled after specific ports were assigned. In some cases, a restart might be necessary.
  - Reassign ports, paying attention to any messages (for example, a port is already used) that might have been overlooked when the ports were originally assigned.

In rare cases, other network devices, including secondary firewalls, might interfere with traffic. Contact your System Administrator and make sure this is not the case.

NAT (Network Address Translation) environment

To support CORBA communication in a NAT environment, both client and server must know each other by the same host name. IP addresses cause communication to fail in a NAT environment because the IP addresses change dynamically. If more than one computer (such as an additional firewall) is performing NAT along a network path, the host names also must be known by this computer.

The existence of NAT in a network does not necessarily cause a problem. However, the requirements described below are necessary when IP addresses for the same computer are different on the client and server side.
All the following conditions must be true when choosing a host name for a computer that communicates via CORBA in a NAT environment:

- The server must know itself by the host name chosen for it.
- Each client must know the server by that same host name.
- Each client must know itself by the host name chosen for it.
- The server must be able to see each client using that client’s chosen host name.

**NOTE**

Variations such as `myserver`, `myserver.domain` and `myserver.domain.com` are *not* considered to be the same host name.

For example, if a client is called `client1`, the command `ping client1` must work both on the client and server side.

It is important to understand these requirements because:

- They are not the usual default in corporate networks today.
- They are not always easy to satisfy. It might be difficult, for example, for the system administrator to get a UNIX server to see each client computer by name, especially if there are many client computers.

If these requirements are met, configure the CONTROL-M/EM servers and clients to use host names or virtual host names as required.

### Deleting entries from the Naming Service

1. Make sure that the Naming Service is running by using the following command:

   ```
   orbadmin ns status
   ```

2. Check the Naming Service corbaloc reference by using the following command:

   ```
   orbadmin variable show --scope default --ORBInitRef
   ```

3. Find the full path of the entry you require to delete by using the following command:

   ```
   orbadmin ns list
   ```

   **NOTE**

   The `-nsdel` command deletes all entries from the `--name` specified and below it.

4. From a local or a remote computer, use the following command:
Naming Service and Firewall functionality

Example

-nsdel -ORBInitRef NameService=corbaloc::1.2@<ns host>:<ns port>/NameService --name "<full path of entry to delete>"

Example

-nsdel -ORBInitRef NameService=corbaloc::1.2@lotus:13075/NameService --name “BMC Software/ECS/GUI”

Normally there is no need to use the -nsdel command and manually delete entries from the Naming Service, as servers clean their references when they shut down. However, in cases where servers are stopped without the chance to clean up their references, the problematic references will stay in the Naming Service repository.

Naming Service failed to start

Use the following procedure when there is a Naming Service failure.

1 Start the Naming Service by using the following command:

    orbdadmin ns start

    This command attempts to start the Naming Service and then attempts to resolve it to verify that the process is running and ready to answer for requests.

2 To make sure that the failure reported by orbdadmin was not a result of a short resolve timeout, use the following command:

    orbdadmin ns status

3 In case the Naming Service is not running, add diagnostics on Naming Service by using the following commands to add diagnostics on Naming Service:

    orbdadmin variable create -scope ns -value 5 -ORBDebugLevel
    orbdadmin variable create -scope ns -value <logfile_fullpath> -ORBLogFile

The Naming Service does not accept certain CONTROL-M/EM parameters, such as:

- -BiDirPolicy
- -APPSSL
- -ThreadPoolSize
- -RTTimeoutPolicy
To display the Naming_Service parameters and make sure there's nothing wrong

Use the following command:

```
orbadmin scope show ns
```

The default setting for the Name Service endpoint is:

```
iiop://hostname:13075
```

To determine the Naming Service endpoint value

Use the following command:

```
orbadmin variable show -scope ns -ORBListenEndpoints
```

To make sure that this endpoint value is valid, that the port is free and that the network interface is valid and identified

Use the following command:

```
netstat -na | grep <port-number>
```

```
nslookup <hostname>
```

If nslookup fails, the computer does not identify itself as the network interface specified in the endpoint (in this case, the computer's short hostname).

To solve this configuration problem perform the following steps

1. Allow the Naming Service to listen on all available network interfaces by removing the listening host from the endpoint value by using the following command:

   ```
   orbadmin variable modify -scope ns -value iiop://:13075 -ORBListenEndpoints
   ```

2. Make sure that the other servers running on this computer are accessible in the network.

3. Find out which network interface is identified (the computer’s explicit IP address, a Fully Qualified Domain Name (FQDN), and so on).

4. Use the orbconfigure utility to set this valid value as the virtual hostname in the Published address drop-down list.
If the steps above still do not solve the problem, send the output of the above steps (including `<logfile_fullpath>`) plus the information detailed below to BMC Customer Support.

**TAO information required when opening a case**

Provide the following from both the computer of the server and from the computer of the client.

**Table 64 TAO information required**

<table>
<thead>
<tr>
<th>UNIX</th>
<th>Microsoft Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>ipconfig -a</td>
<td>ipconfig /all</td>
</tr>
<tr>
<td>/etc/hosts</td>
<td>%windir%/system32/drivers/hosts</td>
</tr>
<tr>
<td>env</td>
<td>set</td>
</tr>
<tr>
<td>N/A</td>
<td>SECS_HOME/etc/domains/config.xml</td>
</tr>
<tr>
<td>list_interfaces</td>
<td>list_interfaces</td>
</tr>
<tr>
<td>generate_ior</td>
<td>catior -x</td>
</tr>
<tr>
<td>generate_ior -ORBDDottedDecimalAddresses 1</td>
<td>catior -x</td>
</tr>
<tr>
<td>orbadmin ns list</td>
<td>orbadmin ns list</td>
</tr>
</tbody>
</table>

**On the client computer**

run nslookup <GSR computer> | run nslookup <GSR computer>

**On the server computer**

run nslookup <GUI computer> | run nslookup <GUI computer>

**Not able to reach a UNIX Naming Service from a Windows computer**

When a Naming Service that runs on a UNIX computer (probably a new computer) cannot be reached from a Windows computer, but you can reach the Naming Service from any other UNIX computer, it means that the UNIX computer is not configured properly.

Use the following command:

```
generate_ior | catior -x
```

This command generates a dummy IOR, and then displays it after it has been parsed by catior.

Examine the hostname. It is likely that it is different from the hostname you are using.
Example 1

The computer with a hostname of banzai was called the same IP address in NIS (nslookup from a UNIX computer).

However, only banzai was mapped in the DNS windows computers are using.

In most cases your system administrator can correct this problem.

Workaround

1. Edit the local \%windir\%/system32/drivers/etc/hosts file.

2. Add the mapping of the missing hostname to the Fully Qualified Domain Name (FQDN).

Example 2

Mapping to be added to the Fully Qualified Domain Name.

172.16.131.190      spot.isr.bmc.com

Client is disconnected due to CORBA::TIMEOUT exception

By default, the GUI Server (GSR) is configured to use a round-trip timeout policy of 1 minute (60000 milliseconds). This value is set using the -RTTimeoutPolicy parameter in the GSR scope in the config.xml file.

The -RTTimeoutPolicy parameter defines the maximum interval between the time a client sends a request to a server until the time the reply is received by the client. Relative round-trip timeouts are useful when the client requires short request-reply intervals.

The GSR, as a client of the GUI (opening Viewpoints and invoking other types of callback requests), does not tolerate slow servers or GUIs, as they affect its performance adversely.

Setting a timeout value for a GUI Server affects only requests that the GUI Server invokes as a CORBA client.

Examples of such requests are:

- updating the GUI with Viewpoint information
- sending results of a callback action, such as Upload Table or Holding an active job
If the GUI, CLI, or the CONTROL-M/Desktop do not return a reply within the timeout interval, a CORBA::TIMEOUT is raised on the server side, communication with the slow client terminates, and a USER_NOT_FOUND exception is received on the client side.

To prevent disconnections from slow clients, set the GSR AddJobsChunkSize system parameter to 100 (the default chunk size is 1000).

This change does not require recycling the GSR.

Alternatively, modify the timeout value in the GSR scope (on the GSR computer) by using the following command:

```
-orbadmin variable modify -scope GSR -value <desired_timeout_milliseconds>
-RTTimeoutPolicy
```

Restart the GSR for those timeout settings to take effect.

--- NOTE ---

BMC recommends decreasing the chunk size instead of increasing the timeout value. Increasing the timeout may decrease the GSR’s performance and memory efficiency since it now tolerates slower clients and will take more time for it to identify "dead" clients that did not disconnect properly.

---

**Analyzing diagnostic data for CONTROL-M/Server**

This section describes some of the more common checks that can be executed after encountering problems using CONTROL-M/Server, prior to contacting BMC Customer Support. Also discussed are basic diagnostic procedures that can be performed so that the resulting log files can indicate to BMC Customer Support upon initial contact what the nature and scope of the problem could be.

**Troubleshooting menu analyzing options**

The following options on the Troubleshooting menu can be used to analyze diagnostic data for CONTROL-M/Server.
Table 65  Troubleshooting Menu options

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Restart New Day Procedure</strong></td>
<td>Starts the New Day procedure again after confirmation.</td>
</tr>
<tr>
<td><strong>Check Kernel Configuration - analyze</strong></td>
<td>[UNIX] Checks whether the current configuration settings of the kernel comply with requirements for CONTROL-M/Server. For more information, see the CONTROL-M/Server and CONTROL-M/Agent Installation Guide. If all parameters are configured correctly, the following message is displayed: Check kernel configuration for &lt;system&gt; terminated successfully. If one or more parameters are not configured correctly, the parameters are listed followed by: Check kernel configuration for &lt;system&gt; terminated unsuccessfully.</td>
</tr>
<tr>
<td><strong>Check directory permissions</strong></td>
<td>Checks the current directory and all sub-directories under it for permissions.</td>
</tr>
<tr>
<td><strong>Reset CONTROL-M Active Environment</strong></td>
<td>Clears all components of the CONTROL-M/Server active environment (Active Jobs file, prerequisite conditions, and so on) and forces CONTROL-M/Server to start a download of the entire Active Jobs file to CONTROL-M/EM. This option is described on page 369.</td>
</tr>
<tr>
<td><strong>Truncate Database Log</strong></td>
<td>[UNIX only] [Sybase only] Truncates the CONTROL-M/Server database log. This option should be used if the Sybase message “Can’t allocate space for &lt;text&gt; in database &lt;name&gt; because the log segment is full” occurs in one of the log files located in directory $CONTROLM_SERVER/proclog. Note: Option 8 only appears for CONTROL-M/Server on UNIX.</td>
</tr>
<tr>
<td><strong>Set Sleep Time</strong></td>
<td>Determines the sleep time for all CONTROL-M/Server processes or for any specific process. For more information, see page 368.</td>
</tr>
<tr>
<td><strong>Force Download</strong></td>
<td>Forces CONTROL-M/Server to start download of the entire Active Jobs file to CONTROL-M/EM.</td>
</tr>
<tr>
<td><strong>Quit</strong></td>
<td>Quits the Troubleshooting menu and returns to the CONTROL-M Main Menu.</td>
</tr>
</tbody>
</table>

Set sleep time

Determines the sleep time for all CONTROL-M/Server processes or for any specific process. The sleep time is the length of time that the process lies dormant before “waking up” to check if any request to perform an action was received. If modified while CONTROL-M/Server is running, the sleep time specified becomes effective immediately.

Prompts similar to the following are displayed:

```
Enter option number --->   [4]: 2
Enter seconds_sleep_time : [30]: 60
Enter PROCESS_NAME [CD,CO,LSL,SL,SU,TR,RT,WD,ALL] : [CD]: ALL```

Specify the desired sleep time (in seconds), and then specify the two-character code for a specific process, or ALL for all CONTROL-M/Server processes.

**Restart New Day procedure**

The New Day procedure is restarted, after confirming that this is the required action. Amongst other actions, the New Day procedure contains instructions for running a number of maintenance and cleanup utilities. For more information about the New Day procedure, see “Customizing the New Day procedure” on page 98.

**Reset CONTROL-M/Server active environment**

**NOTE**

Shut down CONTROL-M/Server before selecting this option.

When selected from the Troubleshooting menu, the Reset CONTROL-M Active Environment option performs the following actions (after confirmation by you):

- The contents of the Active Jobs file are erased.
- All prerequisite conditions, Quantitative resources, and Control resources are deleted.
- The entire Active Jobs file is downloaded to CONTROL-M/EM.

It is also possible to reset the CONTROL-M/Server process sleep times and trace level using the init_prflag utility. This utility performs the following actions:

- The sleep times for all CONTROL-M/Server processes are reset to their initial (installation) values.

The trace level for all CONTROL-M/Server processes is reset to zero.

**Process of elimination**

This section describes some of the more common checks that can be executed by you prior to contacting BMC Customer Support. Some of these checks use a process of elimination to attempt to determine the cause of a problem.
In cases where the cause of issues cannot be remedied relatively simply, also discussed are basic diagnostic procedures that can be performed so that the resulting log files can indicate to BMC Customer Support upon initial contact what the nature and scope of the problem could be.

Below are described some common issues that occur, and the processes of elimination that should be observed before taking diagnostic activity to the next level.

**CONTROL-M/Server, for the first time, fails to communicate with a CONTROL-M/Agent**

**Possibility 1: The CONTROL-M/EM Configuration Agent fails to respond**

Perform the following steps:

1. Run the following command:

   `CTM_diag_comm <agentName>`

2. Examine the report that is generated by this utility:

   - If the computer where the agent resides cannot be reached, check the agent name, or consult your IT department.
   - If the computer where the agent resides can be reached, but the agent itself cannot be reached, then make sure that the value of the Server to Agent parameter, on both CONTROL-M/Server and CONTROL-M/Agent, is the same. If the value of this parameter is the same, then check that the CONTROL-M/Server name exists in the **Permitted server** list in the CONTROL-M/Agent.

**Possibility 2: The status of a job, after being in executing state, is changed to Post Processed after a long delay (15 minutes), although in reality the job has finished execution**

Perform the following steps:

1. On the CONTROL-M/Agent where the job was invoked run the following command

   `ag_ping <serverName>`

2. If the reply indicates a failure, then perform the following steps:

   - Ensure that the value of the Agent to Server parameter is the same on both CONTROL-M/Server and CONTROL-M/Agent.
If the Agent to Server parameter is the same, check that the CONTROL-M/Server is not behind a firewall.

Possibility 3: CONTROL-M/Server has difficulties to start up and in the proclolg sub-directory there are log files which that report *Failed to connect to RT*

Perform the following steps:

1. Use options in the main CONTROL-M/Server menu (ctm_menu) to change the value of the Inter Process Communication Port Number parameter. For more information about ctm_menu, see the *CONTROL-M Administrator Guide*.

2. Re-start CONTROL-M/Server.

Log files: Analyzing

Debug log messages are recorded in either a single log file of unlimited length or a series of cyclical log files, which are stored in the `CONTROLM/EM_home\Log` directory of your local computer.

The environment variable for the logs is `$ECS_LOG_PATH`. The number and length of cyclical log files are determined initialization file parameters for the monitored component. When the last cyclical log file is full, DIAG removes the oldest file and begins a new one.

Log files have a special naming convention that enables you to identify them readily:

- **Non-cyclic log files** (excluding multiple GAS and GSR files):
  
  `prefix_diag.component_hostname.txt`
  
  For example: `gas_diag.ACCT12.txt`

- **Cyclic log files** (excluding multiple GAS and GSR files):
  
  `prefix_diag.component_hostname.date.serial_number.txt`
  
  For example: `gas_diag.ACCT12.20010318.0001.txt`

- **Non-cyclic multiple GAS and GSR files**
  
  `{gas|gsr}_diag.component_hostname.logical_name.txt`

- **Cyclic multiple GAS and GSR files**
  
  `{gas|gsr}_diag.component_hostname.logical_name.date.serial_number.txt`

- If more than one GUI Server or Global Alerts Server exists, the format of the log file for these components contains the name of the server immediately after the hostname. For example: `gsr_log.host1.{GUI_Server_Name}.20040705.#0282.txt`
The log filename is case-sensitive.

Filename component prefixes (prefix) are:
- gas (Global Alerts Server)
- gsr (GUI Server)
- maint (Configuration Agent)
- alertX (Alerts window)
- ecs (CONTROL-M/EM GUI)
- mdesk (CONTROL-M/Desktop)
- tbloader (Loader process)
- vrfy (Verify User process)
- ctl (ctl utility)

The filename date format is yyyyMMdd.

The 4-digit serial number for each file is incremented by 1 for successive files.

Troubleshooting using component logs

By default, all information and error messages displayed by a CONTROL-M/EM Gateway are saved in a special log file.

The gateway log file is stored in the following directories:

- In Microsoft Windows: ControlM-EM\log
- In UNIX: EMHome/log/

The gateway log file name has the following format:

gtw_log.Control-M_name.date.num

GCS_LOG files

Diagnostic activity can be seen in the permanent GCS_LOG file for each process. These log files show the flow of the conditions, their source and destination, when each condition was sent, and all messages regarding condition activities. There are four types of messages:

- **Cond_diag**: Determines the level of diagnostic information for condition transfer activities. Diagnostic information is displayed for conditions received (In) and conditions sent (Out). Transfer confirmation and rejection actions are displayed, including communication problems related to these actions.
■ **db_diag**: Determines the level of diagnostic information for messages related to database activities on GCS recovery tables. Diagnostic information is displayed about condition transfer requests that are inserted or deleted in the database or read from the database for recovery operations.

■ **int_diag**: Determines the level of diagnostic information for messages related to internal GCS actions involving temporary problems and rebound situations. Diagnostic information is displayed about GCS condition handling activities.

■ **msg_diag**: Types of message packets (dsects) that are displayed and written to the GCS_LOG file. Condition transfer requests and messages related to inter-process communication activities are displayed.

You can set the levels of what these messages should report and at what level of detail, by accessing their corresponding system parameters. For more information, see Appendix B, “System parameters.”

### Sample GCS_LOG file and explanation (to move: Analyzing)

**Figure 27  Excerpt from a GCS_LOG File**

```
M< RECEIVE 09:50:07.138: 1109  <msg> OR095007005DABGATEWAY 0009COND_15011104+
C< RECEIVING COND 09:50:07.139: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB
D> INSERT MSG:: 09:50:07.148: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <id> 1
D> INSERT DST 09:50:07.155: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB:: <dst> AAA <id> 1
D> INSERT DST 09:50:07.157: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB:: <dst> AAB <id> 1
I> SEND COND ATTEMPT  09:50:07.213: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <dst> AAA <tryno> 0
C> SENDING COND 09:50:07.213: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <dst> AAA <tryno> 1:: <msg> CR08/18/387DABGCSERV 0009COND_15011104+
I< PENDING ACKNOWLEDGE 09:50:07.213: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <dst> AAA <tryno> 1
I> SEND COND ATTEMPT  09:50:07.213: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <dst> AAB <tryno> 0
C> SENDING COND 09:50:07.213: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <dst> AAB <tryno> 1:: <msg> CR08/18/390DABGCSERV 0009COND_15011104+
I< PENDING ACKNOWLEDGE 09:50:07.214: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> DAB <dst> AAB <tryno> 1
M< RECEIVE 09:50:07.501: 1109  <msg> OR095007005AAGATEWAY 0009COND_15011104+
C< RECEIVING COND 09:50:07.501: 1109  <cnd> COND_1501 <odat> 1104 <op> + <dc> AAA
```
The global conditions traffic trace log can be configured to include the following types of information:

- Condition name, originating datacenter, destination datacenter, odate, add or delete indicator, a timestamp, and other diagnostic data (see Table 67 on page 375).
- Conditions arriving from gateways
- Conditions sent to gateways
- Updates to Global Conditions Server recovery tables (GCS_DSTS and GCS_MSGS)
- Acknowledgements sent to originating gateways
- Acknowledgements and rejections received from destination data centers.
- Loading conditions from GCS recovery tables.
- Communication failures and recovery actions taken.
- Conditions that were treated as “rebound” updates.
- Message contents received from gateways.
- Message contents sent to gateways

The tracing message format facilitates problem tracking. The format supports scripting and automation of research activities.

The GCS_LOG record includes the following fields:

The Action code indicates the type of action associated with the problem. Each log record includes one of the following action codes:
The **Description** describes the action that occurred, in a text string.

The **Timestamp** contains the date and time of the log record in **yyyymmddhhmmssms** format.

The **Data Flag** indicates the type of information that follows the flag, and contains one or more of the following data flags.

### Table 66: Action codes for the GCS_LOG file

<table>
<thead>
<tr>
<th>Action code</th>
<th>Explanation of the Action code</th>
</tr>
</thead>
<tbody>
<tr>
<td>D&gt;</td>
<td>Database writing (insertion or modification or deletion) information</td>
</tr>
<tr>
<td>D&lt;</td>
<td>Database reading (recovery) information</td>
</tr>
<tr>
<td>C&gt;</td>
<td>Condition transfer, problem, and acknowledgement data sent</td>
</tr>
<tr>
<td>C&lt;</td>
<td>Condition transfer, problem, and acknowledgement data received</td>
</tr>
<tr>
<td>I&gt;</td>
<td>Status messages based on condition handling progress in GCS</td>
</tr>
<tr>
<td>I&lt;</td>
<td>Actions due to communication problems or conflict handling policies</td>
</tr>
<tr>
<td>M&gt;</td>
<td>Content of messages sent to gateways by GCS</td>
</tr>
<tr>
<td>M&lt;</td>
<td>Content of messages received for condition transfer requests</td>
</tr>
</tbody>
</table>

### Table 67: Data flags for the GCS_LOG file

<table>
<thead>
<tr>
<th>Data Flag</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>&lt;cnd&gt;</td>
<td>Condition name</td>
</tr>
<tr>
<td>&lt;odat&gt;</td>
<td>Condition odate</td>
</tr>
<tr>
<td>&lt;op&gt;</td>
<td>Condition action (add or delete)</td>
</tr>
<tr>
<td>&lt;dc&gt;</td>
<td>Condition origin</td>
</tr>
<tr>
<td>&lt;dst&gt;</td>
<td>Condition destination</td>
</tr>
<tr>
<td>&lt;id&gt;</td>
<td>GCS ID assigned to condition transfer request</td>
</tr>
<tr>
<td>&lt;siid&gt;</td>
<td>Request message service ID transferred by gateway</td>
</tr>
<tr>
<td>&lt;tryno&gt;</td>
<td>Number of attempts to send a condition to its destination</td>
</tr>
<tr>
<td>&lt;comchkno&gt;</td>
<td>Number of times communication status was checked by GCS for a specific condition and destination</td>
</tr>
</tbody>
</table>

The **Data file** is the information of the type indicated by the Data Flag that precedes it.

---

### Working with Exception Alerts

The Exception Alerts window displays information about each alert, such as the alert ID, severity of the alert, the message that was generated by the alert, and more. Alerts appear with a status of either Handled or Unhandled.
Working with Exception Alerts

NOTE
The maximum number of alerts that are displayed is determined by the MaxXAlerts2Send2Client system parameter. If the number of alerts in the database is greater than the number of alerts determined in the system parameter, a message is displayed in the status bar. For more information, see “Exception handling parameters” on page 447.

To display alerts

1. In the CONTROL-M Configuration Manager, choose Tools -> Exception Alerts. The Exception Alerts window opens.

![Figure 28 Exception Alerts window](image)

2. Do the following as needed:

   - To filter the alerts displayed in the Exception Alerts window, choose View -> Alerts Filter and the criteria by which you want to filter.

   - To group the alerts in a hierarchical tree, choose View -> Alerts Group. Drag the header column by which you want to group the alerts into the grouping area. Repeat this procedure to group by additional columns.

   - To refresh the display, choose View -> Refresh. To set an interval at which the display will automatically refresh, choose Tools -> Options and enter a value (in seconds) for the refresh interval.

   - To preview the message of an alert, choose View -> Preview Message.

   - To export the alerts to a file, choose File -> Export and enter a file name and file type.
■ To delete old alerts currently displayed in the Exception Alerts window, choose **Tools -> Remove Old Alerts** and enter a value.

---

**NOTE**

Normally, alerts are removed based on the value set in the XAlertsMaxAge system parameter. The Remove Old Alerts window does not update the value in the XAlertsMaxAge system parameter. For more information, see “Exception handling parameters” on page 447.

---

■ To view the details of a specific alert, select the alert and then choose **X-Alert -> Properties**. The Alert Properties window appears showing additional information for the specific alert.

**To indicate that an alert has been handled**

In the Alert Properties window, choose the appropriate status as follows:

■ To indicate that you have handled the alert, choose **Handle**.
■ To indicate that you have not yet handled the alert, choose **Not-Handled**.

To add a note to an alert, type the note in the **Note** field in the Properties window of the alert.
Appendixes

This part presents the following topics:

Appendix A
   Configuring CORBA components ........................................... 381

Appendix B
   System parameters ............................................................... 403

Appendix C
   Exits ................................................................................... 523

Appendix D
   SNMP interface ................................................................. 533

Appendix E
   Mass conversion of agents and remote hosts .......................... 537
Configuring CORBA components

This appendix presents the following topics:

Concepts .......................................................... 381
  CORBA overview .................................................. 382
  Naming Service .................................................. 383
  What is an Interoperable Object Reference (IOR)? ................. 386
  Advanced communication policies .................................. 389
  Assigning ports when using a firewall .......................... 391
  XML configuration file scopes .................................. 391
Recommended task summary ...................................... 392
Configuring CORBA components .................................. 392
  Specifying domain settings ..................................... 393
  Specifying Naming Service settings ............................ 396
  Assigning ports ................................................... 398
  Specifying Advanced parameters ................................ 399

Concepts

Figure 29 highlights the basic recommended workflow for connecting CONTROL-M/Enterprise Manager components. This overview section explains concepts that are related to the workflow.

For specific tasks that correspond to each phase of the workflow, see Table 69 on page 392. Following the table, the remainder of the chapter provides step-by-step instructions for completing the tasks.
CORBA overview

Many CONTROL-M/EM server and client components communicate using the CORBA (Common Object Request Broker Architecture) communication protocol created by the Object Management Group to enable application components that are distributed across a network to communicate with one another.

The following CONTROL-M/EM components use a specific CORBA implementation called TAO (The ACE ORB):

- CONTROL-M/EM server components
  - GUI server
  - GAS server
  - CONTROL-M/Forecast server
  - BMC Batch Impact Manager server
  - CMS server (Configuration manager server)
CONTROL-M/EM client components

- CONTROL-M/EM GUI
- CONTROL-M/Desktop
- CONTROL-M Reporting facility
- CONTROL-M Configuration Manager
- cli utility
- Sweep command line utility
- XML utilities

CONTROL-M/EM uses a single XML CORBA configuration file, called `config.xml`, that defines CORBA configuration data for all these components. During installation, this file is configured with default values for the components.

There might, however, be situations where the administrator will want to set or modify CORBA configurations. The following are the more common situations:

- Troubleshooting communication problems
- Setting up a Firewall
- Setting up VPN client
- Implementing SSL

To modify CORBA configuration, the administrator can choose between the following methods, both of which edit the `config.xml` file:

- interactively, using the orbconfigure utility, described in this chapter
- in batch, using orbadmin utility. For details, see the CONTROL-M Utility Guide.

### Naming Service

The Naming Service runs in background mode based on parameter values stored in the XML CORBA configuration file.

Installing Naming Service on Windows requires adding parameters to the registry. Without these parameters, the Naming Service cannot start. These parameters are added automatically at the time of installation based on values in the domain configuration file.
These parameters determine:

- Repository path for Naming Service files (run in persistence mode)
- Listening network interface (host, IP address, or all available adapters)
- Listening port
- SSL communication (enabled or disabled)
- Internal TAO configuration file (required for SSL)

If the configuration is changed, run the following commands to recycle the Naming Service and update the information in the registry:

```
orbadm ns stop
orbadm ns start
```

**NOTE**
On Windows the Naming Service can be stopped only from the Services window. The `orbadm ns stop` command cannot stop the Naming Service, because the CONTROL-M Configuration Server depends on it.

**Description**

The CORBA Naming Service provides a tree-like directory for remote objects much like a file system provides a directory structure for files.

A name-to-object association is called a *name binding*. A name binding is always defined relative to a *naming context*. A naming context is an object that contains a set of name bindings in which each name is unique. Different names can be bound to an object in the same or different contexts at the same time.

To *resolve a name* is to determine the object associated with the name in a given context. To *bind a name* is to create a name binding in a given context. A name is always resolved relative to a context – there are no absolute names.

Because a context is like any other object, it can also be bound to a name in a naming context. Binding contexts in other contexts creates a *naming graph* – a directed graph with nodes and labeled edges where the nodes are contexts. A naming graph allows complex names to reference an object. Given a context in a naming graph, a sequence of names can reference an object. This sequence of names (called a *compound name*) defines a path in the naming graph to navigate the resolution process.

The tree starts with a root node, it may have intermediate nodes, and it ends with the actual objects stored by name at the leaves of the tree. The fully qualified name of an object is the ordered list of its parent nodes, starting with the root node and ending with the name of the object.

*Figure 30* shows how three objects might be stored in a Naming Service directory. In this illustration, the full name of the `UserManager` is `BMC Software, ECS, palace, GAS, UserManager`.  

384  CONTROL-M Administrator Guide
Figure 30  Naming Service directory illustration

BMC Software: naming context
ECS: naming context
    palace: naming context
GAS: naming context

Connecting CORBA clients to CORBA servers

Each CORBA server resolves the Naming Service to register its objects in the Naming Service repository. If the Naming Service is not found, the server exits. A server’s objects are registered in a specific Naming Service under the following context (see “What is an Interoperable Object Reference (IOR)?” on page 386):

BMC Software
ECS
    hostname | EM_NAMING_CONTEXT
    GSR | GAS
        ObjectNameA IOR
        ObjectNameB IOR
        ObjectNameC IOR

Each CORBA client resolves the Naming Service to get the server’s object references so it can connect to the server directly. If the Naming Service is not found, an error message is displayed (for example, the list of server names in the Login dialog box is disabled to indicate no server contexts could be found).

CORBA clients search for the server name under the hierarchy described above and get the IORs. Applications that refer to an object can invoke calls to that object.

NOTE
CORBA applications (both clients and servers) try to resolve the Naming Service according to the value of the –ORBInitRef parameter that was previously specified in the config.xml file and passed to the application during initialization.

Repository

The Naming Service saves the naming structure (including contexts and the objects hierarchy) in readable data files under the $ECS_HOME/var directory.
What is an Interoperable Object Reference (IOR)?

An IOR is a reference to a CORBA object. It is the equivalent of a distributed, network smart, location transparent, platform-independent pointer. An IOR has three main components: the repository ID, the endpoint information, and the object key.

CORBA uses IORs as the universal means of identifying an object. Object references are opaque to the client-side application code and completely encapsulate everything that is necessary to send requests, including the transport and protocol to be used.

Repository ID

The repository ID is a string that identifies the most derived type of the IOR at the time the IOR was created. The repository ID enables you to locate a detailed description of the interface in the Interface Repository (if the ORB provides one). The ORB can also use the repository ID to implement type-safe down-casts.
What is an Interoperable Object Reference (IOR)?

**Endpoint information**

This field contains the information required by the ORB to establish a physical connection to the server implementing the object. The endpoint information specifies which protocol to use and contains physical addressing information appropriate for a particular transport.

--- **EXAMPLE**

For the IIOP, the endpoint information contains an Internet domain name or IP address and a TCP port number.

The endpoint information field may contain the address and port number of the server that implements the object. However, in most cases, it contains the address of an implementation repository that can be consulted to locate the correct server. This extra level of reference permits server processes to migrate from computer to computer without breaking existing references held by clients.

CORBA allows several different protocols and transports to be embedded in the reference so that a single reference can support more than one protocol. The ORB automatically chooses the most appropriate protocol.

**Object key**

The object key contains proprietary information. All ORBs allow the server to embed an application-specific object identifier inside the object key when the server creates the reference. This object identifier is used by the server-side ORB and object adapter to identify the target object in the server for each request it receives.

The client-side sends the object key as a string of binary data with every request it makes. Therefore, it does not matter that the reference data is in a proprietary format. It is never looked at by any ORB except the ORB hosting the target object (which is the same ORB that created the object key).

The combination of endpoint information and object key can appear multiple times in an IOR. Multiple endpoint-key pairs, known as multicomponent profiles, permit an IOR to efficiently support more than one protocol and transport that share information. An IOR can also contain multiple profiles, each containing separate protocol and transport information. The ORB run time dynamically selects which protocol to use depending on what is supported by both client and server.

The essential ingredients for successful request dispatch are encapsulated in a reference. The repository ID provides type checking, the endpoint information is used by the client-side ORB to identify the correct target address space, and the object key is used by the server-side to identify the target object inside the address space.
What is an Interoperable Object Reference (IOR)?

“Stringified” IOR

A typical stringified IOR is illustrated here:

IOR:01000001400000049444c3a557365724d616e6167656e6a6f6e616d65723a312e300001000000000000
0680000001010200600000766572656400e6cc2300000114010604e5354416e639300e
d6c7000000010000000010000000010000000100000002000000020000000000000000000000360a0a54414f000100000140000000360a0a00100010000000000010109000000

You can obtain an object IOR by following the procedure described under “How to verify that a CORBA server is listening on port X” on page 357.

Decoding an IOR

The catior utility accesses a stringified IOR, extracts and decodes readable information from it, and prints the data to the standard output device.

Usage: **catior -f filename**

--- **EXAMPLE** ---

*catior* dumps the following output for the Stringified IOR shown above:

> catior -f ior4example
reading the file ior4example
The Byte Order: Little Endian
The Type Id: "IDL:UserManager:1.0"
Number of Profiles in IOR: 1
Profile number: 1
IIOP Version: 1.2
Host Name: vered
Port Number: 52454
Object Key len: 35
Object Key as hex:
14 01 0f 00 4e 53 54 41 6e 63 93 00 0e d6 c7 00
00 00 01 00 00 01 00 00 00 01 00 00 00 01 00 00 00 01 00 00 02
The Object Key as string: ....NSTAnc.........................
The component <1> ID is 0 (TAG_ORB_TYPE)
  ORB Type: 1413566208 (TAO)
The component <2> ID is 1 (TAG_CODE_SETS)
  Component Length: 20
  The Component Byte Order: Little Endian
  Native CodeSet for char: Hex - 1000100 Description - Unknown CodeSet
  Number of CCS for char: 0
  Native CodeSet for wchar: Hex - 9010100 Description - Unknown CodeSet
  Number of CCS for wchar: 0
Host specification

CORBA Servers listen for clients requests on a specific interface specified by endpoint -ORBListenEndpoints.

Internet Inter-ORB Protocol (IIOP) addresses

IIOP addresses include a hostname (or an IP address) and a TCP port the server should listen on. The hostname is used to select the network interface on which the endpoint is set up. It is not used to set the hostname that goes into the generated IOR. This is especially useful if the endpoint is not setup on the default network interface.

- For multiple network cards, you can set a specific IP address to listen on, instead of using the default IP address.
- To create an endpoint on each network interface, omit the address from the endpoint specification. The selected port is the same for all endpoints. A static port or port range can also be specified for this type of endpoint. Network interface detection only works on platforms that support this feature. If network interface detection is not supported, the default network interface is selected.

In the Domain Settings panel of the Domain Configuration window, select the correct address policy from the drop down list next to Listening host/address.

Advanced communication policies

This section describes the following topics:

Bidirectional IIOP

Relative round-trip timeout policy

Bidirectional IIOP

CORBA 2.3 added GIOP 1.2 and IIOP 1.2 to enable bidirectional communication. This allows client and server to reverse roles without opening a separate connection that may be blocked by a firewall. Therefore, bidirectional communication is important for communication through firewalls.

For example, The Callback mechanism requires a server to also act as a client. GIOP 1.2 allows the server to initiate requests on the connection that was opened by the client. This means that the server does not have to open a separate connection for a callback, only to find itself blocked by a firewall.
Advanced communication policies

**NOTE**
Bidirectional communication is enabled only if both client and server agree to use it.

This allows administrators to disable bidirectional communication over insecure links to prevent clients from masquerading as call-back objects. If bidirectional communication is disabled, GIOP 1.2 uses a separate connection for callbacks.

Clients using bidirectional communication do not listen on a separate port for incoming connections. Therefore, there is no need to assign ports for them in a firewall environment. However, all ports must be open for outgoing connections on the client side.

**NOTE**
A CORBA server using a bidirectional policy can establish a connection with CORBA clients that do not use a bidirectional policy. However, the server will use a separate connection for callbacks.

### Relative round-trip timeout policy

TAO 1.1a supports the Relative Round-trip Timeout policy defined in the CORBA Messaging specification (OMG TC Document orbos/98-05-05). This policy allows you to specify the maximum interval between the time a client sends a request to a server until the time the reply is received by the client. Relative round-trip timeouts are useful when the client requires short request-reply intervals.

You can set a relative round-trip timeout at the client ORB level by adding a parameter to the configuration file in the relevant application scope.

**EXAMPLE**
To set a timeout of 10,000 milliseconds for the GUI application, use the command:
```
orbadmin variable modify -scope GUI -value 10000 -RTTimeoutPolicy
```
and restart the GUI.

All requests made using these settings will timeout if a reply is not received within 10,000 milliseconds. When a timeout occurs, the ORB will raise a `CORBA::TIMEOUT` system exception. If a reply eventually arrives after the timeout period has expired, it will be discarded by the client ORB.

If you set a timeout value for a CORBA Server, it will have an effect only if that CORBA Server is also a CORBA Client.
Therefore, setting a timeout value for a GUI Server affects only requests the GUI Server invokes as a CORBA client. Examples of such requests are:

- updating the GUI with Viewpoint information.
- sending results of a callback action, such as Upload Table or Holding an active job.

If the GUI or the Desktop does not return a reply within the timeout interval, a `CORBA::TIMEOUT` is raised on the server side, communication with the slow client (GUI, CONTROL-M/Desktop, or CLI) terminates, and a USER_NOT_FOUND exception is received on the client side.

Setting a timeout value for GAS has no effect because the GAS does not function as a CORBA client using callback objects.

### Assigning ports when using a firewall

Use the **Ports** panel of the Domain Configuration window to set listening ports (random, static, range) for all EM applications.

When working with firewalls, assign a static port or a range of ports to each CONTROL-M/EM application instead of using the default setting: random ports.

BMC Software recommends setting a range of ports for client applications such as the CONTROL-M/EM GUI, Desktop and CLI, so that more than one session can run simultaneously on the same machine.

The assigned ports should be open for incoming connections. *All* ports should be open for outgoing connections on the client’s side. However, if both sides are using bidirectional IIOP, there is no need to open all ports for outgoing connections on the server’s side as well.

### XML configuration file scopes

The domain XML configuration file is divided into “scopes.” A scope designates a component, service, or utility that uses CORBA communication. Each scope contains name-value pairs relevant to the component, service, or utility designated by that scope.

The scope named “default” contains parameter settings that apply to all scopes (except the Naming Service scope, named `ns`) unless overridden by other scopes.
Recommended task summary

Table 68  Scopes in the XML configuration file

<table>
<thead>
<tr>
<th>Scope name</th>
<th>Component or description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BIM</td>
<td>BMC Batch Impact Manager</td>
</tr>
<tr>
<td>CLI</td>
<td>Command Line Interface utility cli.exe</td>
</tr>
<tr>
<td>CCM</td>
<td>CONTROL-M Configuration Manager GUI</td>
</tr>
<tr>
<td>CMS</td>
<td>CONTROL-M Configuration Server</td>
</tr>
<tr>
<td>default</td>
<td>Defaults for all components/services/utilities except ns</td>
</tr>
<tr>
<td>Desktop</td>
<td>CONTROL-M/Desktop emdesktop.exe</td>
</tr>
<tr>
<td>Forecast</td>
<td>CONTROL-M/Forecast server</td>
</tr>
<tr>
<td>GAS</td>
<td>Global Alerts Server ecs_gasrv</td>
</tr>
<tr>
<td>GSR</td>
<td>GUI Server ecs_guisrv</td>
</tr>
<tr>
<td>GUI</td>
<td>Graphic User Interface emgui.exe</td>
</tr>
<tr>
<td>ns</td>
<td>CORBA Naming Service</td>
</tr>
<tr>
<td>Report</td>
<td>Reporting Facility</td>
</tr>
<tr>
<td>RSI</td>
<td>remote server invocation</td>
</tr>
<tr>
<td>Sweep</td>
<td>Sweep utility</td>
</tr>
<tr>
<td>XmlUtil</td>
<td>deftable, defjob, defcal, copydefcal, copydefjob, deldefjob, duplicatedefjob, updatedef, exportdefjob, exportdeftable, exportdefcal.</td>
</tr>
</tbody>
</table>

Recommended task summary

Table 69 lists specific tasks related to each phase of the workflow (Figure 29 on page 382). Subsequent sections provide step-by-step instructions.

Table 69  Task summary: connecting components

<table>
<thead>
<tr>
<th>Workflow</th>
<th>Specific tasks</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configure CORBA components</td>
<td>Specifying domain settings</td>
<td>393</td>
</tr>
<tr>
<td></td>
<td>Specifying Naming Service settings</td>
<td>396</td>
</tr>
<tr>
<td></td>
<td>Assigning ports</td>
<td>398</td>
</tr>
<tr>
<td></td>
<td>Specifying Advanced parameters</td>
<td>399</td>
</tr>
</tbody>
</table>

Configuring CORBA components

This section describes how to use the Domain Configuration (orbconfig) wizard to configure CONTROL-M/EM CORBA components.

NOTE

Configuration changes made to running processes do not take effect until you recycle the component.
Specifying domain settings

The orbconfigure wizard enables you to specify “well-known” addresses for CORBA components. Use the following steps to do this:

1. Start the Domain Configuration (orbconfigure) wizard as follows:

   A. Ensure you have JRE version 1.4.1 or higher installed on your computer.

   B. Set JAVA_HOME to JRE installation, for example: D:\JavaSoft\jre

   C. On UNIX computers only, enter: `setenv DISPLAY terminal_IP_address:0.0`

   D. Start the Domain Configuration (orbconfigure) wizard with one of the following commands. This displays the Domain Settings panel of the wizard.

      - [UNIX] orbconfigure
      - [Windows] orbconfigure.vbs

---

**WARNING**

The orbconfigure wizard and oradmin utility do not lock records while changing the configuration file. Therefore, running multiple sessions of orbconfigure or oradmin at the same time can corrupt the local configuration.

---

**NOTE**

`java_home` refers to the directory where the Java 2 Runtime Environment (JRE) was installed. The Java 2 SDK (also called the JDK) contains the JRE, but at a different level in the file hierarchy. For example, if the Java 2 SDK or JRE was installed in `/home/user1`, `java_home` would be:

- `/home/user1/jre1.4.x` [JRE]
- `/home/user1/jdk1.4.x/jre` [SDK]
2 Specify the domain name as follows:

- To configure an existing domain, choose the domain name in the Domain Name field drop down list.

- To specify a new domain

  1. Choose <New...> in the Domain Name field drop down list.

  2. In the New Domain dialog box, specify the new domain name click OK.

  3. If an override message prompt is displayed, it means you specified an existing domain. To override the previous settings for that domain with your newly specified settings, click Yes. Otherwise, click No.

3 In the Listening Address field, select one of the following hostname addresses where listening should take place:

- **All** – All CORBA servers listen on all available network interfaces. This policy is the default and is recommended for computers with multiple network adapters.

- **IP address** – Select the IP address from the drop down list.

- **Short hostname** – The value is displayed in a “read-only” text box.

- **Other** – Specify the host/address in the adjacent text box or leave it empty. If you leave it empty, this option is similar to All.
4 In the Published address field, select the appropriate object address type, and where necessary, specify the appropriate value in the accompanying field:

- **Default** (hostname)
- **IP address** – If you select this value, select the IP address from the accompanying drop down list.
- **Short hostname** – The value is displayed in a “read only” textbox.
- **Fully qualified hostname** – Specify the fully qualified host name in the text box.
- **Virtual hostname** – Specify the virtual host name in the adjacent text box.
- **localhost**
- **127.0.0.1**

CORBA clients obtain IORs to invoke requests on object references. The IOR contains endpoint information, that is, the host and port number at which the server listens for requests. The host can be encoded either in dotted-decimal notation (such as 234.234.234.234) or as a host name (such as yoursite.com).

By default, the hostname published in the IOR is the default hostname returned by system call `gethostbyaddr()`.

The hostname encoded in the server’s IOR must be accessible for clients:

- If clients can reach the server only by an IP address, the server IORs must use that IP address instead of the default hostname.
- If clients can reach the server only by an FQDN (Fully Qualified Domain Name), the server IORs must use that FQDN instead of the default hostname.
- If the hostname IP address changes dynamically, server IORs must use a virtual hostname and a DNS to translate the virtual hostname into a valid IP address.

5 To enable one port to be used for communication in both directions, select the Bidirectional IIOP (Internet Inter-ORB Protocol) check box.

---

**NOTE**

If you use bidirectional IIOP, the client or server to which you connect must also use this policy.

---

6 If you are using Secure Sockets Layer (SSL) protocol instead of TCP/IP, select the SSL check box. For information about SSL, see the *CONTROL-M SSL Guide*.

7 To use an internal TAO configuration file to change the default behavior of TAO:
Specifying Naming Service settings

A Select the **Use TAO internal configuration file** check box.

B In the following field, enter, or browse to and select, the full path and name of the (client-server) **svc.conf** file. The default configuration file is called **client_server.conf** and is in the $HOME/etc directory.

8 Either click **Next** to fill in the parameters in the next panel, or keep clicking **Next** until you arrive at the Summary panel and then click **Finish**.

**Specifying Naming Service settings**

1 If the Domain Configuration (orbconfigure) wizard is not already displayed, display it by performing step 1 on page 393.

2 Click next until the Naming Service panel is displayed.

**Figure 32 Naming Service panel—Domain Configuration (orbconfigure) wizard**

3 In the Host field, specify the name or IP address of the computer running the CORBA Naming Service.

4 In the Port field, specify the listening port (digits only) of the Naming Service.

5 To check if communication with the CORBA Naming Service is enabled, click **Test**.

6 To display and possibly modify in which file the local Naming Service settings are saved, click **Show local settings**.
The Repository files path is the directory in which the Naming Service saves the contexts and objects registered in it (to provide consistency between Naming Service runs).

- To save settings in repository files, click Repository files path, you and specify (or browse to and choose) an existing Repository file directory. The default path is $HOME/var.

- To save the settings in TAO internal configuration files, choose Use TAO internal configuration file, you must specify (or browse to and choose) the configuration file to be used (for example, if you are using SSL).

7 Either click Next to fill in the parameters in the next panel, or keep clicking Next until you arrive at the Summary panel.

8 When you display the Summary panel (after the last step or after filling in parameters in other panels), you must choose whether to install or remove the Naming Service as a Windows service. (If the naming service is already installed on your computer, the Install as Windows service check box is selected. Otherwise, it will be blank.)

- To remove the Naming Service, clear the check box
- To install the Naming Service, select the check box.

9 Click Finish.
Assigning ports

The Ports panel is often used for assigning ports when the applications are behind firewalls.

**NOTE**
You do not need to assign ports across firewalls for client applications (CONTROL-M/EM GUI, CONTROL-M/Desktop, cli utility) if you are using bidirectional IIOP. For more information see “Bidirectional IIOP” on page 389.

1. If the Domain Configuration (orbconfigure) wizard is not already displayed, display it by performing step 1 on page 393.

2. Click next until the Ports panel is displayed.

Figure 34 Ports panel—Domain Configuration (orbconfigure) wizard

The Ports panel enables you to specify port numbers for the following applications.
Specifying Advanced parameters

To implement advanced policies, use the Advanced panel which you access from the Summary panel of the orbconfigure wizard.

1 If the Domain Configuration (orbconfigure) wizard is not already displayed, display it by performing step 1 on page 393.

2 Click Next until the Summary panel is displayed. It lists the current Domain, Naming Service, and Listening Ports settings.

3 For each component for which you are assigning a port, select one of the following values, and where needed, specify required additional information.

- **Random** – This is the default value and is recommended if the component is not behind a firewall. The operating system selects a free port automatically.
- **Static** – This value is suitable if there is never more than one instance of the component running at the same time.
- **Range** – Recommended value for components behind a firewall. Two text boxes are displayed. Specify the lowest and highest ports in these text boxes.

4 Click Next to display the Summary panel, and then click Finish.

**NOTE**

Check that components were not active when you assigned their ports. If components were active, stop and restart the components for changes to take effect.
3 Click Advanced to display the Advanced settings panel. This panel contains the current CORBA domain configuration values in tree format.
You can perform the following actions in the **Advanced settings** panel:

- Add a **New** scope to the configuration file.
- Add a **New** parameter and its value to an existing scope node.
- **Edit** an existing scope in the configuration file.
- **Edit** an existing parameter and its value in a scope node.
- **Delete** an existing scope from the configuration file.
- **Delete** an existing parameter from a scope node.

---

**NOTE**

Right-click the relevant node in the CORBA configuration tree to display the pop-up menu. Click the **New**, **Edit**, or **Delete** option to display the appropriate dialog box. Unavailable options are dimmed (grayed out).

---

4 When you are done making the Advanced setting changes, press **OK** in the Advanced settings panel.

5 To save the current domain configuration values in the CORBA configuration file, click **Finish** in the Domain Configuration wizard.
System parameters

This section presents the following topics:

Concepts ................................................................. 403
  Parameter modification ........................................ 404
  Component refresh .............................................. 404
Tasks ........................................................................ 404
  Modifying CONTROL-M/EM system parameters .......... 405
  Modifying CONTROL-M/Server system parameters ....... 406
  Modifying CONTROL-M/Agent system parameters ...... 409
  Modifying CONTROL-M for z/OS system parameters ... 409
  Refreshing CONTROL-M/EM components .................. 410
  Refreshing CONTROL-M/Server components .............. 411
  Refreshing CONTROL-M/Agent components ............... 412
System parameter reference ...................................... 412
  CONTROL-M/EM parameters ..................................... 413
  CONTROL-M/Server parameters ................................. 453
  CONTROL-M/Agent parameters ................................. 505

Concepts

Customization of CONTROL-M components is largely performed by modifying component system parameter values. You can choose whether to accept provided default component system parameter values or modify them at or after installation.

When you modify system parameters, you must be concerned with two issues:

- How do you modify the parameter? For more information, see Parameter modification.
- How is the affected component refreshed following parameter modification? For more information, see Component refresh.
Parameter modification

How you modify system parameters is a function of several factors:

- product (CONTROL-M/EM, CONTROL-M/Server, CONTROL-M/Agent) and version
- parameter type (for example, Communication parameter, database parameter) and location (for example, in the config.dat file)

Parameters can be modified by using the Configuration Manager, editing a file, or running a utility (frequently, an interactive utility).

Component refresh

Before a modified parameter value can take effect, the component that uses the value needs to be refreshed.

Each system parameter has one of the following refresh types:

- **Automatic**—The component is automatically refreshed. In general, an Automatic parameter is called by a utility, which accesses the current value each time it runs.

- **Recycle**—You need to recycle (stop and restart) the component (for example, CONTROL-M/Server) for the change to take effect.

- **Manual**—You need to perform an action that refreshes the parameter value (with no need for recycling the component).

Tasks

This section describes the following topics:

- Modifying CONTROL-M/EM system parameters
- Modifying CONTROL-M/Server system parameters
- Modifying CONTROL-M/Agent system parameters
- Modifying CONTROL-M for z/OS system parameters
- Refreshing CONTROL-M/EM components
Refresh the CONTROL-M/Server components

Refresh the CONTROL-M/Agent components

Modifying CONTROL-M/EM system parameters

**NOTE**
This procedure applies to all CONTROL-M/EM system parameters, except certain GCS and Gateway parameters that appear in the default.rsc file. For instructions on modifying parameters in the default.rsc file, see “Editing the Defaults.rsc file” on page 405.

1. In the CONTROL-M Configuration Manager, choose Tools => System Parameters => CONTROL-M/EM System Parameters.

   The CONTROL-M/EM System Parameters window displays the CONTROL-M/EM system parameters and values.

   Note the following points about the columns in the display:
   - An * in the Component column indicates that the system parameter affects all types of components.
   - The Host Name column indicates the host name of the affected component.
   - The default value is displayed; you can request to restore the default value.
   - The refresh type is displayed. This lets you know if you need to perform a manual refresh or recycle (or if the component is automatically refreshed).

2. To change a system parameter
   - Double click the parameter.
   - Change the value.
   - Click Save (or Restore Default).

**Editing the Defaults.rsc file**

Gateway parameters and certain GCS parameters reside in the Defaults.rsc file. To modify these parameters, you must edit the file (you cannot use the CONTROL-M Configuration Manager).
For example, by editing the appropriate parameters in this file, you can configure maximum communication wait time between Gateway and other components, handle multiple gateway instances for the same CONTROL-M iteration and configure speed and efficiency of downloads (setting memory buffer).

The location of the Defaults.rsc file is:

- On UNIX: `home_directory/site/resource/Defaults.rsc`
- On Windows: `home_directory\Gtwgcs\appl\site\resource\Defaults.rsc`

---

**Modifying CONTROL-M/Server system parameters**

The method used to update CONTROL-M/Server parameters depends on the type of parameter. Use one of the methods described in the following topics:

- Using the Main menu
- Editing the config.dat file
- Editing the cshrc file
- Running the regedit utility

**Using the Main menu**

The CONTROL-M Main Menu displays a number of nested submenus that can be used for updating a great number of CONTROL-M parameters.

1. Log on to the CONTROL-M/Server computer as the CONTROL-M/Server owner.
2. Enter the `ctm_menu` command to display the CONTROL-M Main Menu.

**Figure 37   CONTROL-M Main Menu**

```
CONTROL-M Main Menu
------------------------
Select one of the following menus:
  1 - CONTROL-M Manager
  2 - Database Creation
  3 - Database Maintenance
  4 - Database Mirroring
  5 - Security Authorization
  6 - Parameter Customization
  7 - Node Group
```
3 In the CONTROL-M Main Menu, enter the number of appropriate submenu.

4 Continue entering appropriate menu option numbers until the interactive display lets you fill in appropriate values.

The following is a list of menu sequences appropriate for specific types of parameters.

**System parameters**

CONTROL-M Main Menu => Parameter Customization => System Parameters and Shout Destination Tables => System Parameters

Alternatively, enter the ctmsys command: CONTROL-M System Maintenance Utility Main Menu => System Parameters

**Communication parameters**

CONTROL-M Main Menu => Parameter Customization => (one of the following):

- Basic Communication and Operational Parameters
- Advanced Communication and Operational Parameters

**Operational parameters**

CONTROL-M Main Menu => Parameter Customization => (one of the following):

- Basic Communication and Operational Parameters
- Advanced Communication and Operational Parameters

**Agent communication parameters**

CONTROL-M Main Menu => Parameter Customization => Parameters for Communicating with Agent Platforms

**Database parameters**

CONTROL-M Main Menu => Database Creation
Mirroring parameters

CONTROL-M Main Menu => Database Mirroring

Editing the config.dat file

This file is located in the following location:

- For UNIX: `controlmOwner/ctm_server/data/config.dat`
- For Windows: `controlmOwner\ctm_server\data\config.dat`

You can modify the following types of parameters in this file:

- Performance parameter
- Configuration parameters
- Watchdog process parameters
- Heartbeat Monitor parameters
- User Exit parameters

**NOTE**

There are parameters listed under “CONTROL-M/Server parameters” on page 453 (but which do not appear in the shipped `config.dat`) for which you can change the value by adding the parameter—set to the value that you need—to `config.dat`. For such parameters, the How/where to set row includes a “See ‘Editing the config.dat file’” link.

Editing the cshrc file

This file is located in the following location:

- For UNIX: `controlmOwner/.cshrc`
- For Windows: does not have a cshrc file

You can modify the Environmental parameters in this file.

Running the regedit utility

Running the regedit utility, you can modify the following types of parameters:

- Registry parameters (Windows)
- E-mail configuration parameters (Windows)
Modifying CONTROL-M/Agent system parameters

NOTE
This procedure explains how to use the CONTROL-M Configuration Manager to change CONTROL-M/Agent system parameters. Alternatively, you can run the following utilities:

- ctmag—for all Agent and Control Module configuration parameters.
- ctmunixcfg—for many CM parameters in the OS.dat file (for Unix)
- ctmwincfg—for many CM parameters in the registry file (for Windows)

For details on these utilities, see the CONTROL-M Utility Guide.

1 In the CONTROL-M Configuration Manager, right click the CONTROL-M/Agent whose system parameters you want to view or modify, and choose CONTROL-M/Agent System Parameters.

The CONTROL-M/Agent System Parameters window displays the system parameters and values for the selected CONTROL-M/Agent.

2 To change a system parameter
   
   A Double click the parameter.
   
   B Change the value.
   
   C Click Save (or Restore Default).

Modifying CONTROL-M for z/OS system parameters

You can modify CONTROL-M for z/OS system parameters from the CONTROL-M Configuration Manager—available for CONTROL-M for z/OS versions 6.3.01 fix pack 3, and above. (Alternatively, you can use the INCONTROL™ Installation and Customization Engine (ICE). For details, see the INCONTROL for z/OS Administrator Guide.)

1 In the CONTROL-M Configuration Manager, right click the CONTROL-M for z/OS whose system parameters you want to view or modify, and choose CONTROL-M for z/OS System Parameters.

The CONTROL-M for z/OS System Parameters dialog box displays the system parameters and values for the selected CONTROL-M. Note the following points about the displayed columns:
■ Type displays the parameter member name (CTMPARM, CTRPARM, or IOAPARM)

■ Category displays the name of the section in the parameters member

2 To change a system parameter

A Double click the parameter.

B Change the value.

C Click Save (or Restore Default).

Changes are saved but CONTROL-M is not refreshed until you perform step 3.

3 To refresh CONTROL-M with the modifications, click Activate Changes in the CONTROL-M for z/OS System Parameters dialog box.

NOTE
Ensure that your specified values (content and length) conform to product rules. The values are checked against product rules when you save your modifications.

NOTE
The type of refresh (automatic, manual, or recycle) required by CONTROL-M/EM system parameters is listed in the detail line for each parameter in the System Parameters dialog box in CONTROL-M Configuration Manager.

To manually refresh CONTROL-M/EM components

1 In the Configuration Manager, right-click the component (for example, the GUI server), and choose Control Shell.

2 In the Control Shell dialog box, enter the appropriate REFRESH command and click Apply.

3 Close the dialog box.
Refreshing CONTROL-M/Server components

--- EXAMPLE ---
After modifying CONTROL-M/EM job version management parameters

1. In the CONTROL-M Configuration Manager, right-click the GUI Server component and choose Control Shell.

2. In the Control Shell dialog box, enter the `REFRESH_HISTORY` command and click Apply.

Alternatively, you can refresh a component by entering the relevant line command. For example, to apply changes to the GUI Server, you can use the following command:

```
ctl -U EM_DBO -P EM_DBO_password -C GUI_Server [-M GSR_hostname | -name logical_name_of_GUI_Server | -all] -cmdstr "REFRESH_SECURITY_PARAMS"
```

To recycle CONTROL-M/EM components

1. In the CONTROL-M Configuration Manager, right-click the component whose system parameters have been updated.

2. Choose Desired State => Recycle.

Refreshing CONTROL-M/Server components

Various parameters called by CONTROL-M/Server utilities are updated automatically each time the utility runs. In the tables under “CONTROL-M/Server parameters” on page 453, the Refresh Type indication for such parameters is Automatic.

For some system parameters, you can update a running CONTROL-M/Server with parameter changes by sending a refresh message to all CONTROL-M/Server processes. In this case, you do not have to recycle CONTROL-M/Server. In the tables under “CONTROL-M/Server parameters” on page 453, the Refresh Type indication for such parameters is Manual.

For other system parameters, you must recycle (see Recycling CONTROL-M/Server components) the relevant CONTROL-M/Server process for the changed parameter values to take effect. The relevant process that requires recycling might be any of the following:

- CONTROL-M/Server (ctm/server)
- CONTROL-M Configuration Agent (ctm/CA)
Manually refreshing CONTROL-M/Server components

You perform manual component refresh using the ctmipc utility.

After changing a refreshable CONTROL-M/Server configuration parameter, enter the following command in the command line:

```bash
ctmipc -dest ALL -msgid CFG
```

CONTROL-M/Server reloads the content of the `config.dat` file of running CONTROL-M/Server processes.

Recycling CONTROL-M/Server components

You perform component recycling from the CONTROL-M Configuration Manager.

---

**WARNING**

Recycle a CONTROL-M/Server component only when stopping and starting that component will not negatively impact processing in your production environment.

---

1. In the CONTROL-M Configuration Manager, right-click the component whose system parameters have been updated.
2. Choose **Desired State => Recycle**.

Refreshing CONTROL-M/Agent components

For CONTROL-M/Agent changes to configuration parameters take effect automatically.

System parameter reference

This section describes the following topics:

- CONTROL-M/EM parameters
- CONTROL-M/Server parameters
- CONTROL-M/Agent parameters
CONTROL-M/EM parameters

The CONTROL-M/EM parameters influence the behavior of a wide range of CONTROL-M/EM components and features. This section lists and describes the following categories of CONTROL-M/EM parameters:

<table>
<thead>
<tr>
<th>EM parameter category</th>
<th>Page reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>413</td>
</tr>
<tr>
<td>Gateway (GTW)</td>
<td>425</td>
</tr>
<tr>
<td>Global Conditions Server (GCS)</td>
<td>429</td>
</tr>
<tr>
<td>Global Alerts Server (GAS)</td>
<td>432</td>
</tr>
<tr>
<td>Configuration Agent</td>
<td>435</td>
</tr>
<tr>
<td>GUI</td>
<td>438</td>
</tr>
<tr>
<td>GUI Server (GSR)</td>
<td>439</td>
</tr>
<tr>
<td>Exception Handling</td>
<td>447</td>
</tr>
<tr>
<td>Configuration Manager Server (CMS)</td>
<td>450</td>
</tr>
<tr>
<td>Defaults.rsc parameters</td>
<td>451</td>
</tr>
</tbody>
</table>

**NOTE**

For information on BMC Batch Impact Manager and CONTROL-M/Forecast parameters, see the *Business Service Management Solutions User Guide*.

System parameters are modified using the System Parameters window of the CONTROL-M Configuration Manager. For more information, see “Modifying CONTROL-M/EM system parameters” on page 405.

**NOTE**

System parameters related to BMC Batch Impact Manager are described in the *Business Service Management Solutions User Guide*.

**General parameters**

**NOTE**

After modifying these general parameters, stop and restart all Gateway components for the changes to take effect.
### Table 70 General parameters (part 1 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>act_chk_int_gcs_gui</strong></td>
<td>Do not modify this parameter unless requested by BMC Software Customer Support.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> N</td>
</tr>
<tr>
<td><strong>AllowListEMUserNames</strong></td>
<td>Determines whether users can view a list of user names (used by CONTROL-M Control Module for Advanced File Transfer configuration plug-in).</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 - Not permitted</td>
</tr>
<tr>
<td></td>
<td>■ 1 - Permitted (default).</td>
</tr>
<tr>
<td><strong>AllowReportViewing</strong></td>
<td>Used to specify who is granted permission to view Batch Impact Manager reports in which information is missing.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 - Only administrators are allowed to create reports (default)</td>
</tr>
<tr>
<td></td>
<td>■ 1 - All users are allowed to create reports</td>
</tr>
<tr>
<td><strong>AllowQueryDBFieldValues</strong></td>
<td>Determines whether users can view existing database values.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 - Disabled</td>
</tr>
<tr>
<td></td>
<td>■ 1 - Feature enabled (default)</td>
</tr>
<tr>
<td><strong>AllowQueryFieldValues</strong></td>
<td>Allows user to indicate whether the Available Values option is displayed for selected fields in What If dialogs.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 - Disabled</td>
</tr>
<tr>
<td></td>
<td>■ 1 - Feature enabled (default)</td>
</tr>
<tr>
<td><strong>AuditCleanupIntervalMinutes</strong></td>
<td>When cleanup of audit information from the CONTROL-M/EM database is automatic, this parameter specifies the interval, in minutes, at which the GUI Server performs its cleanup operations.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 60 and up</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 360 (minutes)</td>
</tr>
<tr>
<td><strong>AuditCleanupOn</strong></td>
<td>This parameter specifies whether cleanup of audit information from the CONTROL-M/EM database should occur automatically.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> When automatic cleanup of audit information is activated, the GUI Server first waits the specified number of minutes (as specified in the AuditCleanupIntervalMinutes system parameter) before cleaning the auditing table the first time.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0: Cleanup is performed manually by the user as necessary</td>
</tr>
<tr>
<td></td>
<td>■ 1: Cleanup is automatic</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 1</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>AuditHistoryDays</td>
<td>When cleanup of audit information from the CONTROL-M/EM database is automatic, this parameter specifies the number of days that audit information is retained before being cleaned from the CONTROL-M/EM database.</td>
</tr>
<tr>
<td></td>
<td><strong>Minimum value:</strong> 1</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 1</td>
</tr>
<tr>
<td>AuthenticationMethod</td>
<td>Name of the external authentication plug-in.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> null (for internal CONTROL-M/EM authentication)</td>
</tr>
<tr>
<td>bulk_def_size</td>
<td>Default bulk size for database bulk operation.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 10-10000</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 100</td>
</tr>
<tr>
<td>bulk_def_storage_len</td>
<td>Default value for storage length in bulk operation. Must be at least as long as the longest field involved in the bulk operation.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 264</td>
</tr>
<tr>
<td>ChallengeResponseTimeout</td>
<td>Time interval in seconds after the server issues a challenge during which a response received from the client will be accepted. If a response is not received during this interval, the server sends a FAILURE message and terminates the communication.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 60</td>
</tr>
<tr>
<td>CGSCommUserIGd</td>
<td>ID that GCS uses to identify itself to CONTROL-M. This user must be defined in the CONTROL-M with add or delete condition privileges.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> GCSERV</td>
</tr>
<tr>
<td>CmsCtmNGRefreshInterval</td>
<td>Sets the refresh interval in seconds for collecting node group data.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0-10000 (0 -node group data is not collected)</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 900</td>
</tr>
<tr>
<td>DatabaseCheckInterval</td>
<td>Amount of time between database availability checks by certain server components.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 10</td>
</tr>
<tr>
<td>DatabasePoolSize</td>
<td>Determines the maximum number of connections to the database retained in the connection pool of each server component.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this parameter unless instructed to do so by BMC Software Customer Support.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 5</td>
</tr>
</tbody>
</table>
### CONTROL-M/EM parameters

#### DatabaseRetries
The maximum number of attempts by a server component to perform certain actions with the database.

**Default:** 10

#### DatabaseRetryInterval
The amount of time between the attempts detailed in DatabaseRetries.

**Default:** 10

#### DefaultAverageTime
Average run time for jobs with no statistics. In the format **HH:MM**. This value is often used if no statistics are available.

**Default:** 00:05

#### DeleteChunkSize
Maximum number of rows to be deleted by a single SQL statement, used by `purge_runinfo` and `erase_audit_data` scripts.

**Default:** 10000

**Valid values:** 100-50000

#### DirectoryServiceAuth
Determines the Directory Service mode for authentication purposes.

**Valid values:**
- PrepExt
- On
- PrepInt
- Off

**Default:** Off

**Note:** As of CONTROL-M/EM 6.3.01, this is only for the Active Directory, on Windows.

#### DirectoryServerHostPort
The full domain name of the host on which the Active Directory server is installed and the port on which to communicate with the Active Directory server.

**Format:** `full domain name:port number`

**Example:** `CTMhost1.DOMAIN1.level1:1530`

**Default:** <null>

**Note:** Multiple active directory servers can be defined. This enables CONTROL-M/EM to perform authentication against backup active directory servers when the primary server is unavailable.
### Table 70  General parameters (part 4 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DirectoryServerProtocol</td>
<td>Determines the security level of communication with the Directory Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ TCP</td>
</tr>
<tr>
<td></td>
<td>■ SSL</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> TCP</td>
</tr>
<tr>
<td>HandleAlertsOnRerun</td>
<td>Determines how to handle alerts when a job is rerun.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 – Alerts for this job that are in the Alerts window before the job is</td>
</tr>
<tr>
<td></td>
<td>rerun are not automatically changed to HANDLED. If the rerun fails, a new</td>
</tr>
<tr>
<td></td>
<td>alert is displayed in the Alerts window.</td>
</tr>
<tr>
<td></td>
<td>■ 1 – Alerts for this job that are in the Alerts window before the job is</td>
</tr>
<tr>
<td></td>
<td>rerun are automatically changed to HANDLED.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td>HostPort</td>
<td>Host name and port number for a specified component. This parameter can</td>
</tr>
<tr>
<td></td>
<td>have multiple values, each related to a different component or a different</td>
</tr>
<tr>
<td></td>
<td>host computer.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> null</td>
</tr>
<tr>
<td></td>
<td><strong>Format:</strong> host name:port number</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> CTMhost1:1530</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> See “HostPortList” on page 427.</td>
</tr>
<tr>
<td>I18N</td>
<td>Indicates whether the system is configured for CJK languages or Latin1</td>
</tr>
<tr>
<td></td>
<td>languages.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> This parameter is automatically set during installation,</td>
</tr>
<tr>
<td></td>
<td>according to the specified choices, and must not be changed manually.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the CONTROL-M Installation Guide</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ cjk</td>
</tr>
<tr>
<td></td>
<td>■ latin1</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> latin1 or cjk</td>
</tr>
</tbody>
</table>
### Table 70  General parameters (part 5 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Language  | Language for the CONTROL-M/EM application. These values are not case-sensitive.  
**Valid values:**  
- use_account_locale — language set for the account and computer  
us_english  
- english  
- german  
- french  
- spanish  
**Default:** use_account_locale |
| LimitGCDistribActivate | Enables and disables limitations on the distribution of global conditions using the Global Conditions Distribution facility.  
**Valid values:**  
- 1 – The Global Conditions Distribution facility distributes global conditions according to limitations defined using the LimitGCDistribMaxDays and LimitGCDistribExcludeDates parameters.  
- 0 – The Global Conditions Distribution facility imposes no limitations on the distribution of global conditions.  
**Default:** 1 |
| LimitGCDistribExcludeDates | Dates for which global conditions are distributed, regardless of limitations specified using the LimitGCDistribMaxDays parameter. Dates are specified in mmdd format and separated with commas.  
**Default:** STAT |
| LimitGCDistribMaxDays | The range of days within which conditions can be distributed.  
**Valid values:** 1-28  
**Default:** 7 |
| LMGUI_Collection_Cfg | License Manager address. Not yet implemented.  
**Default:** null |
| LockAccountForMinutes | Time interval, in minutes, after which an account that was automatically locked is automatically unlocked. (Accounts locked by an administrator are not unlocked automatically.)  
If set to 0, the account is not automatically unlocked but an administrator can manually unlock it.  
**Default:** 0 |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| MaxAuditsToDelete       | When cleanup of audit information from the CONTROL-M/EM database is automatic, this parameter specifies the maximum number of audit records to delete during each automatic cleanup operation. If the number of audit records to clean is higher than this number, no records are deleted and a message is issued to the GUI Server diagnostic log asking you to clean audit records manually using the erase_audit_data script.  
  **Default:** 2000                                                  |
| MaxPasswordLength       | The maximum number of characters for user passwords.                                                                                                                                                        |
  **Note:** If a CONTROL-M administrator uses the Authorization facility to set a password, this parameter is ignored.  
  **Valid values:** Any value between the MinPasswordLength and 32 (inclusive).  
  **Default:** 32                                                      |
| MaxUpdatedJobsToAudit   | Maximum number of updated jobs recorded in the Audit log when writing a scheduling table to the CONTROL-M/EM database. If this number is exceeded, or if any job in the scheduling table is added or deleted, only one audit record is recorded at scheduling table level and audit data is not recorded at the job level.  
  **Default:** 25                                                      |
| MinPasswordLength       | The minimum number of characters for user passwords.                                                                                                                                                        |
  **Note:** If a CONTROL-M administrator uses the Authorization facility to set a password, this parameter is ignored.  
  **Valid values:** Any value between 1 and the MaxPasswordLength (inclusive).  
  **Default:** 6                                                      |
| NrHandledAlarms         | The maximum number of handled alerts saved in the database (in addition to not-yet-handled alerts).                                                                                                          
  **Default:** 2000                                                  |
  **Note:** When set to 0, handled alerts are not deleted.            |
| NumberOfFailedLogins    | The number of sequential failed logins after which an account is locked.                                                                                                                                     
  **Valid values:** 0-100                                             
  **Default:** 0 (indicates that “automatic account locking” is not enabled and accounts are never automatically locked)
### Table 70 General parameters (part 7 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **NumberOfPasswordReplacements** | The number of password changes that must occur before a password can be reused if `PasswordHistoryOnOff` is set to 1.  
  **Note:** If a CONTROL-M administrator uses the Authorization facility to set a password, this parameter is ignored.  
  **Valid values:** 1-20  
  **Default:** 10 |
| **PasswordComplexityOnOff**      | Indicates if passwords need to comply with complexity rules.              |
|                                  | **Note:** If a CONTROL-M administrator uses the Authorization facility to set a password, this parameter is ignored.  
  **Valid values:**  
  ■ 0 (no = off)  
  ■ 1 (yes = on)  
  **Default:** 0 |
| **PasswordComplexityRules**      | One, some, or all of the following values separated by a blank space. Multiple values are joined by AND logic.  
  **Note:** If a CONTROL-M administrator uses the Authorization facility to set a password, this parameter is ignored.  
  **Valid values:**  
  ■ PWD_DIGIT: using digits is mandatory  
  ■ PWD_UPPER: using letters in upper case is mandatory  
  ■ PWD_LOW: using letters in lower case is mandatory  
  ■ PWD_NON_LETDIG: non-alphanumeric characters are mandatory  
  ■ PWD_DIGIT PWD_UPPER PWD_LOW PWD_NON_LETDIG: all of these rules to be satisfied. (Default) |
| **PasswordEncode**               | Indicates how user passwords are transmitted by clients to the server. For more information, see “Authentication methods” on page 151.  
  **Valid values:**  
  ■ 0 - Clear text (not encoded). Often used with External Authentication.  
  ■ 1 - Encrypted by the client.  
  ■ 2 - Challenge-response. Recommended if SSL is not used.  
  **Default:** 2 |
### Table 70  General parameters (part 8 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **PasswordExpirationOnOff** | Determines whether password expiration parameters should be checked. For more information, see “Implementing password expiration policy” on page 163.  
  **Valid values:**  
  - 0 (off, password expiration is not checked).  
  **Note:** When set to 0, other password expiration parameters can be edited but are ignored.  
  - 1 (on, password expiration is checked).  
  **Default:** 0 |
| **PasswordHistoryOnOff** | Determines whether password history is recorded.  
  **Note:** If a CONTROL-M administrator uses the Authorization facility to set a password, this parameter is ignored.  
  **Valid values:**  
  - 0 (no). If set to 0, new passwords are not checked against previous passwords.  
  - 1 (yes)  
  **Default:** 0 |
| **PasswordLifetimeDays** | Provides the default value of $n$ in the Password will expire every $n$ days option. Used in the password expiration date computation by the set_pwd_def_lifetime script. For more information, see “Implementing password expiration policy” on page 163.  
  **Valid values:** 1 - 365  
  **Default:** 60 |
| **PermitManualUnlock** | This parameter specifies whether non-administrators can manually unlock their own scheduling tables (for example, if tables are locked during an abnormal disconnect from the GUI Server).  
  **Note:** Non-administrators will not be able to unlock other users’ scheduling tables.  
  **Valid values:**  
  - 1 - Users can unlock their own tables  
  - 0 - Only administrators can unlock the table  
  **Default:** 1 |
### Table 70  General parameters (part 9 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunTimeDeleteHistChunkSize</td>
<td>Indicates the maximum number of rows in the database of historical data to be deleted, each time a deletion is performed.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 25000</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This system parameter is relevant only if CONTROL-M/Forecast is installed. For more information, refer to the CONTROL-M Business Service Management Solution User Guide.</td>
</tr>
<tr>
<td>RunTimeDeleteHistInterval</td>
<td>Interval in seconds between the deletion of historical records.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 21600</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This system parameter is relevant only if CONTROL-M/Forecast is installed. For more information, refer to the CONTROL-M Business Service Management Solution User Guide.</td>
</tr>
<tr>
<td>SendAlarmToScript</td>
<td>Full path name of the script that is activated when an alert is generated. This script is activated only if the value of SendSnmp is either 1 or 2.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> script_name</td>
</tr>
<tr>
<td></td>
<td>When Alert data is sent as input to a script, the parameters are sent in the following format:</td>
</tr>
</tbody>
</table>
|                               | ```bash
    call_type: "<call_type>" alert_id: "<alert_id> " data_center: "<data_center> " memname: "<memname> " order_id: "<order_id>" severity: "<severity>" status: "<status> " send_time: "<send_time>" last_user: "<last_user> " last_time: "<last_time> " message: "<message> " owner: "<owner> " group: "<group> " application: "<application> " job_name: "<job_name> " node_id: "<node_id> " alert_type: "<alert_type> " closed_from_em: "<closed_from_em> " ticket_number: "<ticket_number> " run_counter: "<run_counter> 
```

**Example** for testing SNMP traps when enabling this parameter

**On UNIX:**
```bash
#!/bin/sh
echo $* > /tmp/snmptest.out
```

**On Windows:**
```bash
echo %1% %2% %3% %4% %5% > c:snmptest.out
```

**Note:** On Windows, double backslashes should be used as a delimiter.
### Table 70  General parameters (part 10 of 12)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SendSnmp</strong></td>
<td>Indicates where Alert data is to be sent.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>0 - SNMP only</td>
</tr>
<tr>
<td></td>
<td>1 - User-defined script only</td>
</tr>
<tr>
<td></td>
<td>2 - SNMP and user-defined script</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Alert data is sent to SNMP (values 0 or 2) only if the value of</td>
</tr>
<tr>
<td></td>
<td>the <strong>SnmpSendActive</strong> parameter is set to 1.</td>
</tr>
<tr>
<td><strong>SnmpHost</strong></td>
<td>Host name or list of host names (if a list, using semi-colons (;) as</td>
</tr>
<tr>
<td></td>
<td>delimiters) to send the SNMP trap on an alert. Specific ports can be set</td>
</tr>
<tr>
<td></td>
<td>using a colon (:) as a delimiter.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> &lt;no_host&gt;</td>
</tr>
<tr>
<td></td>
<td><strong>Example:</strong> dhost1;jhost2;myhost3:2000</td>
</tr>
<tr>
<td><strong>SnmpSendActive</strong></td>
<td>Determines whether SNMP messages for Active Alerts are generated.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>0—SNMP messages for Active alerts are not generated</td>
</tr>
<tr>
<td></td>
<td>1—SNMP messages for Active alerts are generated</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>UnsupportedClientVersions</strong></td>
<td>For BMC Software Customer Support use only.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>UserAuditContext</strong></td>
<td>Specifies the activities that are audited and recorded.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>ALL – All of the activities listed below</td>
</tr>
<tr>
<td></td>
<td>NONE – None of the activities listed below</td>
</tr>
<tr>
<td></td>
<td>AUTH – Authentication (logon tries, logouts, password actions)</td>
</tr>
<tr>
<td></td>
<td>SCHED – Scheduling definition activities</td>
</tr>
<tr>
<td></td>
<td>J_CONT – Active network activities (control requests)</td>
</tr>
<tr>
<td></td>
<td>J_INFO – Active job information activities (order, force, hold ...)</td>
</tr>
<tr>
<td></td>
<td>RES – Quantitative and Control resource activities</td>
</tr>
<tr>
<td></td>
<td>ALERT – Alerts</td>
</tr>
<tr>
<td></td>
<td>ACCOUNT – Account management activities</td>
</tr>
<tr>
<td></td>
<td>AUTH SCHED J_CONT J_INFO RES ALERT ACCOUNT (Default)</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>UserAuditOn</strong></td>
<td>Indicates if activities specified in UserAuditContext are recorded in the CONTROL-M/EM database.</td>
</tr>
</tbody>
</table>
| **Valid values:**                 | ■ 0 (no) - When 0, the UserAuditContext parameter is ignored.  
■ 1 (yes) Default: 0                                                                                                                                     |
| **VMAdditionalJobsRelateFields**  | Additional job related key fields to be defined by a user.                                                                                                                                                  |
|                                   | BMC Software recommends that you not use the same job name (or mem name, in CONTROL-M for z/OS) for multiple jobs. If you use the same name for multiple jobs, use this field to identify additional key fields that CONTROL-M/EM can use to distinguish between different jobs with the same name/mem name, so as not to confuse or switch their job histories. |
|                                   | A space must be used as a delimiter between key field values. For example: NODE_ID OWNER CMD_LINE                                                                                                          |
| **Recommended Values:**           | DESCRIPTION, MEM_LIB, NODE_ID, OWNER, DAYS_CAL, WEEKS_CAL, CONF_CAL, CMD_LINE, FROM_TIME, TO_TIME, ACTIVE_FROM, ACTIVE_TILL                                                                             |
| **Default:**                      | <empty>                                                                                                                                                                                                   |
| **Refresh Type:**                 | Manual                                                                                                                                                                                                   |
| **VMVersionsNumberToKeep**        | The number of versions of the job to keep, including the current version.                                                                                                                                   |
| **Note:**                         | A job version is deleted only when all of the following are true:  
■ The version exceeds VMVersionsNumberToKeep.  
■ The version exceeds VMMaxDaysRetainCurJobsHistory.  
■ Automatic cleanup has run, as determined by VMCleanupIntervalMinutes. For more information, see “Implementing job version management” on page 105. |
|                                   | BMC Software recommends not setting a value greater than 30 because of possible performance degradation.                                                                                                   |
|                                   | To deactivate version history, set the parameter to 1 (keep current version only).                                                                                                                         |
| **Default:**                      | 2 (current version, and one history version)                                                                                                                                                              |
| **Refresh Type:**                 | Manual                                                                                                                                                                                                   |
**Gateway parameters**

**Table 70  General parameters (part 12 of 12)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WarningPasswordExpirationDays</td>
<td>Number of days prior to password expiration during which a warning message is generated when certain utilities or scripts are run or a successful logon occurs.</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Implementing password expiration policy” on page 163.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values</strong>: 0-90</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 0 (no warning is generated)</td>
</tr>
<tr>
<td>WarningSSLExpirationDays</td>
<td>Number of days prior to certificate expiration during which the GUI server and GAS generate a warning message in the CONTROL-M Configuration Manager.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values</strong>: 1-365</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 60</td>
</tr>
</tbody>
</table>

**Table 71  Gateway parameters (part 1 of 4)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlertOnAbend</td>
<td>Flag that indicates whether alerts are (1) or are not (0) sent for jobs that end NOTOK.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values</strong>: 0 - Alerts are not created. 1 - Alerts are created</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 1</td>
</tr>
<tr>
<td>CommCtmBufferSize</td>
<td>The number of bytes buffered in Gateway that are waiting to be sent to the CONTROL/M Server. If the number of bytes are exceeded, communication with CONTROL/M Server is terminated.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 10000000</td>
</tr>
<tr>
<td>CommEMBufferSize</td>
<td>The number of bytes buffered in Gateway that are waiting to be sent to other EM Servers. If the number of bytes are exceeded in GSR,GAS,GCS components, communication with CONTROL/M Server is terminated.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 10000000</td>
</tr>
<tr>
<td>DeltaMaxActMinutes</td>
<td>Age, in minutes, for a net to be considered valid for distribution of Global Conditions.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 2160</td>
</tr>
</tbody>
</table>
### Table 71  Gateway parameters (part 2 of 4)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| DownCreAlerts              | Flag that indicates whether to send alerts for downloaded jobs that end NOTOK when they are run. **Note:** `AlertOnAbend` must be set to `1` for `DownCreAlert` to be operational.  

Valid values:
- `0` - Alerts are not sent.
- `1` - Alerts are sent.

Default: `1` |
| EBCDIC_cp                  | For MVS data centers: This parameter defines the EBCDIC code page to which ASCII data is translated.  

Valid values:
- `0` - Instructs the gateway to use the translation table that was used by the previous version.
- `1047` for English (USA)
- `285` for English (British)
- `273` for German
- `297` for French
- `284` for Spanish

Default: `0` |
| GatewayDefaultTraceOptions | Enables you to set command line trace options for multiple gateways.  

**Note:** If a gateway already has a trace option specified, the `GatewayDefaultTraceOptions` parameter value is ignored.  

Valid values: All Gateway trace option parameters

Default: `<empty>` |
| GtwCondDispatchErr         | For Customer Support use only.  

Default: CTM5050 CTM5301 CTM5311 CTM5312 CTM5323 |
| GtwNumUpdateThreads        | Only available if GtwParallelProcessingMode is on. *(See below.) The number of threads in the multi-thread processing mode is indicated by the value of this parameter.  

Valid values: `2-16`

Default: `2` |
| GtwParallelProcessingMode  | Enables multi-threading processing mode. The value `off` indicates single-thread processing.  

Valid values:
- `on`
- `off`

Default: `0` |
### Table 71  Gateway parameters (part 3 of 4)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HostPortList</td>
<td>Listening port host name and port number for gateways. Format: ( CONTROL-M_name1=host1:port1;CONTROL-M_name2=host2:port2 )</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: null</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: This parameter is overridden by the HostPort parameter. See “HostPort” on page 417.</td>
</tr>
<tr>
<td>InsertAlertTries</td>
<td>Number of times that the gateway attempts to insert an alert into CONTROL-M/EM. The number includes the initial attempt and can be any whole number equal to or greater than 1.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 10</td>
</tr>
<tr>
<td>MaxDownHistDays</td>
<td>Number of days that the list of downloads is saved. This list contains abbreviated information about each download, such as date and time, net name, and number of downloaded jobs and resources.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 100</td>
</tr>
<tr>
<td>MaxOldDay</td>
<td>Downloads are kept in the CONTROL-M/EM database for not more than the number of days specified in this parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 2</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The number of downloads stored in the database is never more than the smaller of the MaxOldDay value and the MaxOldTotal value.</td>
</tr>
<tr>
<td>MaxOldTotal</td>
<td>Number of downloads that can be stored in a CONTROL-M/EM database. If this number is exceeded, the oldest download is deleted.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 4</td>
</tr>
<tr>
<td>MaxUploadBufferMPM</td>
<td>For Customer Support use only.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 60000</td>
</tr>
<tr>
<td>MaxUploadBufferMVS</td>
<td>For Customer Support use only.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 60000</td>
</tr>
<tr>
<td>RunInfoErrorLevel</td>
<td>For BMC Software Customer Support use only.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 0</td>
</tr>
<tr>
<td>RunInfoIgnoreDevCnt</td>
<td>Indicates the maximum and minimum length of elapsed run time between calculation discards.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 2</td>
</tr>
<tr>
<td>RunInfoMaxSamples</td>
<td>Indicates the maximum number of run samples to be kept per job.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: 20</td>
</tr>
</tbody>
</table>
### Table 71  Gateway parameters (part 4 of 4)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunInfoProcRecords</td>
<td>Maximum number of run detail records processed in one loop.</td>
<td>100</td>
</tr>
<tr>
<td>RunInfoTimeCvtOpt</td>
<td>The start and end times of a job kept in the database according to the time as set in the CONTROL-M iteration.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ None – no conversion is done, time is saved as received from CTM</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ GMT – converted to GMT</td>
<td></td>
</tr>
<tr>
<td>RunInfoUpdCtx</td>
<td>Configures the context in which run information is processed.</td>
<td>1</td>
</tr>
<tr>
<td>RunInfoWaitInterval</td>
<td>Interval in seconds between processing of run details in the Gateway.</td>
<td>10</td>
</tr>
<tr>
<td>SSLRetries</td>
<td>Number of times CONTROL-M/EM attempts to establish communication with the gateway before turning SSL on or off. SSL can either be enabled or disabled when CONTROL-M/EM initially tries to connect to the gateway. After making the specified number of attempts, SSL is toggled on or off (as required). This parameter is relevant only when SSL Enabled communication is selected. It does not work when only TCP/IP is selected.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2</td>
<td></td>
</tr>
<tr>
<td>SSSyncTime</td>
<td>Replaces the value of the Sync_Timeout parameter (in the <code>Defaults.rsc</code> file) that determines the period of time between attempts to establish communication with the gateway when changing the communication protocol to SSL Enabled.</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 90</td>
<td></td>
</tr>
</tbody>
</table>
## Global Conditions Server parameters

Table 72  Global Conditions Server (GCS) administration parameters (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>BalanceIntSecs</strong></td>
<td>During periods of heavy administrative activity, interval, in seconds, after which GCS stops performing low-priority administrative tasks and handles waiting events on its sockets. <strong>Default:</strong> 120</td>
</tr>
<tr>
<td><strong>BcpForDb</strong></td>
<td>Indicates whether GCS should use bulk insertion to place values in the database for recovery purposes. <strong>Valid Values:</strong> 0 - Do not use bulk copy 1- Use bulk copy wherever possible. <strong>Default</strong></td>
</tr>
<tr>
<td><strong>BulkSendIntSecs</strong></td>
<td>Interval (in seconds) between sending groups of conditions to a reconnecting data center. <strong>Default:</strong> 60</td>
</tr>
<tr>
<td><strong>BulkSendMax</strong></td>
<td>Maximum number of messages to send in a group to a reconnected data center. <strong>Default:</strong> 100</td>
</tr>
<tr>
<td><strong>CleanOldIntSecs</strong></td>
<td>Maximum time, in seconds, unused conditions wait in the database before they are removed. These conditions may have no data center destinations. <strong>Default:</strong> 86400 (24 hours)</td>
</tr>
<tr>
<td><strong>DoneGcDelIntSecs</strong></td>
<td>Interval, in seconds, after which GCS cleans already handled conditions from memory and the database. <strong>Default:</strong> 120</td>
</tr>
<tr>
<td><strong>DoneGcDelQuota</strong></td>
<td>during heavy periods of cleanup of old conditions, number of cleaned conditions after which GCS will check to see if the time interval specified in the <strong>balance_gcs_int_secs</strong> system parameter has been reached. <strong>Default:</strong> 50</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> To prevent the GCS from pausing to check the <strong>balance_gcs_int_secs</strong> interval, and possibly stopping cleanup before it is complete, set the value of <strong>handled_gc_del_quota</strong> to 0.</td>
</tr>
<tr>
<td><strong>GcDoneWaitSecs</strong></td>
<td>Minimum time (in seconds) global conditions wait in memory, after they have been sent to all connected data centers, before they are removed. This “waiting period” prevents conditions from being sent again. <strong>Default:</strong> 120</td>
</tr>
</tbody>
</table>
**Table 72  Global Conditions Server (GCS) administration parameters (part 2 of 3)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| GcHandleMultiple  | How to handle conflicting add or delete requests for global conditions when the requests are received within the interval specified in **Delete Time for Sent Conditions**.\[1\]  

**Valid Values:**  
0 – Each time a new request conflicts with the current request, stop processing the current request and start processing the new request.  
1 – The first time a new request conflicts with the current request, stop processing the current request and start processing the new request (as in value 0 above). However, ignore all subsequent conflicting requests and continue processing the second request.  
2 – Continue processing the current request and ignore all conflicting requests.  
3 – This value differentiates processing depending on the CONTROL-M type and version that issues the request, as follows (Default):  
  - If the request comes from CONTROL-M for z/OS versions 6.2 or earlier, or CONTROL-M for AS-400, it works like the value 1.  
  - For all other supported CONTROL-M types and versions, it works like the value 0. |
| GcMaxRetries      | Maximum number of retries to send conditions to a data center that had previously returned a temporary error. **Default:** 5                          |
| GcRetryIntSecs    | Interval (in seconds) between attempts to send conditions to a data center that had previously returned a temporary error. **Default:** 180      |

**Note:** In CONTROL-M/EM environments with high workloads, the Global Conditions server may not respond to life check requests because it is busy communicating with gateways and re-sending messages. Increase this parameter to 360 or more to avoid overloading the Global Conditions server and help it respond to the Maintenance Agent. |
| GcUnsentWaitSecs  | Time (in seconds) unsent global conditions wait in memory before they are removed. **Default:** 36000 (10 hours)                                      |
| PortNum           | Default port where GCS waits for requests from clients (such as ctl commands or life check messages). This value is used only if a port has not been defined using the HostPort system parameter. Furthermore, this port is used only if it is not busy; otherwise GCS selects a free port at random. **Default:** 1000                      |
Table 72  Global Conditions Server (GCS) administration parameters (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SetGcMultipleHandling</td>
<td>Mode used to handle conflicting add or delete requests for global conditions in relation to the <strong>Method for Handling Conflicting Conditions</strong> setting.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid Values:</strong></td>
</tr>
<tr>
<td></td>
<td>0 – If the request is from CONTROL-M/Server version 6.1.0 or higher, ignore the <strong>Method for Handling Conflicting Conditions</strong> setting. Instead, handle all requests until they are sent to all destinations.</td>
</tr>
<tr>
<td></td>
<td>1 – Always handle conflicting requests as specified in the <strong>Method for Handling Conflicting Conditions</strong> option. <strong>Default</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If CONTROL-M/EM or CONTROL-M/Server version 6.1.00 through 6.1.02 was used at your site and you used global conditions in job scheduling, consider setting the value of this parameter to 0 (to ensure that the same method that was used in version 6.1.01 or 6.1.02 is used in the current version).</td>
</tr>
<tr>
<td>ShortestSlptimeMicros</td>
<td>Time interval, in microseconds, during which the process will check the socket for new requests. This parameter takes effect when the time out of a previously scheduled event has just been reached. <strong>Default:</strong> 1 (microsecond)</td>
</tr>
<tr>
<td>SlptimeRatio</td>
<td>Value to be used in a ratio that determines the time that the process will wait for outside requests before leaving to idle time processing. <strong>Default:</strong> 10</td>
</tr>
<tr>
<td></td>
<td>The actual wait time is determined by the time-out interval of the next scheduled high priority production activity, divided by this SlptimeRatio value.</td>
</tr>
<tr>
<td>SrvrsPollIntSecs</td>
<td>Interval (in seconds) between attempts to communicate with a gateway. <strong>Default:</strong> 60</td>
</tr>
<tr>
<td>UpdCommIntSecs</td>
<td>Interval (in seconds) between readings of the Communication Table in the CONTROL-M/EM database for new data centers. <strong>Default:</strong> 60</td>
</tr>
</tbody>
</table>

Table 73  Global Conditions Server (GCS) logging parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CondLogLvl</td>
<td>Logging information level for condition transfer activities. Information is displayed for conditions received (In), conditions sent (Out), transfer confirmation and rejection actions, and communication problems.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid Values:</strong></td>
</tr>
<tr>
<td></td>
<td>0 – No diagnostics</td>
</tr>
<tr>
<td></td>
<td>1 – Condition transfer, problem, and information received</td>
</tr>
<tr>
<td></td>
<td>2 – Condition transfer, problem, and information sent</td>
</tr>
<tr>
<td></td>
<td>3 – Value 1 + value 2 (Default)</td>
</tr>
<tr>
<td>DbLogLvl</td>
<td>Logging information level for messages related to database activities. Diagnostic information is displayed about condition transfer requests inserted or deleted in the database or read from the database for recovery operations.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid Values:</strong></td>
</tr>
<tr>
<td></td>
<td>0 – No diagnostics</td>
</tr>
<tr>
<td></td>
<td>1 – Messages about database writing (insert, update, delete)</td>
</tr>
<tr>
<td></td>
<td>2 – Value 1 plus database reading (recovery operations) activity (Default)</td>
</tr>
</tbody>
</table>
CONTROL-M/EM parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>IntLogLvl</td>
<td>Determines the logging information level for messages related to internal GCS actions involving temporary problems and rebound situations. The information is displayed about GCS condition handling activities.</td>
</tr>
</tbody>
</table>
|             | **Valid Values:**  
|             | 0 – No diagnostics  
|             | 1 – Condition actions based on conflict handling policies  
|             | 2 – Value 1 plus communication problems (Default)  
|             | 3 – Value 2 plus condition handling status messages  |
| LogSize     | Maximum number of record lines in the GCS_LOG file. When the number of record lines in the currently open GCS_LOG file reaches the value specified in this parameter, the file is closed and a new GCS_LOG file is opened. **Default:** 25000 |
|             | **Note:** 0 = Never close the file because there is no maximum size.  |
| MsgLogLvl   | Determines the message packets (dsects) that are displayed and written to the GCS_LOG file. Condition transfer requests and messages related to inter-process communication activities are displayed. Valid values:  |
|             | **Valid Values:**  
|             | 0 – No diagnostics  
|             | 1 – Condition transfer request messages (Default)  
|             | 2 – Content of all messages sent to gateways by GCS  
|             | 3 – Values 1 and 2  
|             | 4 – Value 3 plus life check messages received by GCS  |
| MaxLogs     | Maximum number of log files to be managed cyclically. When the number of GCS_LOG files reaches the value specified in this parameter, the oldest file is deleted, in order for a new GCS_LOG file to be created. **Default:** 5 |
|             | **Note:** 0 = Never delete an old GCS_LOG file because there is no maximum quantity.  |

**Global Alerts Server (GAS) parameters**

**NOTE**

After modifying Global Alerts Server parameters, stop and restart all Global Alerts Server components for the changes to take effect.
Table 74  Global Alerts Server (GAS) parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AlertReaderRetries</td>
<td><strong>For Customer Support use only.</strong> Maximum number of times the Global Alerts Server tries to read an alert from the database in case of a failure.</td>
</tr>
<tr>
<td></td>
<td>Valid values: Any integer greater than 1.</td>
</tr>
<tr>
<td></td>
<td>Default: 10</td>
</tr>
<tr>
<td>AlertsMapRefreshInterval</td>
<td>Frequency, in seconds, at which the Global Alerts updates its database about which Alerts were deleted and why. The update occurs only when both the specified time has passed and one or more alerts have been deleted.</td>
</tr>
<tr>
<td></td>
<td>Default: 60</td>
</tr>
<tr>
<td>DefaultUserTimeoutSec</td>
<td>Time, in seconds, that a CONTROL-M/EM API client user token is valid, if no value is supplied during API user registration. After this time, the Global Alerts Server can invalidate the token.</td>
</tr>
<tr>
<td></td>
<td>Default: 900</td>
</tr>
<tr>
<td>FailCheckDBTimeout</td>
<td>Time, in seconds, until the Global Alerts Server checks to confirm whether communication with the database server has been disrupted. If communication is still disrupted after this period of time has passed, communication is considered to be disrupted and the action indicated by the StopIfDBConnectionFail parameter is implemented.</td>
</tr>
<tr>
<td></td>
<td>Note: This parameter is relevant only after the Global Alerts Server determines that communication with the database server is disrupted.</td>
</tr>
<tr>
<td></td>
<td>Default: 5</td>
</tr>
<tr>
<td>GatewayOutgoingQueueSize</td>
<td>Maximum number of bytes buffered in the GUI/GAS servers waiting to be sent to CONTROL-M/Server. For example, as a result of a Save JCL request.</td>
</tr>
<tr>
<td></td>
<td>Warning: Do not change this parameter unless instructed to do so by BMC Software Customer Support.</td>
</tr>
<tr>
<td></td>
<td>Default: 500000</td>
</tr>
<tr>
<td>MaxUserTimeoutSec</td>
<td>Maximum amount of time, in seconds, that a CONTROL-M/EM API client user token is valid. After this time, the Global Alerts Server can invalidate the token.</td>
</tr>
<tr>
<td></td>
<td>Default: 10800</td>
</tr>
</tbody>
</table>
## Table 74  Global Alerts Server (GAS) parameters (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RemedyCloseTicketMode</strong></td>
<td>Indicates in which mode a Remedy ticket is closed, and what effect that has on the alert status.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>- <strong>HANDLE_ON_CLOSE</strong> - The alert status is updated to <strong>Handled</strong> automatically when the ticket is closed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>CLOSE_ON_HANDLE</strong> - When the alert status is <strong>Handled</strong>, the ticket is automatically closed.</td>
</tr>
<tr>
<td></td>
<td>- <strong>BIDIRECTION_CLOSE_HANDLE</strong> - Either an alert becoming <strong>Handled</strong> closes a ticket, or closing a ticket causes the alert status to be <strong>Handled</strong>.</td>
</tr>
<tr>
<td></td>
<td>- <strong>SEPERATE_CLOSE_HANDLE</strong> - Close and Handle are two separate actions that do not affect each other.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> <strong>HANDLE_ON_CLOSE</strong></td>
</tr>
<tr>
<td><strong>SockRecrMaxAtmp</strong></td>
<td>The maximum number of times that the Global Alerts Server can attempt to create a socket.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> -1 (no limit)</td>
</tr>
<tr>
<td><strong>SockRecrWtIntr</strong></td>
<td>Interval, in seconds, between successive attempts to create a socket.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 10</td>
</tr>
<tr>
<td><strong>StandartCheckDBTimeOut</strong></td>
<td>Interval, in seconds, between attempts by the Global Alerts Server to confirm that communication with the database server is not disrupted.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If communication with the database server is disrupted, the interval between the current and next communication check is determined by the <strong>FailCheckDBTimeOut</strong> parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 60</td>
</tr>
<tr>
<td><strong>StopIfDBConnectionFail</strong></td>
<td>Action to take if communication between the Global Alerts Server and the database server is disrupted.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>- 0 — The Global Alerts Server is shut down until communication with the database server is restored. When communication is restored, the Configuration Agent restarts the Global Alerts Server.</td>
</tr>
<tr>
<td></td>
<td>- 1 — The Global Alerts Server remains operational. However, during this time, it has <strong>Warning</strong> status (as displayed in the CONTROL-M Configuration Manager) and may not function.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
</tbody>
</table>
# Configuration Agent parameters

*NOTE*
After modifying Configuration Agent parameters, stop and restart the Configuration Agent component for the changes to take effect.

## Table 75  Configuration Agent parameters (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ActivateRetries</strong></td>
<td>The number of times that the Configuration Agent tries to start an inactive component.</td>
</tr>
<tr>
<td></td>
<td><em>Note</em>: After the specified number of retries are attempted without success, use the CONTROL-M Configuration Manager to reset the unresponsive component. Change the state of the unresponsive component to a state other than <em>Up</em>, then change it to <em>Up</em>, and then try again to activate the component.</td>
</tr>
<tr>
<td></td>
<td><em>Valid values</em>: Minimum of 3</td>
</tr>
<tr>
<td></td>
<td><em>Default</em>: 10</td>
</tr>
<tr>
<td><strong>ComponentRestartInterval</strong></td>
<td>Frequency, in minutes, at which the Configuration Agent makes an attempt to start a CONTROL-M/EM component that is not responding. This parameter can be modified from the CONTROL-M Configuration Manager.</td>
</tr>
<tr>
<td></td>
<td><em>Valid values</em>: 3-10</td>
</tr>
<tr>
<td></td>
<td><em>Default</em>: 3</td>
</tr>
<tr>
<td><strong>ComponentShowState</strong></td>
<td>Some CONTROL-M/EM components, such as the GUI Server, the gateways, and the Global Conditions server, operate hidden from the user. These components can be displayed in command prompt windows by setting this parameter to 1, stopping the Configuration Agent, and restarting the agent.</td>
</tr>
<tr>
<td></td>
<td><em>Valid values</em>: 0 and 1</td>
</tr>
<tr>
<td></td>
<td><em>Default</em>: 0</td>
</tr>
<tr>
<td><strong>LifeCheckRespTimeout</strong></td>
<td>Time, in seconds, that the Configuration Agent waits for a component to respond to a life check.</td>
</tr>
<tr>
<td></td>
<td><em>Valid values</em>: Minimum of 15</td>
</tr>
<tr>
<td></td>
<td><em>Default</em>: 30</td>
</tr>
<tr>
<td><strong>LifeCheckRetries</strong></td>
<td>Number of life checks the Configuration Agent performs before the component is treated as malfunctioning.</td>
</tr>
<tr>
<td></td>
<td><em>Valid values</em>: Minimum of 1</td>
</tr>
<tr>
<td></td>
<td><em>Default</em>: 5</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| LifeCheckRetryTime | Interval, in seconds, after performing a life check to which there was no response until another life check is performed.  
|                  | Default: 15                                                                                                                                                                                                 |
| LogCleanInterval | Interval, in minutes, between LogReg log cleaning operations by the Configuration Agent.  
|                  | **Note**: The Configuration Agent cleans the LogReg log every time it is activated.  
|                  | Default: 360                                                                                                                                                                                                |
| LogCleanLevel   | Amount of detail the clean operation erases from the LogReg log.  
|                  | **Valid values**:
|                  | ■ 0 - No deletion
|                  | ■ 1 - Cleans only the agent's own log messages
|                  | ■ 2 - Cleans all log messages
|                  | Default: 1                                                                                                                                                                                                  |
| LogHistoryDays  | Number of days that log entries are retained before they can be cleaned from the log.  
|                  | **Valid values**: Minimum of 0  
|                  | Default: 1                                                                                                                                                                                                  |
| LogInfoLevel    | Level of detail in LogReg log entries recorded by the Configuration Agent.  
|                  | **Valid values**:
|                  | ■ 0 - No entry
|                  | ■ 1 - Configuration Agent-related messages
|                  | ■ 2 - Brief component and agent related messages
|                  | ■ 3 - Detailed component and agent related messages
|                  | Default: 2                                                                                                                                                                                                  |
| SockRecrMaxAtmp | Maximum number of times that the Configuration Agent can attempt to create a socket.  
|                  | Default: -1 (no limit)                                                                                                                                                                                      |
| SockRecrWtIntr  | Interval, in seconds between successive attempts to create a socket.  
<p>|                  | Default: 10                                                                                                                                                                                                  |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>StdoutLogInfoLevel</td>
<td>Level of detail in standard output messages reported by the Configuration Agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>- 0 - No entry</td>
</tr>
<tr>
<td></td>
<td>- 1 - Configuration Agent-related messages</td>
</tr>
<tr>
<td></td>
<td>- 2 - Brief component and agent related messages</td>
</tr>
<tr>
<td></td>
<td>- 3 - Detailed component and agent related messages</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2</td>
</tr>
<tr>
<td>StopGracePeriodSec</td>
<td>Time, in seconds, that a component is given to shut down following a Stop command. When this time is exceeded, the Configuration Agent again tries to stop the component. If the number of retries specified by the StopTries parameter is exceeded, the agent kills the component.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 45</td>
</tr>
<tr>
<td>StopTries</td>
<td>Number of times that the Configuration Agent tries to stop the component using the Stop command before performing a kill operation.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> Minimum of 1</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2</td>
</tr>
</tbody>
</table>
## GUI parameters

**NOTE**
After modifying GUI parameters, stop and restart the relevant GUI components for the changes to take effect.

### Table 76  GUI parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| OrbShutdownWait     | For Customer Support use only. If CONTROL-M/EM and CONTROL-M/Desktop wait for acknowledgement from the CORBA Object Request Broker (ORB) before shutting it down.  
  **Valid values:**  
  - 0 (No) - CONTROL-M/EM and CONTROL-M/Desktop do not wait for confirmation that the ORB was shut down.  
  - 1 (Yes) - CONTROL-M/EM and CONTROL-M/Desktop wait for confirmation that the ORB was shut down.  
  **Default:** 1                                                                                       |
| ProcessCommandsPerVP| For Customer Support use only. Number of GUI Server commands that CONTROL-M/EM can process at a time for each ViewPoint. These commands include submitting, adding, and updating jobs, and making refresh requests.  
  **Default:** 1                                                                                       |
| ProcessMFCommands   | For Customer Support use only. Number of GUI Server commands CONTROL-M/EM can process at a time. These commands are not related to specific ViewPoints and include displaying pop-up windows and task bar messages in the CONTROL-M/Enterprise Manager window.  
  **Default:** 10                                                                                      |
| ProcessVPsCommands  | For Customer Support use only. Number of GUI Server commands CONTROL-M/EM can process at a time for all ViewPoints. These commands include submitting jobs, adding jobs, updating jobs, and refresh requests.  
  **Default:** 10                                                                                      |
| UserChangePassword  | Determines if a user can change his or her own password.                                                                                            
  **Valid values:**  
  - 0 - Only users who have Full or Update permission to modify security definitions can change their own password.  
  - 1 - All users can change their own password.                                                         
  **Default:** 1                                                                                      |
### GUI Server parameters

**NOTE**
If a CONTROL-M/EM administrator uses the Authorization facility to set a password, the password complexity, length, and history requirements are ignored.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action_OrderForce_AuthLevel</strong></td>
<td>Indicates if users with Browse access can order or force jobs.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ UPDATE_ACCESS – Only users with Update access can order or force a job.</td>
</tr>
<tr>
<td></td>
<td>■ BROWSE_ACCESS – Users with Browse access or Update access can order and force jobs.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> UPDATE_ACCESS</td>
</tr>
<tr>
<td><strong>AddJobsChunkSize</strong></td>
<td>Chunk size of jobs during View Point opening.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this parameter unless requested to do so by BMC Software.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 1000</td>
</tr>
<tr>
<td><strong>AllowQueryDBFieldValues</strong></td>
<td>Indicates whether Available Values options are displayed for certain fields in the Job Editing form.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 1 (On)</td>
</tr>
<tr>
<td><strong>AuthenticationLevel</strong></td>
<td><strong>Note:</strong> Do not change this parameter unless requested to do so by BMC Software.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2</td>
</tr>
</tbody>
</table>
**CONTROL-M/EM parameters**

**Table 77 GUI Server parameters (part 2 of 9)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **AuthorSecurity** | Indicates whether a very strict (restrictive), strict, or lenient (permissive) security policy is enforced for submitting jobs during New Day processing. The CONTROL-M security mechanism uses the **Author** parameter and the **AuthorSecurity** system parameter to ensure that only authorized users can submit jobs during New Day processing. In all modes, the administrator is authorized to change the author.  
**Note:** If this parameter is modified, CONTROL-M/Desktop users who are offline must log on to become synchronized with the new setting.  
See “Ensuring owner verification during New Day processing job ordering” on page 197.  
**Valid values:**  
- 1 (Permissive mode) - Editing the author is enabled. Users can retain the original Author when running utilities or performing a Write to CONTROL-M/EM, or, alternatively, change the author to another user.  
- 2 (Restrictive mode) - Author is the user currently performing a Write to CONTROL-M/EM. However, the original author can be retained for existing job processing definitions (whose associated tables are locked).  
- 3 (Very restrictive mode) - The author is set to the user currently performing a Write to CONTROL-M/EM for all job processing definitions.  
**Default:** 1 |
| **BIMCommLoop Interval** | **Note:** Do not change this parameter unless instructed to do so by BMC Software Customer Support. |
| **BIMThreadPool IdleTime** | **Note:** Do not change this parameter unless instructed to do so by BMC Software Customer Support. |
| **BIMThreadPool MaxSize** | **Note:** Do not change this parameter unless instructed to do so by BMC Software Customer Support. |
| **BIMThreadPool MinSize** | **Note:** Do not change this parameter unless instructed to do so by BMC Software Customer Support. |
| **bulk_act_cond** | Bulk size in bulk operation for retrieve conditions.  
**Note:** Do not change any of the four bulk_act.xxx parameters unless requested to do so by BMC Software.  
**Valid values:** 10 -10000  
**Default:** 250 |
| **bulk_act_grp** | Bulk size in bulk operation for retrieve scheduling groups.  
**Valid values:** 10-10000  
**Default:** 100 |
### Table 77  GUI Server parameters (part 3 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bulk_act_job</td>
<td>Bulk size in bulk operation for retrieve jobs.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 250</td>
</tr>
<tr>
<td>bulk_act_res</td>
<td>Bulk size in bulk operation for retrieving control or quantitative resources.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 10 - 10000</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 50</td>
</tr>
<tr>
<td>CloseOldDownloads</td>
<td><strong>Note:</strong> Do not change this parameter unless instructed to do so by BMC Software Customer Support.</td>
</tr>
<tr>
<td>ConcurrentCollections</td>
<td>The number of collections that can be read in parallel.</td>
</tr>
<tr>
<td></td>
<td>If set to 1, collections are read serially. Increasing this number improves response time but may use more CPU resources.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> If you increase the value of this parameter, monitor the system for several days, especially during periods of heavy usage, to ensure that performance is not degraded. You may want to increase the value of this parameter gradually (for example, by one or two at a time), to avoid CPU bottlenecks.</td>
</tr>
<tr>
<td></td>
<td>After modifying this parameter, stop and restart all GUI Server components for the change to take effect.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 1-10</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 4</td>
</tr>
<tr>
<td>ControlResourceLoadLimit</td>
<td>The maximum number of control resources that can be loaded into memory from the CONTROL-M/EM database at the same time. This parameter can help control memory usage. However, if this parameter is set to -1, there is no maximum limit.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> -1</td>
</tr>
<tr>
<td>DelayBeforePinning</td>
<td>The number of seconds before the GUI Server begins processing the <code>pin_collection.ini</code> file.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Do not change this parameter unless requested to do so by BMC Software.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 10</td>
</tr>
<tr>
<td>DeletedJobsLoadLimit</td>
<td>The number of jobs displayed to the user in the “Deleted Jobs” dialog box in the CONTROL-M/Desktop.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid value:</strong> 0 or any negative value</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2000</td>
</tr>
</tbody>
</table>
### Table 77  GUI Server parameters (part 4 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| EMAPIActiveJobsLoadLimit   | The number of jobs in the active environment that are checked by the GUI Server when processing the request_act_retrieve_jobs request, and included in the request response.  
**Valid values**: from 10 to -1 (unlimited)  
**Default**: 1000                                                                                      |
| EMThreadPoolIdleTime       | **Note**: Do not change this parameter unless instructed to do so by BMC Software Customer Support.                                                                                                             |
| EMThreadPoolMaxSize        | **Note**: Do not change this parameter unless instructed to do so by BMC Software Customer Support.                                                                                                             |
| EMThreadPoolMinSize        | **Note**: Do not change this parameter unless instructed to do so by BMC Software Customer Support.                                                                                                             |
| ExcludedJobFields          | Identifies fields (database columns) that should not be downloaded from the database when retrieving collections, thereby decreasing memory load and improving response time.  
Any or all of the following fields can be excluded. Use spaces, commas, colons, or semicolons to separate multiple entries.  
**Warning**: BMC Software recommends that you not exclude data (change the value of this parameter to 1) without first consulting BMC Software Customer Support. If you do change the value to 1, be sure to modify job processing definitions do that they do no contain excluded data.  
**Note**: CONTROL-M/EM GUI users cannot perform a find or query on excluded fields. You can modify fields to exclude by adding or removing fields in this parameter. After modifying this parameter, stop and restart all GUI Server components for the change to take effect.  
**Valid values**:  
- Database Column - Description  
- MAX_WAIT- Maximum Wait  
- ODATE - Order date  
- OWNER - Owner  
- DESCRIPTION- Description  
- CPU_ID - Node ID  
**Default**: null (no fields are excluded)                                                                                      |
Table 77  GUI Server parameters (part 5 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ExcludeJobControlRes</td>
<td>Determines whether control resources are (0) or are not (1) downloaded from the database when retrieving collections. If unneeded control resources are not downloaded, memory requirements are reduced and response time is improved.</td>
</tr>
<tr>
<td></td>
<td><strong>Warning:</strong> BMC Software recommends that you not exclude data (change the value of this parameter to 1) without first consulting BMC Software Customer Support. If you do change the value to 1, be sure to modify job processing definitions so that they do not contain excluded data.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> CONTROL-M/EM GUI users cannot perform a find or query on excluded control resources. After modifying this parameter, stop and restart all GUI Server components for the change to take effect.</td>
</tr>
</tbody>
</table>
|                       | **Valid values:**  
|                       |   - 0 – Do not exclude control resources.  
|                       |   - 1 – Exclude control resources.  
|                       | **Default:** 0 |
| ExcludeJobQuantRes    | Determines whether quantitative resources are downloaded from the database when retrieving collections. If unneeded quantitative resources are not downloaded, memory requirements are reduced and response time is improved. |
|                       | **Warning:** BMC Software recommends that you not exclude data (change the value of this parameter to 1) without first consulting BMC Software Customer Support. If you do change the value to 1, be sure to modify job processing definitions so that they do not contain excluded data. |
|                       | **Note:** CONTROL-M/EM GUI users cannot perform a find or query on excluded quantitative resources. After modifying this parameter, stop and restart all GUI Server components for the change to take effect. |
|                       | **Valid values:**  
|                       |   - 0 – Do not exclude quantitative resources.  
|                       |   - 1 – Exclude quantitative resources.  
|                       | **Default:** 0 |
### Table 77  GUI Server parameters (part 6 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FailCheckDBTimeOut</td>
<td>Time, in seconds, until the GUI Server checks the communication status of the database server. If communication is still down, communication is considered to be disrupted and the action specified in <strong>StopIfDBConnectionFail</strong> is implemented. <strong>Note:</strong> This parameter is relevant only after the GUI Server determines that communication with the database server is disrupted. After modifying this parameter, stop and restart all GUI Server components for the change to take effect. <strong>Valid values:</strong> 1-60 <strong>Default:</strong> 5</td>
</tr>
<tr>
<td>LimitArchiveJobsInMem</td>
<td>The maximum number of archive jobs in memory per GUI Server. <strong>Default:</strong> 40000</td>
</tr>
<tr>
<td>MaxObsoleteJobs</td>
<td><strong>Note:</strong> Do not change this parameter unless instructed to do so by BMC Software Customer Support.</td>
</tr>
<tr>
<td>MaxUserTimeoutSec</td>
<td>Time, in seconds, that a CONTROL-M/EM API client user token can be valid. Afterwards, the GUI Server can invalidate the token. <strong>Note:</strong> After modifying this parameter, stop and restart all GUI Server components for the change to take effect. <strong>Default:</strong> 10800</td>
</tr>
<tr>
<td>NumberOfMyWorldJobs</td>
<td>Total number of job nodes that are displayed when Local View is used. For information about Local View, see the Alerts chapter in the CONTROL-M User Guide. <strong>Note:</strong> After modifying this parameter, stop and restart all GUI Server components for the change to take effect. <strong>Valid values:</strong> 2-30,000 <strong>Default:</strong> 100</td>
</tr>
<tr>
<td>PrereqConditionsLoadLimit</td>
<td>The maximum number of prerequisite conditions that can be loaded into memory from the CONTROL-M/EM database at the same time. This parameter helps control memory usage. When PrereqConditionsLoadLimit is -1, there is no maximum limit. <strong>Default:</strong> -1</td>
</tr>
<tr>
<td>QuantResourceLoadLimit</td>
<td>The maximum number of quantitative resources that can be loaded into memory from the CONTROL-M/EM database at the same time. This parameter helps control memory usage. When QuantResourceLoadLimit is -1, there is no maximum limit. <strong>Default:</strong> -1</td>
</tr>
</tbody>
</table>
### Table 77  GUI Server parameters (part 7 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>QueriedCollection</strong></td>
<td>Collection of jobs to include in the Network Neighborhood Collection.  &lt;br&gt;  &lt;br&gt; <strong>Valid values:</strong>  &lt;br&gt;  ■ CURRENT – The collection of jobs in the ViewPoint from which the user opened the Network Neighborhood.  &lt;br&gt;  ■ All Jobs – The collection includes all jobs, not only the jobs in the current ViewPoint.  &lt;br&gt;  <strong>Default:</strong> CURRENT</td>
</tr>
<tr>
<td><strong>SecuredExcludedFields</strong></td>
<td>Determines if the GUI Server is in Secure mode. If the GUI Server is in Secure mode, user requests to view or modify fields that are included in the Security filter of a ViewPoint are rejected.  &lt;br&gt;  <strong>Warning:</strong> BMC Software recommends that you not exclude data (change the value of this parameter to 1) without first consulting BMC Software Customer Support.  &lt;br&gt;  <strong>Valid values:</strong>  &lt;br&gt;  ■ 0 - The GUI Server is not in Secure mode; it prompts the user for confirmation whether to continue processing the request.  &lt;br&gt;  ■ 1 - The GUI Server is in Secure mode; it denies the request because opening any ViewPoint might involve a security breach. The user cannot open any ViewPoint until the Authorization Filter for the user is changed by the system administrator so that it no longer contains excluded fields.  &lt;br&gt;  If the GUI Server prompts for confirmation, carefully consider the following factors before confirming the request:  &lt;br&gt;  ■ If a ViewPoint hierarchy definition contains an excluded field, the ViewPoint groups the jobs as if they all have the same empty value (“”) and the hierarchy is incorrect.  &lt;br&gt;  ■ If a Collection, Filter, or User Authorization filter contains criteria that match excluded fields, a match is assumed for those filtering criteria, yielding unwanted filtering results.  &lt;br&gt;  ■ If a User Authorization filter includes only jobs for which the user is the owner, but Owner is an excluded field, then a match on Owner is assumed for every job in the Active Environment. This could cause every job in the Active Environment to be loaded (if there are no other exclusion criteria).  &lt;br&gt;  <strong>Default:</strong> 0</td>
</tr>
</tbody>
</table>
## Table 77  GUI Server parameters (part 8 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **SockRecrMaxAtmp**        | Maximum number of times that the GUI Server can attempt to create a socket.  
  **Note:** After modifying this parameter, stop and restart all GUI Server components for the change to take effect.  
  **Default:** -1 (no limit) |
| **SockRecrWtIntr**         | Interval, in seconds between successive attempts to create a socket.  
  **Note:** After modifying this parameter, stop and restart all GUI Server components for the change to take effect.  
  **Default:** 10 |
| **StopIFDBConnectionFail** | Action to take if communication between the GUI Server and the database server is disrupted.  
  **Note:** After modifying this parameter, stop and restart all GUI Server components for the change to take effect.  
  **Valid values:**  
  ■ 0 – The GUI Server is shut down until communication with the database server is restored. When communication is restored, the Configuration Agent restarts the GUI Server.  
  ■ 1 – The GUI Server remains operational. However, its status is **Warning** (as displayed in the CONTROL-M Configuration Manager) and it may not function.  
  **Default:** 0 |
| **UseQueriedCollectionForFind** | Determines the collection of jobs to be searched when performing a Find from within a ViewPoint screen.  
  **Valid values:**  
  ■ 1 (Yes) - When performing a find from within a ViewPoint, limit the search to jobs that satisfy the QueriedCollection system parameter.  
  ■ 0 (No) - Perform the search using all jobs.  
  **Default:** 1 |
Table 77  GUI Server parameters (part 9 of 9)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ViewpointPolicy</td>
<td>Determines which group scheduling tables are passed to the ViewPoint.</td>
</tr>
<tr>
<td></td>
<td>For information about defining Group scheduling table filtering policy, see</td>
</tr>
<tr>
<td></td>
<td>“Group scheduling table displays in ViewPoints” on page 93 and</td>
</tr>
<tr>
<td></td>
<td>“Displaying empty Group scheduling tables in ViewPoints” on page 125.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ SELECT_JOBS - Filtering criteria are applied only to the jobs. Only jobs</td>
</tr>
<tr>
<td></td>
<td>satisfying the filtering criteria, and only group scheduling tables</td>
</tr>
<tr>
<td></td>
<td>containing at least one such job, are passed and displayed. (No empty</td>
</tr>
<tr>
<td></td>
<td>scheduling groups are passed.)</td>
</tr>
<tr>
<td></td>
<td>■ SELECT_JOBS_AND_SG - Filtering criteria are applied both to jobs and</td>
</tr>
<tr>
<td></td>
<td>group scheduling tables. In addition to passing the same jobs and</td>
</tr>
<tr>
<td></td>
<td>group scheduling tables that are passed for the SELECT_JOBS value, the</td>
</tr>
<tr>
<td></td>
<td>Server also passes any group scheduling tables that match the filtering</td>
</tr>
<tr>
<td></td>
<td>criteria (and pass the security criteria) even if they are empty.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> SELECT_JOBS</td>
</tr>
<tr>
<td>ViewpointTimeoutForBIM</td>
<td>The number of milliseconds within which the CONTROL-M/EM GUI Server should</td>
</tr>
<tr>
<td></td>
<td>receive a reply from the BMC Batch Impact Manager after sending a request.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 600000</td>
</tr>
<tr>
<td>UpdatesQueueLimit</td>
<td>Default size of the updates queue for a ViewPoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 5000</td>
</tr>
<tr>
<td>UpdatesQueueMaxLimit</td>
<td>The maximum possible size of the updates queue for a ViewPoint.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 60000</td>
</tr>
</tbody>
</table>

**Exception handling parameters**

Table 78  Exception handling (XAlerts) parameters (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XAlertsEnableSending</td>
<td>Determines whether the option to send exception alerts is enabled or disabled.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 1 - Enable.</td>
</tr>
<tr>
<td></td>
<td>■ 0 - Disable</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 1</td>
</tr>
<tr>
<td>IdenticalXAlertTimeDelta</td>
<td>Determines the interval, in minutes, within which an alert is defined as</td>
</tr>
<tr>
<td></td>
<td>identical to a previous matching alert.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 30 minutes</td>
</tr>
</tbody>
</table>
### Table 78  Exception handling (XAlerts) parameters (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IdenticalXAlertCompareDesc</strong></td>
<td>Determines whether the MESSAGE field is used to compare identical alerts.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 1 - Compare the MESSAGE field</td>
</tr>
<tr>
<td></td>
<td>■ 0 - Do not compare the MESSAGE field.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>XAlertsSendSnmp</strong></td>
<td>Determines whether an alert will be sent as an SNMP trap, to a script, both, or neither.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 0 - Not active</td>
</tr>
<tr>
<td></td>
<td>■ 1 - Sent as an SNMP trap</td>
</tr>
<tr>
<td></td>
<td>■ 2 - Sent to a script</td>
</tr>
<tr>
<td></td>
<td>■ 3 Sent as an SNMP trap and to a script.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>IdenticalXAlertHandling</strong></td>
<td>Determines whether identical alerts are sent as an SNMP trap or to a script.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 1 - Identical alerts are sent as an SNMP trap and to a script.</td>
</tr>
<tr>
<td></td>
<td>■ 0 - Identical alerts are not sent as an SNMP trap and to a script.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter is only valid when the XAlertsSendSnmp system parameter has a value of 1, 2, or 3.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>HandledXAlertHandling</strong></td>
<td>Determines whether handled alerts are sent as an SNMP trap or to a script.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ 1 - Handled alerts are sent as an SNMP trap and to a script.</td>
</tr>
<tr>
<td></td>
<td>■ 0 - Handled alerts are not sent as an SNMP trap and to a script.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter is only valid when the XAlertsSendSnmp system parameter has a value of 1, 2, or 3.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td><strong>XAlertsMaxAge</strong></td>
<td>Determines, in days, how long XAlerts are saved before they are deleted by the Configuration Management Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 180 days</td>
</tr>
<tr>
<td><strong>XAlertsMaxHandled</strong></td>
<td>The maximum number of handled XAlerts that are displayed in the Exception Alerts window.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 100</td>
</tr>
</tbody>
</table>
### Table 78 Exception handling (XAlerts) parameters (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>XAlertsSnmpHosts</td>
<td>Specifies the host names of the machines to which you want to send the SNMP trap. Separate multiple hosts with a semicolon. To add a specific port for each host, enter the host name followed by a colon and the port number.</td>
</tr>
<tr>
<td>Example</td>
<td>XAlertsmachine:7000;SNMPmachine;Scriptsmachine:7001</td>
</tr>
<tr>
<td>Default</td>
<td>null</td>
</tr>
<tr>
<td>XAlertsSend2Script</td>
<td>Specify the full path and file name of the script to be sent. This parameter is used only when the XAlertsSendSnmp system parameter is set to either 2 or 3.</td>
</tr>
<tr>
<td>Default</td>
<td>null</td>
</tr>
<tr>
<td>CmsXAlertsHost</td>
<td>Specify the host or IP address on which the CMS is forced to receive XAlerts.</td>
</tr>
<tr>
<td>Note</td>
<td>If no value is entered for this parameter, the host name on which the CMS is installed is used.</td>
</tr>
<tr>
<td>Default</td>
<td>null</td>
</tr>
<tr>
<td>CmsXAlertsPort</td>
<td>Specify the port through which the XAlerts are received.</td>
</tr>
<tr>
<td>Default</td>
<td>0</td>
</tr>
<tr>
<td>Note</td>
<td>The default value 0 means that any random port is used.</td>
</tr>
<tr>
<td>XAlertsDisableMsgIDs</td>
<td>Specify the message IDs for which no XAlerts are sent. By default, no message IDs are listed. Use a comma to separate multiple message IDs.</td>
</tr>
<tr>
<td>Default</td>
<td>none</td>
</tr>
<tr>
<td>XAlertsMinSeverityFilter</td>
<td>Specify the severity level filter. XAlerts with a value equal to or greater than the specified severity level are sent to the Exception Alerts window.</td>
</tr>
<tr>
<td>Valid values:</td>
<td><img src="https://example.com" alt="Warning" /> ■ Error ■ Severe</td>
</tr>
<tr>
<td>Default</td>
<td>Warning</td>
</tr>
<tr>
<td>MaxXAlertsSend2Client</td>
<td>Note: Do not change this parameter unless instructed to do so by BMC Software Customer Support.</td>
</tr>
<tr>
<td></td>
<td>Determines the maximum number of exception alerts sent from the CMS to the Exception Alerts window.</td>
</tr>
<tr>
<td>Default</td>
<td>2000</td>
</tr>
</tbody>
</table>
**CMS parameters**

Table 79  **Configuration Management Server (CMS) parameters**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AdminRequestTimeout</td>
<td><strong>Note:</strong> Do not change this parameter unless instructed to do so by BMC Software Customer Support. If you are instructed to change this parameter, you must restart the CMS for the change to take effect.</td>
</tr>
</tbody>
</table>
| CmsCommMode                | The mode with which the Configuration Management Server connects to the CONTROL-M/Server Configuration Agent.  
**Valid values:**  
- **TCP** - A non-secure connection is established.  
- **SSL** - Connect using SSL only.  
- **Auto** - The system automatically detects the type of connection that is established.  
**Default:** TCP |
| CmsCtmRefreshInterval      | The Configuration Management Server (CMS) refreshes the status and topology of the CONTROL-M/Servers on a regular basis. This system parameter governs the length of time in seconds between each refresh episode.  
**Default:** 60 |
| CmsEmRefreshInterval       | The CMS refreshes its internal image of CONTROL-M/EM component status on a regular basis. This system parameter governs the length of time in seconds between each refresh episode.  
**Default:** 60 |
| CmsGateAdditionalParams    | **Note:** Do not change this parameter unless instructed to do so by BMC Software Customer Support. |
| DeletedJobsLoadLimit       | The maximum number of deleted jobs to be displayed to the user. If the number of deleted jobs exceeds this value, the more recently deleted jobs are displayed.  
**Default:** 2000 |
| MaxTableJobsToAudit        | The maximum number of jobs in the scheduling table to be audited.  
**Default:** 1000 |
| RemoteCmdTimeout           | The amount of time, in seconds, that the CMS will wait for a reply to a remote request sent through the Configuration Management Server to CONTROL-M/Server, CONTROL-M/Agent, and Control Modules, before timing out.  
An example of such a request is a ping agent request.  
**Default:** 300 |
### Table 79  Configuration Management Server (CMS) parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RunInfoStatsPurgeDays</td>
<td>The number of days to retain deleted statistics, after which the statistics will be deleted when automatic purge is performed. Default: 100 days</td>
</tr>
<tr>
<td>RunInfoStatsPurgeInterval</td>
<td>Interval, in minutes, between activations of automatic purging of periodic statistics the CMS. Note: To disable automatic purging, set the value to 0. Default: 30</td>
</tr>
<tr>
<td>VMCleanupIntervalMinutes</td>
<td>Interval, in minutes, between activations of automatic job history cleanup by the CMS. Note: To disable automatic cleanup, set the value to 0. Default: 30</td>
</tr>
<tr>
<td>VMMaxDaysRetainCurJobsHistory</td>
<td>The number of days after which the history of the current jobs should be deleted automatically. Note: A job version is deleted only when all of the following are true: The version exceeds VMVersionsNumberToKeep. The version exceeds VMMaxDaysRetainCurJobsHistory. Automatic cleanup has run, as determined by VMCleanupIntervalMinutes. For more information, see “Implementing job version management” on page 105. Default: 0</td>
</tr>
<tr>
<td>VMNumDaysRetainDeletedJobs</td>
<td>The number of days to retain deleted jobs and their history. Deleted tables will also be deleted according to this value. Default: 180</td>
</tr>
</tbody>
</table>

### CONTROL-M/EM parameters in the Defaults.rsc file

---

**NOTE**  
The tables in this section list the parameters located in the Defaults.rsc file. For instructions on modifying these parameters, see “Editing the Defaults.rsc file” on page 405.
### Table 80  Gateway parameters in the defaults.rsc file (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>bulk_batch_size</td>
<td>Indicates how many job and resource details the gateway should load into memory at a time before saving the entities in the CONTROL-M/EM database when performing a download from CONTROL-M. A larger number causes the download to occur faster and more efficiently, at the expense of virtual memory.</td>
</tr>
<tr>
<td></td>
<td>Default: 100</td>
</tr>
<tr>
<td>continue_not_responding</td>
<td>Indicates how the new gateway handles multiple gateway instances for the same CONTROL-M installation if all attempts to stop and kill the original gateway are unsuccessful.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ Y- Both gateway occurrences are allowed to run concurrently. This is not recommended.</td>
</tr>
<tr>
<td></td>
<td>■ N- The original gateway continues in its “hubg” state. The new gateway stops running.</td>
</tr>
<tr>
<td></td>
<td>Default: N</td>
</tr>
<tr>
<td>dal_rel_cache_size</td>
<td>This only when instructed by BMC Software technical support.</td>
</tr>
<tr>
<td>dal_select_min_bulksize</td>
<td>These parameters indicate the bulk size being used by the database access layer during bulk insert and choose SQL operation. Larger numbers cause the insert and choose SQL operations to occur faster and more efficiently, at the expense of virtual memory.</td>
</tr>
<tr>
<td>dal_select_max_bulksize</td>
<td></td>
</tr>
<tr>
<td>dal_insert_min_bulksize</td>
<td></td>
</tr>
<tr>
<td>dal_insert_max_bulksize</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Default:</td>
</tr>
<tr>
<td></td>
<td>dal_select_min_bulksize: 10</td>
</tr>
<tr>
<td></td>
<td>dal_select_max_bulksize:</td>
</tr>
<tr>
<td></td>
<td>■ MSSQL: 20</td>
</tr>
<tr>
<td></td>
<td>dal_insert_min_bulksize: 10</td>
</tr>
<tr>
<td></td>
<td>dal_insert_max_bulksize:</td>
</tr>
<tr>
<td>ecs_connect_method</td>
<td>Indicates in which mode the gateway opens communication connections.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ 1 - The gateway establishes connections in blocking mode.</td>
</tr>
<tr>
<td></td>
<td>■ 2 - The gateway establishes connections in non-blocking mode.</td>
</tr>
<tr>
<td>gtw_send_ctl_timeout</td>
<td>Timeout period, in seconds, for determining if the original gateway is responsive (up).</td>
</tr>
<tr>
<td></td>
<td>Default: 45</td>
</tr>
</tbody>
</table>
This section lists and describes the following categories of CONTROL-M/Server parameters:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>kill_not_responding</td>
<td>Indicates whether a new gateway stops or kills existing gateway instances for the same CONTROL-M installation.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ Y - The new gateway tries to kill the original gateway and, if successful, continues to run. If the original gateway cannot be killed, the new gateway handles the original gateway according to the continue_not_responding parameter.</td>
</tr>
<tr>
<td></td>
<td>■ N - The new gateway tries to stop the original gateway (using the cutil utility) and, if successful, continues to run. If the original gateway is not stopped after 3 attempts, the new gateway handles the original gateway according to the continue_not_responding parameter.</td>
</tr>
<tr>
<td>Default: N</td>
<td></td>
</tr>
<tr>
<td>nonBlockTimeout</td>
<td>If a gateway is in non-block mode and part of a message is not received during the number of seconds specified in this parameter, the gateway assumes communication is down.</td>
</tr>
<tr>
<td>Default: 40.</td>
<td>This parameter is relevant only if the useNonBlock parameter is set to Y.</td>
</tr>
<tr>
<td>useNonBlock</td>
<td>Indicates whether the gateway operates in blocking mode or non-blocking mode. This mode determines whether the gateway receives entire messages or parts of messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ N - The gateway waits and receives for the entire message to arrive in blocking mode, regardless of length of time.</td>
</tr>
<tr>
<td></td>
<td>■ Y - The gateway receives parts of messages (non-blocking mode). Communication is assumed to be down if part of a message is not received within the time interval specified in the nonBlockTimeout field.</td>
</tr>
<tr>
<td>Default: N</td>
<td></td>
</tr>
</tbody>
</table>

### CONTROL-M/Server parameters

This section lists and describes the following categories of CONTROL-M/Server parameters:

<table>
<thead>
<tr>
<th>Server parameter category</th>
<th>Page reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>system</td>
<td>454</td>
</tr>
<tr>
<td>communication</td>
<td>459</td>
</tr>
<tr>
<td>operational</td>
<td>462</td>
</tr>
<tr>
<td>Agent communication</td>
<td>464</td>
</tr>
<tr>
<td>database</td>
<td>467</td>
</tr>
</tbody>
</table>
## System parameters

Table 81 lists the CONTROL-M/Server system parameters. These parameters are assigned default values during installation. For some of the parameters, you can use the `ctmsys` utility to change the parameter value.

### Table 81  CONTROL-M/Server system parameters (part 1 of 5)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Shout Table</td>
<td>currently active Shout Destination table</td>
</tr>
<tr>
<td>Default: SYSTEM</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Automatic</td>
<td></td>
</tr>
<tr>
<td>Computer System</td>
<td>computer type and model where CONTROL-M/Server is installed (for example, HP700)</td>
</tr>
<tr>
<td>CONTROL-M Date</td>
<td>date that CONTROL-M/Server regards as the actual working date (Odate)</td>
</tr>
<tr>
<td>To determine this date, CONTROL-M/Server uses the operating system date and the value of the Day Time parameter (listed in this table).</td>
<td></td>
</tr>
<tr>
<td>Note: The New Day procedure updates this value each time the procedure runs.</td>
<td></td>
</tr>
<tr>
<td>Valid Values: dates in the format <code>yyyyymmd</code> (for example, 20080215 for February 15, 2008)</td>
<td></td>
</tr>
<tr>
<td>Default: <code>00000000</code> at installation</td>
<td></td>
</tr>
<tr>
<td>CONTROL-M Version</td>
<td>version number of the CONTROL-M/Server</td>
</tr>
<tr>
<td>Database Version/Schema</td>
<td>internal database schema version number</td>
</tr>
<tr>
<td>Note: This number is not the Sybase or MSSQL version number.</td>
<td></td>
</tr>
</tbody>
</table>
Table 81  CONTROL-M/Server system parameters (part 2 of 5)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Day Time</td>
<td>start-of-day time that CONTROL-M uses</td>
</tr>
<tr>
<td></td>
<td>This time is when the CONTROL-M date (Odate) changes and the New Day</td>
</tr>
<tr>
<td></td>
<td>procedure runs.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid Values</strong>: either of the following formats (where ( hh ) indicates</td>
</tr>
<tr>
<td></td>
<td>hours and ( mm ) indicates minutes):</td>
</tr>
<tr>
<td></td>
<td>-  ( +hhmm ) changes the CONTROL-M date at the specified time after</td>
</tr>
<tr>
<td></td>
<td>midnight.</td>
</tr>
<tr>
<td></td>
<td>-  ( -hhmm ) changes the CONTROL-M date at the specified time before</td>
</tr>
<tr>
<td></td>
<td>midnight.</td>
</tr>
<tr>
<td></td>
<td>These values reflect 24-hour time. For example, 2200 is equivalent to 10 P.</td>
</tr>
<tr>
<td></td>
<td><strong>Examples</strong></td>
</tr>
<tr>
<td></td>
<td>If you use ( +0600 ), the hours between midnight and 6:00 A.M. are</td>
</tr>
<tr>
<td></td>
<td>considered part of the previous date’s work day. Thus, system date February</td>
</tr>
<tr>
<td></td>
<td>10, 5:59 A.M. is considered part of the February 9 work day.</td>
</tr>
<tr>
<td></td>
<td>If you use ( -2200 ), the hours between 10 P.M. and midnight are</td>
</tr>
<tr>
<td></td>
<td>considered part of the next date’s work day. Thus, at 10:00 P.M. on</td>
</tr>
<tr>
<td></td>
<td>system date February 10, the CONTROL-M date changes to February 11.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: ( +0700 )</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set</strong>: Use the ctmsys utility to change the parameter</td>
</tr>
<tr>
<td></td>
<td>value.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type</strong>: Automatic</td>
</tr>
<tr>
<td>Executable Path</td>
<td>location where CONTROL-M/Server expects to find all of its executable</td>
</tr>
<tr>
<td></td>
<td>programs (for example, /usr/controlm/ctm_server/exe_Solaris)</td>
</tr>
<tr>
<td>Full Security</td>
<td>whether CONTROL-M operates with a restricted or unrestricted level of</td>
</tr>
<tr>
<td></td>
<td>security</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: A user for whom one or more authorizations have been assigned in</td>
</tr>
<tr>
<td></td>
<td>the security database can perform only the actions for which the user is</td>
</tr>
<tr>
<td></td>
<td>specifically authorized.</td>
</tr>
<tr>
<td></td>
<td>( Y ) (restricted) means a user who is not defined in the CONTROL-M</td>
</tr>
<tr>
<td></td>
<td>security database does not have any application authorizations.</td>
</tr>
<tr>
<td></td>
<td>( N ) (unrestricted) means a user who is not defined in the CONTROL-M</td>
</tr>
<tr>
<td></td>
<td>security database is regarded as having all application authorizations.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong>: ( N )</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type</strong>: Automatic</td>
</tr>
</tbody>
</table>

Appendix B  System parameters  455
### Table 81  CONTROL-M/Server system parameters (part 3 of 5)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ignore New Day Conditions</td>
<td>whether the New Day procedure should ignore prerequisite conditions if their reference date (day and month) matches the CONTROL-M date + 1. <strong>How / where to set:</strong> Use the ctmsys utility to change the parameter value. <strong>Refresh Type:</strong> Automatic</td>
</tr>
</tbody>
</table>
| Max. Days to Retain Sysout Files | number of days that job SYSOUT files are retained for jobs executed by agent computers  
  
  After this period, the New Day procedure deletes all job SYSOUT files.  
  
  This parameter also affects the number of days that old nets are saved. To view SYSOUT files of jobs in old nets, in some cases SYSOUT files must be saved for an extra calendar day.  
  
  **Default:** 1  
  
  **How / where to set:** Use the ctmsys utility to change the parameter value. **Refresh Type:** Automatic |
| Maximum Days Retained by CONTROL-M Log | The maximum number of days that entries are retained in the CONTROL-M log before the New Day cleanup procedure deletes them  
  
  **Note:**  
  
  If this value exceeds 2, the syslogs might run out of space. Either delete the transaction log or use ALTER DATABASE to increase the size of the segment.  
  
  For Sybase, if this value exceeds 4, increase the size of the temporary database. BMC recommends using the following formula to determine the optimum size for the database: 6% of the data portion size of the database multiplied by the number of days to retain entries.  
  
  For example, if the data device size is 400 MB and you want to retain history for 10 days, enlarge the temporary database to 240 MB. For more information, see “Extending the CONTROL-M/Server database” on page 309  
  
  **Default:** 2  
  
  **How / where to set:** Use the ctmsys utility to change the parameter value. **Refresh Type:** Automatic |
| Maximum Retries | The number of times that the CONTROL-M auto-recovery mechanism can reactivate CONTROL-M/Server processes when a failure occurs  
  
  If this number is exceeded, CONTROL-M/Server shuts down.  
  
  **Default:** 10  
  
  **How / where to set:** Use the ctmsys utility to change the parameter value. |
Table 81  CONTROL-M/Server system parameters (part 4 of 5)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Operating System</td>
<td>An operating system that is running on the server computer (for example, AIX)</td>
</tr>
</tbody>
</table>

**Valid Values:**

- **INACTIVE**—CONTROL-M/Server works in non-SSL mode. If CONTROL-M/Agent is in SSL mode, the server tries to switch that agent to non-SSL mode.

- **DISABLED**—CONTROL-M/Server works in non-SSL mode. If CONTROL-M/Agent is in SSL mode, the server does not try to switch that agent to non-SSL mode.

- **ENABLED**—CONTROL-M/Server works in SSL mode.

**Default:** Disabled

**How / where to set:** In the CONTROL-M Main Menu, choose Parameter Customization => System Parameters and Shout Destination Tables => System Parameters => Next Page => Secure Sockets Layer. The parameter that is updated is the CTM_CONFIG_AGENT_SSL_ENBL parameter. For more information, see “Using the Main menu” on page 406.

**Refresh Type:** manual
### Table 81  CONTROL-M/Server system parameters (part 5 of 5)

<table>
<thead>
<tr>
<th>Parameter Name</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Start Day of the Week</strong></td>
<td>Day on which the work week starts at your site</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter affects the <strong>Weekdays</strong> job processing parameter</td>
</tr>
<tr>
<td></td>
<td>(discussed in the <em>CONTROL-M User Guide</em>).</td>
</tr>
<tr>
<td></td>
<td><strong>Valid Values:</strong> 0 (Saturday) through 6 (Friday)</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2 (Monday)</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> Use the ctmsys utility to change the parameter value.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Automatic</td>
</tr>
<tr>
<td><strong>Statistics</strong></td>
<td>Whether job statistics should be written to the CONTROL-M/Server database</td>
</tr>
<tr>
<td></td>
<td>For more information, see “Job statistics generated by CONTROL-M/Server” on page 93 and “Implementing job statistics generated by CONTROL-M/Server” on page 122</td>
</tr>
<tr>
<td></td>
<td><strong>Y</strong> tells CONTROL-M to record job statistics.</td>
</tr>
<tr>
<td></td>
<td><strong>N</strong> tells CONTROL-M not to record job statistics.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Y</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> Use the ctmsys utility to change the parameter value.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Automatic</td>
</tr>
</tbody>
</table>
## Communication parameters

Tables 82 and 83 list the CONTROL-M/Server communication parameters.

### Table 82  CONTROL-M/Server communication parameters (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Agent-to-Server Port Number</strong></td>
<td>The listening port number of the NS process (not to be used for any other purpose in the server computer). CONTROL-M/Server communicates with CONTROL-M/Agent using two TCP/IP ports. CTMS_PORT_NUM specifies the port for data flowing from CONTROL-M/Server to CONTROL-M/Agent. The other port is specified using <strong>Server-to-Agent Port Number</strong> parameter (described in “Agent communication parameters” on page 464). Note: This number must match the value assigned to the <strong>Agent-to-Server Port Number</strong> parameter on the agent computer.</td>
</tr>
<tr>
<td><strong>Valid Values:</strong></td>
<td>1024–65534</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>7447 (On UNIX, the default value is overridden during the value given during installation.)</td>
</tr>
<tr>
<td><strong>How / where to set:</strong></td>
<td>In the CONTROL-M Main Menu, choose Parameter Customization =&gt; Basic Communication and Operational Parameters =&gt; Agent to Server Port. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td><strong>Refresh Type:</strong></td>
<td>Recycle</td>
</tr>
<tr>
<td><strong>Communication Protocol</strong></td>
<td>Protocol used to communicate with the agent computers. (The protocol specified here must be the same as that specified on the agent computer.)</td>
</tr>
<tr>
<td><strong>Valid Values:</strong></td>
<td>TCP</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>TCP</td>
</tr>
<tr>
<td><strong>How / where to set:</strong></td>
<td>For UNIX, see “Editing the config.dat file” on page 408. For Windows, edit the Communication Protocol registry parameter.</td>
</tr>
<tr>
<td><strong>Refresh Type:</strong></td>
<td>Recycle</td>
</tr>
<tr>
<td><strong>EM Gateway Port</strong></td>
<td>port number that CONTROL-M/Server uses to listen for communication from CONTROL-M/EM</td>
</tr>
<tr>
<td><strong>Valid Values:</strong></td>
<td>1025–32767</td>
</tr>
<tr>
<td><strong>Refresh Type:</strong></td>
<td>Recycle</td>
</tr>
</tbody>
</table>
### Table 82  CONTROL-M/Server communication parameters (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Inter Process Communication (IPC) Port Number</strong></td>
<td>The listening port number of the RT process.</td>
</tr>
<tr>
<td>Valid Values</td>
<td>1025–32767</td>
</tr>
<tr>
<td>Default</td>
<td>6005</td>
</tr>
<tr>
<td>How / where to set</td>
<td>In the CONTROL-M Main Menu, choose Parameter Customization =&gt; Basic Communication and Operational Parameters =&gt; IPC Port. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td>Refresh Type</td>
<td>Recycle</td>
</tr>
<tr>
<td><strong>Local IP Host Interface Name</strong></td>
<td>host interface name of the TCP/IP network interface card on the server computer to use for communication with CONTROL-M/EM</td>
</tr>
<tr>
<td>Valid Values</td>
<td>host name, or host IP address (for example, 192.123.186.20)</td>
</tr>
<tr>
<td>Default</td>
<td>the default host interface name defined in the server computer operating environment</td>
</tr>
<tr>
<td><strong>Configuration Agent Port</strong></td>
<td>port number for the CONTROL-M/Server Configuration Agent</td>
</tr>
<tr>
<td>Valid Values</td>
<td>1025–32767</td>
</tr>
<tr>
<td>Default</td>
<td>2369</td>
</tr>
<tr>
<td>Refresh Type</td>
<td>Recycle</td>
</tr>
<tr>
<td><strong>CD_MAX_DBU</strong></td>
<td>When there is no current CONTROL-M/EM session, CONTROL-M accumulates database updates before downloading them to CONTROL-M/EM. <strong>CD_MAX_DBU</strong> determines the maximum number of updates to accumulate before requesting a download.</td>
</tr>
<tr>
<td>Valid Values</td>
<td>100–2^31</td>
</tr>
<tr>
<td>Default</td>
<td>1000</td>
</tr>
<tr>
<td>How / where to set</td>
<td>In the CONTROL-M Main Menu, choose Parameter Customization =&gt; Advanced Communication and Operational Parameters =&gt; Maximum Job State Changes. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td>Refresh Type</td>
<td>Manual</td>
</tr>
</tbody>
</table>
Table 82  CONTROL-M/Server communication parameters (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTM_PRM_KPA_ACTIVE</td>
<td>Whether the Heartbeat monitor operates in active or passive mode. (For more information, see “Heartbeat monitor and Watchdog facility” on page 266 and “Implementing Heartbeat Monitors and the Watchdog facility” on page 275.)</td>
</tr>
<tr>
<td></td>
<td>Valid Values: Y (for active) or N (for passive)</td>
</tr>
<tr>
<td></td>
<td>Default: Y</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Recycle</td>
</tr>
<tr>
<td>CTM_PRM_KPA_BETWEEN_MSGS</td>
<td>Time in seconds between heartbeat checks</td>
</tr>
<tr>
<td></td>
<td>Valid Values: 1–2(^{31}) (integer)</td>
</tr>
<tr>
<td></td>
<td>Default: 300</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Recycle</td>
</tr>
<tr>
<td>CTM_PRM_KPA_ROUND_TRIP_TIMEOUT</td>
<td>Time in seconds to wait for a confirmation from CONTROL-M/EM</td>
</tr>
<tr>
<td></td>
<td>If confirmation does not arrive, a timeout is generated and the connection is severed.</td>
</tr>
<tr>
<td></td>
<td>Valid Values: any integer</td>
</tr>
<tr>
<td></td>
<td>Default: 300</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Recycle</td>
</tr>
</tbody>
</table>
### Table 83  CONTROL-M/Server communication and debug parameters

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Description</th>
</tr>
</thead>
</table>
| COMTIMEOUT     | Communication timeout in seconds  
| Valid Values: 10–2³¹  
| Default: 60 (seconds)  
| How / where to set: In the CONTROL-M Main Menu, choose Parameter Customization => Default Parameters for Communicating with Agent Platforms => Communication Timeout. For more information, see “Using the Main menu” on page 406.  
| Refresh Type: Recycle |
| COMTRYNO       | Communication retry value  
| Valid Values: 1–2³¹ (seconds)  
| Default: 5  
| How / where to set: In the CONTROL-M Main Menu, choose Parameter Customization => Default Parameters for Communicating with Agent Platforms => Maximum Retries. For more information, see “Using the Main menu” on page 406.  
| Refresh Type: Recycle |
| OS_PRM_HOSTNAME | Used in various ways, for example, the name of the server to be sent to the Agent, for later comparison with the Agent's permitted server list.  
| Valid Values: 255 characters  
| Default: gethostname  
| How / where to set:  
| ■ (UNIX) In the CONTROL-M Main Menu, choose Parameter Customization => Basic Communication and Operational Parameters => Local IP host interface name. For more information, see “Using the Main menu” on page 406.  
| ■ (UNIX or Windows) See “Editing the config.dat file” on page 408.  
| Refresh Type: Recycle |

### Operational parameters

Table 84 lists the general CONTROL-M/Server operational parameters.
Table 84  CONTROL-M/Server operational parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| CONTROL-M/EM TCP/IP Port Number | CONTROL-M communicates with CONTROL-M/EM using a pair of consecutive TCP/IP ports (for example, 2370 and 2371). The lower port is used for data flowing from CONTROL-M to CONTROL-M/EM. The higher port is used for data flowing in the reverse direction.

This parameter is used to specify the lower of the two port numbers and must correspond to the value assigned to field TCP/IP Port Number in the definition of the CONTROL-M data center in the CONTROL-M Definition dialog box in the CONTROL-M Configuration Manager. Verify that the two port numbers are not used for any other purpose on the server computer.

**Valid Values:** between 1025 and 32767 inclusive.

**Default:** 2370

**Refresh Type:** Recycle

| Maximum Job State Changes | Number of job state changes retained by CONTROL-M/Server in the event communication with CONTROL-M/EM is interrupted. If the number of job state changes that occur exceeds the value specified for this parameter, CONTROL-M/Server will initiate a download when communication with CONTROL-M/EM is resumed.

**Default:** 1000

| Maximum Server Processes | Maximum number of communication server (CS) processes that communicate with the CONTROL-M/Server gateway process concurrently.

**Default:** 2

| Minimum Server Processes | Minimum number of communication server (CS) processes that communicate with the CONTROL-M/Server gateway process concurrently.

**Default:** 2
Table 84  CONTROL-M/Server operational parameters (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| Number of Tracker Worker Threads (TRACKER_WORKE\_RS\_NUM) | This parameter determines the number of worker threads available for the tracker process at startup.  
  Valid Values: 1–100  
  Default: 5  
  How / where to set: See “Editing the config.dat file” on page 408.  
  Refresh Type: Recycle |
| Maximum Number of Tracker Worker Threads (TRACKER_MAX_WORKE\_RS\_NUM) | Determines the maximum number of worker threads that the tracker can create.  
  Valid Values:  
  ■ Minimum: TRACKER_WORKE\_RS\_NUM  
  ■ Maximum: 100  
  Default: 20  
  How / where to set: See “Editing the config.dat file” on page 408.  
  Refresh Type: Recycle |
| Statistics Mode                                     | Mode used by the ctmjsa utility to collect summary statistics. JOBNAME compiles statistics for each CONTROL-M Job Name/Scheduling Table and Node ID where the job was submitted. MEMNAME compiles statistics for each CONTROL-M Mem Name/Mem Lib and Node ID.  
  Valid Values: MEMNAME, JOBNAME  
  Default: MEMNAME  
  How / where to set: Perform one of the following:  
  ■ “Defining the CONTROL-M/Server statistics collection mode” on page 123  
  ■ “Editing the config.dat file” on page 408  
  Refresh Type: Manual |

Agent communication parameters

Table 85 lists the CONTROL-M/Server parameters for communicating with agent computers.

The values specified for these parameters are used as the default values for communication with each agent computer. You can change values for specific agent computers individually.
### Table 85  CONTROL-M/Server parameters for communicating with agent computers (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Allow Agent Disconnection** | Set the ALLOW_AG_DISCONNECTION parameter to determine if the current connection to this AGT can be disconnected when MAX_CONCURRENT_SESSIONS is reached.  
*Valid Values:* Y and N  
*Default:* Y |
| **Check Interval**         | Interval (in seconds) between status checks for each CONTROL-M/Agent that communicates with CONTROL-M/Server.  
*Default:* 7200 (2 hours) |
| **Communication Protocol Version** | Version of CONTROL-M/Agent.  
*Valid values:*  
  - 06 – 6.1.0x and 6.2.0x  
  - 07 – 6.3.0x  
  - 08 - 6.4.0x  
*Default:* 08 |
| **Communication Timeout**  | Maximum length of time (in seconds) that CONTROL-M/Server should spend attempting to communicate with an agent computer before assigning it Unavailable status.  
During this time, CONTROL-M/Server attempts to communicate with the agent computer x times, where x is the value specified by parameter Maximum Retries.  
*Example*  
If the value of Communication Timeout is 120 and Maximum Retries is 12, CONTROL-M/Server attempts to communicate with the agent computer once every 10 seconds (120/12) during the timeout period.  
*Default:* 120 |
### Table 85  CONTROL-M/Server parameters for communicating with agent computers (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Maximum Concurrent Sessions</strong></td>
<td>Indicates the maximum number of concurrent sessions that the NS process will hold. Once the maximum of the MAX_CONCURRENT_SESSIONS parameter is reached, the session with the maximum idle time will be terminated in order to open a new connection. If this agent connection is marked as not allowed to be disconnected (see the ALLOW_AG_DISCONNECTION parameter) then the next one in line will be disconnected. <strong>Valid Values:</strong> All integers in the range of 16 to the maximum available according to the operating system. <strong>Default:</strong> 256</td>
</tr>
<tr>
<td><strong>Maximum Disconnect Time</strong></td>
<td>Sets the maximum time in which the NS allows an agent to be disconnected before it will initiate a session with it (although there’s nothing to submit to it). The MAX_DISCONNECT_TIME parameter is relevant only if the ALLOW_COMM_INIT parameter on the agent is set to <strong>NO</strong>. <strong>Valid Values:</strong> integers in the range 30 - 86400 (in seconds) <strong>Default:</strong> 300</td>
</tr>
<tr>
<td><strong>Maximum Retries</strong></td>
<td>Number of communication retries to attempt in the period of time specified before assigning the Unavailable status to an agent computer. <strong>Default:</strong> 12</td>
</tr>
<tr>
<td><strong>Persistent Connection</strong></td>
<td>Indicates the persistent connection setting. Set the PERSISTENT_CONNECTION parameter to connect to a specific agent with either a persistent or transient connection. When <strong>Persistent Connection</strong> is set to <strong>Y</strong> (for example, with an agent version 6.2.01), the NS process creates a persistent connection with the agent and manages the session with this agent. If the connection is broken with an agent or NS is unable to connect with an agent, the agent is marked as <strong>Unavailable</strong>. When the connection with the agent is resumed, the NS recreates a persistent connection with the agent and marks the agent as <strong>Available</strong>. <strong>Valid Values:</strong> <strong>Y</strong> or <strong>N</strong> <strong>Default:</strong> <strong>N</strong> for a new agent installation and <strong>N</strong> for an agent that is known to CONTROL-M/Server before upgrading to version 6.2.01 and above.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>---------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Polling Interval</td>
<td>Time interval (in seconds) between requests from CONTROL-M/Server for status updates from agent computers that are executing jobs.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 900</td>
</tr>
<tr>
<td>Retry Interval</td>
<td>Length of time to wait (in seconds) between attempts to communicate with an agent computer whose status is Unavailable.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 90</td>
</tr>
<tr>
<td>Server-to-Agent Port Number</td>
<td>Port number in the agent computer through which data is received from the server computer. The value assigned to this parameter must correspond to the value assigned to the Server-to-Agent Port Number field in the Configuration file on the corresponding agent computer.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 7006</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>Session Idle Timeout</td>
<td>Indicates the maximum time a session can be in idle before NS terminates it.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid Values:</strong> integers in the range 30 - 86400 (in seconds)</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 900</td>
</tr>
<tr>
<td>Unavailability Shout Urgency</td>
<td>Indicates messages with a high priority sent from an agent assigned Unavailable status. Urgent message are sent with a special indication so that the recipient of the message is aware of the urgency.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> R, U, or V</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> R</td>
</tr>
</tbody>
</table>

### Database parameters

Database configuration parameters are specified during installation, before the CONTROL-M/Server database is created. You can subsequently change these parameters and rebuild the CONTROL-M/Server database by using the Database Creation menu, described in Chapter 11, “Maintaining databases and CONTROL-M data.”
This section lists configuration parameters for the following databases:

- Sybase (Table 86 on page 468)
- Oracle (Table 87 on page 471)
- MSSQL (Table 88 on page 473)
- PostgreSQL (Table 89 on page 475)

Table 86  CONTROL-M/Server database parameters for the Sybase environment (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-M Database Data Device Name</td>
<td>Name of Sybase device on which CONTROL-M/Server database will be created. Default: ctrlm_ux</td>
</tr>
<tr>
<td>CONTROL-M Database Log Device Name</td>
<td>Name of Sybase device on which CONTROL-M/Server database log will be created. Default: ctrlm_log</td>
</tr>
<tr>
<td>CONTROL-M Database Name</td>
<td>Name for the CONTROL-M/Server database. This name must be unique. Default: ctrlm</td>
</tr>
<tr>
<td>CONTROL-M Database Owner</td>
<td>Sybase name for the CONTROL-M/Server database owner. The custom script creates this user in the database. This name is used by CONTROL-M when accessing its database. Default: ctrlm</td>
</tr>
<tr>
<td>Data Device Type</td>
<td>Type of disk storage (raw partition or file system) used for the CONTROL-M/Server database. Default: FILE</td>
</tr>
<tr>
<td>Data Physical Device/Path Name</td>
<td>For Data Device Type FILE: Full path name where the CONTROL-M/Server database will be located. For Data Device Type RAW: Physical device name of the raw partition in which the CONTROL-M/Server database will be located. Default: /&lt;controlm_home_dir&gt;/sybase/data(ctrlm_ux.dat</td>
</tr>
</tbody>
</table>
### Table 86  CONTROL-M/Server database parameters for the Sybase environment (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Database (Data Portion) Size</td>
<td>Amount of space (in MB) to allocate for the data portion of the CONTROL-M/Server database.</td>
</tr>
<tr>
<td></td>
<td>If the database will be located in a file system, the custom script allocates the amount of space you specify plus an additional 33% to accommodate the Sybase transaction log. For example, if you specify 60 MB, the amount of space actually allocated is 80 MB.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 50</td>
</tr>
<tr>
<td>Database Administrator's Password</td>
<td>Password (6 to 30 characters, alphanumeric) for the Sybase database administrator (user sa). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M utilities to access restricted sections of the CONTROL-M/Server database.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> password</td>
</tr>
<tr>
<td>DBO Password</td>
<td>Sybase password for the CONTROL-M/Server database owner (6 to 30 characters, alphanumeric). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the CONTROL-M/Server database.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> password</td>
</tr>
<tr>
<td>Log Device Type</td>
<td>Type of disk storage (raw partition or file system) used for the CONTROL-M/Server database log.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> password</td>
</tr>
<tr>
<td>Log Physical Device/Path Name</td>
<td>For Log Device Type FILE: Full path name where the CONTROL-M/Server database log will be located.</td>
</tr>
<tr>
<td></td>
<td>For Log Device Type RAW: Physical device name of the raw partition in which the CONTROL-M/Server database log will be located.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> /&lt;controlm_home_dir&gt;/sybase/data/ctrlm_log.da</td>
</tr>
</tbody>
</table>
### Table 86  CONTROL-M/Server database parameters for the Sybase environment (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Master Device Type</strong></td>
<td>Type of disk storage (raw partition or file system) used for the master Sybase database. (A raw partition installation offers enhanced database integrity.) If you want Sybase to use a raw partition, type <code>y</code> in response to the prompt. An additional prompt will be displayed requesting the physical device name (described below). <strong>Default</strong>: FILE</td>
</tr>
<tr>
<td><strong>Master Physical Device/Path Name</strong></td>
<td>For Master Device Type FILE: Full path name where the master Sybase database will be located. For Master Device Type RAW: Physical device name of the raw partition on which the Sybase database will be located. <strong>Default</strong>: <code>&lt;controlm_home_dir&gt;/sybase/data/master.dat</code></td>
</tr>
<tr>
<td><strong>Query Socket Port Number</strong> and <strong>Backup Socket Port Number</strong></td>
<td>Sybase utilizes these two TCP/IP ports for communication between CONTROL-M and Sybase SQL Server. The port numbers must be different from each other. If these port numbers are already used by an existing application, choose other values, each in the range 1024 to 65534 inclusive. <strong>Default</strong>: 7102 and 7103 <strong>Refresh Type</strong>: Recycle</td>
</tr>
<tr>
<td><strong>Remote Sybase Host Name</strong></td>
<td>Name of the host for an existing Sybase Database server installation.</td>
</tr>
<tr>
<td><strong>Sybase Interface Directory</strong></td>
<td>Directory in which the Sybase interfaces file is located. This path should be visible to CONTROL-M.</td>
</tr>
<tr>
<td><strong>Sybase Server Name</strong></td>
<td>Name of the SQL server. When you choose to modify this value, the custom script reads the Sybase interfaces file and displays a list of the available SQL servers. Specify the name of an SQL server from the displayed list (contact your system administrator for this information). <strong>Default</strong>: SYBASE</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>CONTROL-M Database Instance name</strong></td>
<td>The name of the Oracle SQL server (1 to 8 characters, alphabetic plus “_”). Default: ctrlm</td>
</tr>
<tr>
<td><strong>CONTROL-M INDEX tablespace file location</strong></td>
<td>Full path name to the CONTROL-M INDEX tablespace file. Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlm/indx01.dbf</td>
</tr>
<tr>
<td><strong>CONTROL-M INDEX tablespace size</strong></td>
<td>Size of the CONTROL-M INDEX tablespace file. Default: 50 MB</td>
</tr>
<tr>
<td><strong>CONTROL-M Listener port number</strong></td>
<td>Oracle utilizes this TCP/IP port for communication between CONTROL-M and Oracle SQL Server. The port must be dedicated to this purpose. Choose a number in the range 1024 to 65534 inclusive. Default: 1521 Refresh Type: Recycle</td>
</tr>
<tr>
<td><strong>CONTROL-M RBS (Rollback Segment) tablespace file location</strong></td>
<td>Full path name to the CONTROL-M RBS tablespace file. Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlm/rbs01.dbf</td>
</tr>
<tr>
<td><strong>CONTROL-M RBS tablespace size</strong></td>
<td>Size of the CONTROL-M RBS tablespace file. Default: 50 MB</td>
</tr>
<tr>
<td><strong>CONTROL-M SYSTEM tablespace file location</strong></td>
<td>Full path name to the CONTROL-M SYSTEM tablespace file. Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlm/system01.dbf</td>
</tr>
<tr>
<td><strong>CONTROL-M SYSTEM tablespace size</strong></td>
<td>Size of the CONTROL-M SYSTEM tablespace file. Default: 50 MB</td>
</tr>
<tr>
<td><strong>CONTROL-M TEMP tablespace file location</strong></td>
<td>Full path name to the CONTROL-M TEMP tablespace file. Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlm/temp01.dbf</td>
</tr>
</tbody>
</table>
### Table 87  CONTROL-M/Server database parameters for the Oracle environment (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-M TEMP tablespace size</td>
<td>Size of the CONTROL-M TEMP tablespace file.</td>
</tr>
<tr>
<td>Default: 100 MB</td>
<td></td>
</tr>
<tr>
<td>Name of the first database log file</td>
<td>Full path name of the first database log file.</td>
</tr>
<tr>
<td>Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlm/log01.dbf</td>
<td></td>
</tr>
<tr>
<td>Name of the second database log file</td>
<td>Full path name of the second database log file.</td>
</tr>
<tr>
<td>Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlm/log02.dbf</td>
<td></td>
</tr>
<tr>
<td>Name of the Tablespace data file</td>
<td>Full path name of CONTROL-M/Server database data file.</td>
</tr>
<tr>
<td>Default: /&lt;controlm_home_dir&gt;/oracle/oradata/ctrlmdata.dbf</td>
<td></td>
</tr>
<tr>
<td>Oracle CDROM name</td>
<td>Name of CDROM device containing the Oracle installation CDROM.</td>
</tr>
<tr>
<td>Oracle home directory</td>
<td>Directory where Oracle binary files are stored.</td>
</tr>
<tr>
<td>Default: /&lt;controlm_home_dir&gt;/oracle</td>
<td></td>
</tr>
<tr>
<td>Oracle Server Host name</td>
<td>The host computer name of an existing Oracle server.</td>
</tr>
<tr>
<td>Oracle SYSTEM user password</td>
<td>Password of the Oracle SYSTEM user.</td>
</tr>
<tr>
<td>Size of CONTROL-M database log files</td>
<td>The size of each database log file. There are two files of equal size.</td>
</tr>
<tr>
<td>Default: 20 MB</td>
<td></td>
</tr>
<tr>
<td>Tablespace size</td>
<td>Total size of the CONTROL-M/Server database.</td>
</tr>
<tr>
<td>Default: 250 MB</td>
<td></td>
</tr>
</tbody>
</table>
### Table 87  CONTROL-M/Server database parameters for the Oracle environment (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tablespace User</td>
<td>Name of CONTROL-M/Server database user. Default: controlm</td>
</tr>
<tr>
<td>User Password</td>
<td>Password for the CONTROL-M/Server database user (6 to 30 characters, alphanumeric). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the CONTROL-M/Server database. Default: password</td>
</tr>
</tbody>
</table>

### Table 88  CONTROL-M/Server database parameters for the MSSQL environment (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Host Name</td>
<td>Host name of the machine where the SQL Server resides. If the dedicated SQL Server was installed, the value is the current machine. For a silent installation the value of this parameter is blank, and the installation procedure uses the name of the current machine.</td>
</tr>
<tr>
<td>Query Port Number</td>
<td>The database utilizes these two TCP/IP ports for communication between CONTROL-M/Server and the SQL Server. The port numbers must be different from each other. If these port numbers are already used by an existing application, choose other values, each in the range 1024 to 65534 inclusive. Default: 7102 and 7103</td>
</tr>
<tr>
<td>Backup Port Number</td>
<td>Refresh Type: Recycle</td>
</tr>
<tr>
<td>System Administrator (SA)</td>
<td>Password (6 to 30 alphanumeric characters) for the database administrator (user sa). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M/Server utilities to access restricted sections of the CONTROL-M/Server database. Default: password</td>
</tr>
<tr>
<td>Database Name</td>
<td>Name for the CONTROL-M/Server database. This name must be unique. Default: ctrlm</td>
</tr>
</tbody>
</table>
### Table 88  CONTROL-M/Server database parameters for the MSSQL environment (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONTROL-M/Server Database Owner</strong></td>
<td>Database name for the CONTROL-M/Server database owner. The installation</td>
</tr>
<tr>
<td></td>
<td>script creates this user in the database. This name is used by</td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/Server when accessing its database.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> ctrlm</td>
</tr>
<tr>
<td><strong>CONTROL-M/Server Database Owner (DBO) Password</strong></td>
<td>Password for the CONTROL-M/Server database owner (6 to 30 alphanumeric</td>
</tr>
<tr>
<td></td>
<td>characters). The characters you enter are not echoed for security reasons.</td>
</tr>
<tr>
<td></td>
<td>The first character must be a letter (A – Z). This password is used by</td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/Server processes and utilities to access the</td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/Server database.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> password</td>
</tr>
<tr>
<td><strong>Data Device Logical Name</strong></td>
<td>Name of the device on which the CONTROL-M/Server database will be</td>
</tr>
<tr>
<td></td>
<td>located.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> ctrlm_ux</td>
</tr>
<tr>
<td><strong>Data Device Path</strong></td>
<td>Full path name for the CONTROL-M/Server database.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> c:&lt;sql_dir&gt;\data\ctrlm_ux</td>
</tr>
<tr>
<td><strong>Data Device Size</strong></td>
<td>Amount of space (MB) to allocate for the data portion of the</td>
</tr>
<tr>
<td></td>
<td>CONTROL-M/Server database.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 75 (MB)</td>
</tr>
<tr>
<td><strong>Log Device Logical Name</strong></td>
<td>Name of the device on which the CONTROL-M/Server database log will be</td>
</tr>
<tr>
<td></td>
<td>located.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> ctrlm_log</td>
</tr>
</tbody>
</table>
Table 88  CONTROL-M/Server database parameters for the MSSQL environment (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log Device Location</td>
<td>Full path name where the CONTROL-M/Server database log will be located.</td>
</tr>
<tr>
<td></td>
<td>Default: <code>c:\&lt;sql_dir&gt;\data\ctrlm_log</code></td>
</tr>
<tr>
<td>Log Device Size</td>
<td>Amount of space (MB) to allocate for the CONTROL-M/Server database log.</td>
</tr>
<tr>
<td></td>
<td>Default: 25 (MB)</td>
</tr>
</tbody>
</table>

Table 89  CONTROL-M/Server database parameters for the PostgreSQL environment (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Interface Name</td>
<td>Host name of the machine where the PostgreSQL Server resides. If the dedicated PostgreSQL Server was installed, the value is the current machine. For a silent installation the value of this parameter is blank, and the installation procedure uses the name of the current machine.</td>
</tr>
<tr>
<td>Port Number</td>
<td>The database utilizes this TCP/IP port for communication between CONTROL-M/Server and the PostgreSQL Server. If this port number is already used by an existing application, choose another value, in the range 1024 to 65534 inclusive. Default: 5432</td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
<tr>
<td>Database Administrator (postgres) Password</td>
<td>Password for the database administrator (user postgres). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M/Server utilities to access restricted sections of the CONTROL-M/Server database.  Note: The single apostrophe symbol (‘ ’) is not permitted for PostgreSQL.</td>
</tr>
<tr>
<td>CONTROL-M/Server Database Name</td>
<td>Name for the CONTROL-M/Server database. This name must be unique, and must contain up to 30 alphanumeric lowercase characters (including the underscore character).</td>
</tr>
<tr>
<td>CONTROL-M/Server Database Owner</td>
<td>Database name for the CONTROL-M/Server database owner. The installation script creates this user in the database. This name is used by CONTROL-M/Server when accessing its database.</td>
</tr>
</tbody>
</table>
CONTROL-M/Server parameters

### Table 89  CONTROL-M/Server database parameters for the PostgreSQL environment (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CONTROL-M/Server Database Owner (DBO) Password** | Password for the CONTROL-M/Server database owner. This name must be unique, and must contain up to 30 alphanumeric lowercase characters (including the underscore character). The characters you enter are not echoed for security reasons. The first character must be a letter. This password is used by CONTROL-M/Server processes and utilities to access the CONTROL-M/Server database.  
  
  **Note:** The single apostrophe symbol (‘ ‘) is not permitted for PostgreSQL. |
| **Database Scalability**            | Amount of resources in the operating system of the computer on which the PostgreSQL server is employed.  
  
  **Valid values:**  
  ■ Small  
  ■ Medium  
  ■ Large |
| **Database Server Home Directory (Windows only)** | Full path name of the location in which the PostgreSQL database server resides: `<CONTROL-M/Server path>/pgsql`.  
  
  **Note:** Only for PostgreSQL database server on Windows. |
| **Database Location (UNIX only)**   | Full path name of the location in which the CONTROL-M/Server database should be installed: `$PGHOME`  
  
  You must create this location prior to installing the CONTROL-M/Server database.  
  
  **Note:** Only for PostgreSQL database server on UNIX. |

**MIRRDRING parameters**

Parameters for database mirroring (Table 90) are specified when mirroring is initialized, either during CONTROL-M/Server installation or subsequently. You can subsequently change these parameters by using the Database Mirroring menu described in Chapter 11, “Maintaining databases and CONTROL-M data.”
### Table 90 CONTROL-M/Server mirroring parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CONTROL-M Mirror tablespace name</strong>&lt;br&gt;(Oracle)</td>
<td>Name of the Oracle CONTROL-M/Server mirror database. This name must be unique.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctrlm</td>
</tr>
<tr>
<td><strong>CONTROL-M Mirror Database Owner</strong>&lt;br&gt;(Sybase, Oracle, PostgreSQL)</td>
<td>Name for the CONTROL-M/Server mirror database owner. The install_mirror script creates this user in the database. This name is used by CONTROL-M when accessing the mirror database.&lt;br&gt;&lt;br&gt;Note: After specifying this utility, you are prompted to enter the DBA password to access the CONTROL-M/Server database server.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctrlm (For Sybase and Oracle only)</td>
</tr>
<tr>
<td><strong>CONTROL-M Mirror Database Data Device Name</strong>&lt;br&gt;(Sybase)</td>
<td>Name of the Sybase device on which the CONTROL-M/Server mirror database will be created.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctm</td>
</tr>
<tr>
<td><strong>CONTROL-M Mirror Database Log Device Name</strong>&lt;br&gt;(Sybase)</td>
<td>Name of the Sybase device on which the CONTROL-M/Server mirror database log will be created.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctmlog</td>
</tr>
<tr>
<td><strong>CONTROL-M Mirror database data device name</strong>&lt;br&gt;(Sybase)</td>
<td>Name of the Sybase device on which the CONTROL-M/Server mirror database will be created.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctrlm_ux</td>
</tr>
<tr>
<td><strong>CONTROL-M Mirror database log device name</strong>&lt;br&gt;(Sybase)</td>
<td>Name of the Sybase device on which the CONTROL-M/Server mirror database log will be created.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctrlm_log</td>
</tr>
<tr>
<td><strong>CONTROL-M Mirror database name</strong>&lt;br&gt;(Sybase, MSSQL, PostgreSQL)</td>
<td>Name of the CONTROL-M/Server mirror database. This name must be unique.&lt;br&gt;&lt;br&gt;<strong>Default:</strong> ctrlm&lt;br&gt;&lt;br&gt;(Only for Sybase)</td>
</tr>
</tbody>
</table>
### Table 90  CONTROL-M/Server mirroring parameters (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>DBO Password</strong> (Sybase, Oracle, PostgreSQL)</td>
<td>Password for the CONTROL-M/Server mirror database owner (6 to 30 characters, alphanumeric). The characters you enter are not echoed for security reasons. This password is used by CONTROL-M processes and utilities to access the CONTROL-M mirror database. <strong>Note:</strong> The single apostrophe symbol (‘ ‘) is not permitted for PostgreSQL.</td>
</tr>
<tr>
<td><strong>Mirror Oracle Instance name (SID)</strong> (Oracle)</td>
<td>The name of the Oracle mirror SQL server (1 to 8 characters, alphabetic plus ‘_’). <strong>Default:</strong> ctrlm</td>
</tr>
<tr>
<td><strong>Mirror Sybase Server Name</strong> (Sybase)</td>
<td>Name of the SQL server to which CONTROL-M will connect for mirroring. When you choose to modify this value, the install_mirror script reads the Sybase interfaces file and displays a list of the available SQL servers. Specify the name of an SQL server from the displayed list (contact your system administrator for this information). <strong>Default:</strong> CTRLM2</td>
</tr>
<tr>
<td><strong>Mirror Host Name</strong> (Sybase, Oracle, PostgreSQL)</td>
<td>Host name of computer that runs the instance of the database SQL Server used for mirroring.</td>
</tr>
<tr>
<td><strong>Mirror Port Number</strong> (Sybase, Oracle, PostgreSQL)</td>
<td>TCP/IP query port number for the database SQL Server used for mirroring. If you are using a CONTROL-M dedicated database SQL Server for the mirror database, the Sybase/Oracle Port Number can be found in the QUERY_SPN field in the <code>&lt;controlm_owner&gt;/install/install_defs</code> file, and for PostgreSQL, in the <code>&lt;PostgreSQL Home&gt;/data/postgresql.conf</code> file. <strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td><strong>Mirror Retry</strong> (Sybase, Oracle, PostgreSQL)</td>
<td>The CTM_MIRROR_RETRY parameter sets the number of retries the CONTROL-M/Server will attempt before marking the mirror as damaged. Valid values are 0-99 seconds. <strong>Default:</strong> 10 seconds</td>
</tr>
</tbody>
</table>

## Performance parameter

A special parameter in the CONTROL-M `<controlm_owner>/ctm_server/data/config.dat` file is available for tuning CONTROL-M performance. This parameter affects how jobs are selected for both scheduling and post-processing. Table 91 describes the performance parameter. The variable `<controlm>` is the CONTROL-M home directory.
The sleep time setting for CONTROL-M processes can also affect the performance and functionality of CONTROL-M. For example, setting the sleep time of the Selector (SL) and/or Tracking (TR) process to 5, will improve performance, but CONTROL-M will consume more CPU.

**Configuration parameters**

Table 91 describes the parameters in the CONTROL-M/Server configuration parameter file (~<controlm_owner>/ctm_server/data/config.dat on the server computer).

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SL_BREAK_COUNT</td>
<td>This parameter is for tuning CONTROL-M/Server select for submission performance. It counts the number of submitted jobs before jumping to the beginning of the Active Jobs file list. If SL_BREAK_COUNT = 0, no break occurs.</td>
</tr>
</tbody>
</table>
### Table 92  CONTROL-M/Server configuration parameters (part 1 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENTS_CLEANUP_IN_NEWDAY</td>
<td>Specifies whether the New Day procedure sends a request to CONTROL-M/Agents to remove SYSOUT files and exit status files that are no longer needed.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> Y, N</td>
</tr>
<tr>
<td></td>
<td>- Y—The New Day procedure sends a request to CONTROL-M/Agents to remove SYSOUT files and exit status files that are no longer needed.</td>
</tr>
<tr>
<td></td>
<td>- N —The New Day procedure does not send a request to the CONTROL-M/Agents to remove SYSOUT files and exit status files that are no longer needed.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can speed up the New Day procedure by specifying N for this parameter and running the ctmagcln utility. For more information, see the CONTROL-M Utility Guide.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Y</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>ALARM_DEST</td>
<td>Logical name of the Shout destination for critical Alert messages.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>- ECS—CONTROL-M/EM GI</td>
</tr>
<tr>
<td></td>
<td>- IOALOG—CONTROL-M IOALOG files</td>
</tr>
<tr>
<td></td>
<td>- CONSOLE—Server console</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> ECS</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Manual</td>
</tr>
</tbody>
</table>
### Table 92  CONTROL-M/Server configuration parameters (part 2 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>AUTOEDIT_INC_SEC</strong></td>
<td>Indicates which AutoEdit variables are sent to the agent for each submitted job. Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>SYSTEM</strong>—All the AutoEdit variables for each submitted job are sent to the agent. These include System, Global, Group, and Local variables.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>GLOBAL</strong>—Global, Group, and Local AutoEdit variables are sent to the agent for each submitted job. System AutoEdit variables are not sent.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>GROUP</strong>—Group and Local AutoEdit variables are sent to the agent for each submitted job. System and Global variables are not sent.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>LOCAL</strong>—Only Local AutoEdit variables are sent to the agent.</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>LOCAL</td>
</tr>
<tr>
<td><strong>How / where to set:</strong></td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td><strong>Refresh Type:</strong></td>
<td>Manual</td>
</tr>
<tr>
<td><strong>CTM_AUTOEDIT_ALLOW_HYPHEN</strong></td>
<td>Enables user-defined autoedit variables to contain the - (hyphen) character. Valid values: N, Y</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>N</td>
</tr>
<tr>
<td><strong>How / where to set:</strong></td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td><strong>Refresh Type:</strong></td>
<td>Manual</td>
</tr>
<tr>
<td><strong>CTM_ADJUST_COND_SCOPE</strong></td>
<td>For jobs in the Group Scheduling table, determines conditions of which unscheduled predecessor jobs to ignore. Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ <strong>AJF</strong>—Ignore predecessor jobs in the Active Jobs file level. When selected, jobs in the Group Scheduling table ignore conditions set by jobs in the active jobs file that are not scheduled.</td>
</tr>
<tr>
<td></td>
<td>■ <strong>GROUP</strong>—Ignore predecessor jobs in the group level. When selected, jobs in the Group Scheduling table ignore conditions set by jobs in the Group Scheduling table that are not scheduled. Default.</td>
</tr>
<tr>
<td><strong>Note:</strong></td>
<td>This parameter is relevant only when ADJUST_COND is set to Y. For more information, see ADJUST_COND in the CONTROL-M Parameter Guide.</td>
</tr>
<tr>
<td><strong>Default:</strong></td>
<td>GROUP</td>
</tr>
<tr>
<td><strong>How / where to set:</strong></td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td><strong>Refresh Type:</strong></td>
<td>Manual</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| **CTM_CONFIG_AGENT_AGENT_UNAVAIL_THRESHOLD** | The CONTROL-M/Server Configuration Agent issues the following message when the number of unavailable agents is equal to or greater than the threshold: Some of the CONTROL-M/Agents are unavailable.  
Valid values: 1–2<sup>31</sup>  
Default: 1  
How / where to set: See “Editing the config.dat file” on page 408.  
Refresh Type: Manual |
| **CTM_CONFIG_AGENT_GET_HOSTNAME_INTERVAL** | Frequency, in hours, with which CONTROL-M/Server will retrieve operating system, platform, and Agent version information from CONTROL-M/Agents and remote hosts so that the updated information is available to the end user via CONTROL-M Configuration Manager.  
Default: 24 (hours) |
| **CTM_CONFIG_AGENT_INITIAL_GET_HOSTNAME_INTERVAL** | For CONTROL-M/Agents and remote hosts for which CONTROLM/Server has not previously identified the operating system and Agent version, the frequency, in minutes, with which CONTROL-M/Server will try to retrieve that information so that it is available to the end user via CONTROL-M Configuration Manager.  
Default: 5 (minutes) |
| **CTM_CONFIG_AGENT_MODE** | Determines the mode of the CONTROL-M/Server Configuration Agent.  
Valid values:  
- 0 (OFF_MODE): Disable Configuration Agent process, no communication with CMS is allowed.  
- 1 (READ_MODE): Only life check and information requests are honored, any modifying request is rejected.  
- 2 (ALL_MODE) Any CMS request is honored.  
Default: 2  
How / where to set: See “Editing the config.dat file” on page 408.  
Refresh Type: Recycle |
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTM_CONFIG_AGENT_PORT_NUMBER</td>
<td>The CONTROL-M/Server Configuration Agent listening port number.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 1025–32767</td>
</tr>
<tr>
<td></td>
<td>Default: 2369</td>
</tr>
<tr>
<td></td>
<td>How / where to set: In the CONTROL-M Main Menu, choose Parameter Customization =&gt; Basic Communication and Operational Parameters =&gt; Configuration agent Port. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Recycle</td>
</tr>
<tr>
<td>CTM_CONFIG_AGENT_DEBUG_LEVEL</td>
<td>Specifies the CONTROL-M/Server Configuration Agent debug level.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 0 –5 (where 0 means only critical messages are displayed)</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td></td>
<td>How / where to set: In the CONTROL-M Main Menu, choose Troubleshooting =&gt; Set Diagnostics Level. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Automatic</td>
</tr>
<tr>
<td>CTM_CONFIG_AGENT_MODULE_LEVEL</td>
<td>Specifies the CONTROL-M/Server Configuration Agent module level.</td>
</tr>
<tr>
<td></td>
<td>Valid values: ■ 0—All components.</td>
</tr>
<tr>
<td></td>
<td>■ 1—Common functionality flow. Default.</td>
</tr>
<tr>
<td></td>
<td>■ 2—Event manager.</td>
</tr>
<tr>
<td></td>
<td>■ 3—Database layer.</td>
</tr>
<tr>
<td></td>
<td>Default: 1</td>
</tr>
<tr>
<td></td>
<td>How / where to set: In the CONTROL-M Main Menu, choose Troubleshooting =&gt; Set Diagnostics Level. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Automatic</td>
</tr>
<tr>
<td>CTM_DB_TIMEOUT</td>
<td>Timeout value for long New Day database transactions.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 300–3600 (seconds)</td>
</tr>
<tr>
<td></td>
<td>Default: 300 (seconds)</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Recycle</td>
</tr>
</tbody>
</table>
### CTM_GROUP_ADJUST_DUMMY

Controls creation of dummy jobs that run in place of unscheduled prerequisite jobs.

**Valid values:**

- **Y**—A dummy job waits for the prerequisite conditions expected by the job it is replacing, and performs the post processing of the job. When a Group Scheduling table is ordered, jobs in the group that should not be ordered at this time are ordered as DUMMY jobs. This functionality is useful for data centers that require identical job flow regardless of whether certain jobs in a group are ordered for a specific instance of the group.

- **N**—Out conditions of the jobs that were not ordered are ignored by the ordered jobs in the group scheduling table.

**Note:** This parameter is relevant only when ADJUST_COND is set to Y. For more information, see ADJUST_COND in the CONTROL-M Parameter Guide.

**Default:** N

**How / where to set:** See “Editing the config.dat file” on page 408.

**Refresh Type:** Manual

---

### CTM_GROUP_RECHECK

Indicates if group conditions should be checked for each job in a Group Scheduling table after the groups conditions have been satisfied.

**Valid values:**

- **N**—group conditions are ignored when ordering specific jobs in a group.
- **Y**—group conditions are checked for each job in the group (in addition to conditions specified for the job).

**Note:** If N is specified for this parameter, groups are activated when the necessary conditions exist, and remain active regardless of whether or not any of those conditions are deleted.

**Default:** N

**How / where to set:** See “Editing the config.dat file” on page 408.

**Refresh Type:** Manual
### Table 92  CONTROL-M/Server configuration parameters (part 6 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **CTM_MULTIP_LIB_REPLACE** | Indicates if AutoEdit variable `%MEMLIB` overrides the MEMLIB value for all jobs in a Scheduling table with a command such as:  
  
  `ctmorder -schedtab test2...-jobname "*" -autoedit %MEMLIB d:/testdir`  
  
  If you use the same command for a specific jobname, this parameter is ignored.  
  
  Valid values: Y, N  
  
  Default: N  
  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  
  **Refresh Type:** Manual                                                                                                    |
| **CTM_SLP_SUSPEND**      | During New Day or Download of the AJF to CONTROL-M/EM, the `ctmcreate`, `ctmudly`, `ctmorder` utilities and `ctmac` and CS processes are suspended (when trying to order). They stay suspended until the Download or New Day is completed. This parameter indicates the maximum number of times to wait, where each time is configured, in seconds, by the parameter `CTM_SUS_SLEEP_TIME`.  
  
  Valid values: 1–120 (times)  
  
  Default: 30  
  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  
  **Refresh Type:** Manual                                                                                                    |
| **CTM_SUS_SLEEP_TIME**   | During New Day or Download of the AJF to CONTROL-M/EM, the `ctmcreate`, `ctmudly`, and `ctmorder` utilities and the `ctmac` and CS processes are suspended (when trying to order). They stay suspended until the Download or New Day is complete. This parameter indicates the specified number of seconds to wait before initiating a download or the New Day procedure.  
  
  See also `CTM_SLP_SUSPEND`.  
  
  Valid values: 1–180 (seconds)  
  
  Default: 60 (seconds)  
  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  
  **Refresh Type:** Manual                                                                                                    |
### Table 92  CONTROL-M/Server configuration parameters (part 7 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTM_SNMP_SEND_FORMAT</td>
<td>Indicates whether Single (S) or Multiple (M) variable format is used for SNMP traps. For more information, see the description of the ctm2snmp utility in the <em>CONTROL-M Utility Guide</em>.</td>
</tr>
<tr>
<td>Valid values: S, M</td>
<td>Default: S</td>
</tr>
<tr>
<td>How / where to set:</td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Automatic</td>
</tr>
<tr>
<td>CTM_TIMEZONE_DISPLAY</td>
<td>Indicates if job run time is adjusted to time zone.</td>
</tr>
<tr>
<td>Valid values:</td>
<td>– N – the Next Run time of a job is in local computer time, not adjusted to time zone.</td>
</tr>
<tr>
<td></td>
<td>– Y – the Next Run time of a job is adjusted to the correct time zone.</td>
</tr>
<tr>
<td>Default: N</td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Manual</td>
</tr>
<tr>
<td>CTM_WRITE_CONSOLE</td>
<td>If this parameter is set, critical alerts are sent to the console of the server in addition to being sent as Shout messages to CONTROL-M/EM.</td>
</tr>
<tr>
<td>Valid values: YES, NO</td>
<td>Default: NO</td>
</tr>
<tr>
<td>How / where to set:</td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Recycle</td>
</tr>
<tr>
<td>CTMLOG_DEL_CHK</td>
<td>When set to Y, the use of the ctmlog utility for delete operation to CONTROL-M is restricted. Administrator only.</td>
</tr>
<tr>
<td>Valid values: Y, N</td>
<td>Default: N</td>
</tr>
<tr>
<td>How / where to set:</td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Automatic</td>
</tr>
</tbody>
</table>
### Table 92  CONTROL-M/Server configuration parameters (part 8 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CTMORDER_FORCE</strong></td>
<td>The default action of the utility is to order, not force, jobs in the Active Jobs file. This action can be modified by adding keyword Force to the command that invokes the utility. To change the default to force, set this parameter to Y.</td>
</tr>
<tr>
<td></td>
<td>Valid values: Y, N</td>
</tr>
<tr>
<td></td>
<td>Default: N</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Automatic</td>
</tr>
<tr>
<td><strong>DO_NOT_COPY_LOG_TO_MIRROR</strong></td>
<td>This parameter improves the performance of initialize mirroring. When set to YES, the CONTROL-M/Server log is truncated on the secondary database when mirroring is initialized. When restoring from the mirror, the log is truncated in the primary database. CONTROL-M/Server log is not copied during initializing or restoring from mirroring.</td>
</tr>
<tr>
<td></td>
<td>Valid values: YES, NO</td>
</tr>
<tr>
<td></td>
<td>Default: NO</td>
</tr>
<tr>
<td></td>
<td>How / where to set:</td>
</tr>
<tr>
<td></td>
<td>■ For Windows, see “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>■ For UNIX, see “Editing the cshrc file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Automatic</td>
</tr>
<tr>
<td><strong>SCHED_NON_EXIST_DAY</strong></td>
<td>When DAYS is &gt;n, or &lt;n, should we order the job on the next (&gt;n), or previous (&lt;n) working day, if n is a non-existing day for the specific month? If the parameter is set to Y, then we should order the job.</td>
</tr>
<tr>
<td></td>
<td>Valid values: N, Y</td>
</tr>
<tr>
<td></td>
<td>Default: N</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
</tbody>
</table>
### Table 92  CONTROL-M/Server configuration parameters (part 9 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CYCLIC_MAXWAIT</td>
<td>Indicates when cyclic jobs, that have previously executed at least once, are removed from the Active Jobs file by the New Day procedure.</td>
</tr>
<tr>
<td>Valid values:</td>
<td>• KEEP – each job is removed when MAXWAIT days have passed regardless of whether it ended OK.</td>
</tr>
<tr>
<td></td>
<td>• NOT_KEEP – each job (non-cyclic and cyclic) is removed from the Active Jobs file at the next run of the New Day procedure. Cyclic jobs are not removed if they are executing when the New Day procedure begins. Instead, they are removed at the run of the following New Day procedure.</td>
</tr>
<tr>
<td>Default: KEEP</td>
<td></td>
</tr>
<tr>
<td>How / where to set:</td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Recycle</td>
</tr>
<tr>
<td>CYCLIC_RERUN</td>
<td>If a cyclic job ends NOTOK and this parameter is set to OK, the cyclic job will be rerun. If set to NOTOK, the job will not be rerun.</td>
</tr>
<tr>
<td>Valid values:</td>
<td>OK, NOTOK</td>
</tr>
<tr>
<td>Default: OK</td>
<td></td>
</tr>
<tr>
<td>How / where to set:</td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Manual</td>
</tr>
<tr>
<td>CTM_GD_FORWARD</td>
<td>Indicates if job with a time zone specified should be ordered according to the current odate, or tomorrow’s odate.</td>
</tr>
<tr>
<td>Valid values:</td>
<td>Y – During the New Day Procedure, jobs with a specified time zone are ordered only if they are scheduled for tomorrow’s Odate.</td>
</tr>
<tr>
<td></td>
<td>N – During the New Day Procedure, jobs with a specified time zone are ordered only if they are scheduled for the current Odate.</td>
</tr>
<tr>
<td>Default: Y</td>
<td></td>
</tr>
<tr>
<td>How / where to set:</td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td>Refresh Type:</td>
<td>Recycle</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| IOALOG_DEL_INT                 | During the New Day procedure, old IOALOG records are removed. The default is to delete the old records in hourly bundles. If set to 24, all the old logs are deleted in one bundle.  
Valid values: 1–24  
Default: 1  
How / where to set: See “Editing the config.dat file” on page 408.  
Refresh Type: Recycle |
| NEW_DAY_ASYNC_SP_EXECUTION     | (Windows) Improves the performance of initialize mirroring.  
Valid values:  
- Y—the cleanup is performed in an asynchronous way.  
- N—the cleanup is performed sequentially.  
Default: Y |
| NOT_ORDERED_JOB_ALERT          | Type of Alert message to send to CONTROL-M/EM when a job is not ordered due to scheduling criteria.  
Valid values:  
- 0 – One General Alert per User Daily: ONE OR MORE JOBS IN DAILY <daily_name> WERE NOT ORDERED  
- 1 – One Alert message per job: DAILY <daily_name> FAILED TO ORDER JOBNAME <jobname>  
- 2 – Do not issue Alert messages  
Default: 0  
How / where to set: See “Editing the config.dat file” on page 408.  
Refresh Type: Recycle |
Table 92 CONTROL-M/Server configuration parameters (part 11 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RUNINF_CUTOFF_NUMERBER</td>
<td>Affects the statistics cleanup algorithm that is performed during New Day when the RUNINF_PURGE_MODE is set to 0 (default). If the number of records to be deleted from the table is less than the value of this parameter, then records are deleted directly from the statistics table. Otherwise a temporary table is used to delete the records.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0 - 65K</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 2000</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>RUNINF_CUTOFF_RATIO</td>
<td>Affects the statistics cleanup algorithm that is performed during New Day when the RUNINF_PURGE_MODE is set to 0. If the ratio between the number of records to be deleted and the number of records in the table is less than the value of this parameter, then records are deleted directly from the statistics table. Otherwise a temporary table is used to delete the records.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> decimal fraction between 0–1</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0.33</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>RUNINF_PURGE_LIMIT</td>
<td>Number of Run Information records to keep for a given MemName/MemLib/NodeID. If RUNINF_PURGE_MODE is 0, the New Day Procedure deletes all Run Information records for each unique name except the last n records, where n is the value of this parameter.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 1–2^31</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 20</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
</tbody>
</table>
### Table 92  CONTROL-M/Server configuration parameters (part 12 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| RUNINF_PURGE_MODE | Valid values: 0, 1  
0 – Performs -PURGE cleanup. Statistics records per job are kept according to the specified Statistics Mode (either MEMNAME or JOBNAME). Default: 20 records of each MEMNAME or JOBNAME are kept.  
If the RUNINF_PURGE_LIMIT in the config.dat is specified, the number of records that are kept is determined by this parameter.  
1 – Performs -DELETE cleanup. Only the amount of days that are specified are kept. Default: The number of days kept is specified by the How Many Days to Retain ioalog parameter.  
If the RUNINF_PURGE_LIMIT in the config.dat is specified, the number of days that are kept is determined by this parameter.  
Default: 0  
How / where to set: See “Editing the config.dat file” on page 408.  
Refresh Type: Recycle |
| STATISALG          | Specifies mode used to collect summary statistics by ctmjsa. In addition it is used for actions on statistics such as average and deletion.  
Valid values:  
  - JOBNAME – compiles statistics for each CONTROL-M Job Name/Scheduling Table and Node ID where the job was submitted  
  - MEMNAME – compiles statistics for each CONTROL-M Mem Name/Mem Lib and Node ID  
Default: MEMNAME  
How / where to set: See “Editing the config.dat file” on page 408.  
Refresh Type: Recycle |
### Table 92  CONTROL-M/Server configuration parameters (part 13 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>STATISTICS_CLEANUP_IN_NEWDAY</td>
<td>Specifies whether the statistics cleanup action is executed during the New Day procedure.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ Y—The statistics cleanup action is executed during New Day procedure.</td>
</tr>
<tr>
<td></td>
<td>■ N—The statistics cleanup action is not executed during New Day procedure.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You can speed up the New Day procedure by specifying N for this parameter and running ctmruninf -PURGE.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Y</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>STATS_TIME</td>
<td>For statistics calculation, indicates how the START TIME and END TIME for a job should be set.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ SERVER – START TIME and END TIME are set by CONTROL-M/Server.</td>
</tr>
<tr>
<td></td>
<td>■ AGENT – START TIME and END TIME are set using information received from the CONTROL-M/Agent.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> SERVER</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Manual</td>
</tr>
<tr>
<td>SYSOUT_LIMIT_SIZE</td>
<td>Maximum SYSOUT size that can be viewed by the sysout command from CONTROL-M/Server and CONTROL-M/EM. The value is set in Kilobytes.</td>
</tr>
<tr>
<td></td>
<td>If a SYSOUT file exceeds the value specified by the SYSOUT_LIMIT_SIZE configuration parameter, it cannot be viewed from CONTROL-M/Server or CONTROL-M/EM, and the following message is displayed:</td>
</tr>
<tr>
<td></td>
<td><strong>SYSOUT FILE EXCEEDED LIMIT SIZE (CAN BE VIEWED FROM FILE SYSTEM)</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0–2^31</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0 (unlimited)</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Manual</td>
</tr>
</tbody>
</table>
## Table 92  CONTROL-M/Server configuration parameters (part 14 of 14)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SYSOUT_WINDOW_SIZE</td>
<td>Specifies the maximum number of characters for a SYSOUT file line.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 80–132 characters</td>
</tr>
<tr>
<td></td>
<td>Default: 80</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
<tr>
<td>UDLY_PARTCOPY_ERR</td>
<td>Error code returned by ctmudly utility if one or more jobs in a scheduling table are not ordered by a User Daily job (due to scheduling criteria or security settings)</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ 0 – User Daily job ends with an exit code of 0 even if not all jobs are ordered.</td>
</tr>
<tr>
<td></td>
<td>■ 1 – User Daily job ends with an exit code of 14 if not all jobs are ordered.</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Automatic</td>
</tr>
<tr>
<td>STOP_SUBMISSION_BEFORENEWDAY</td>
<td>Specifies the number of seconds preceding launch of the NewDay procedure during which jobs are not submitted.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 0–3600 (seconds)</td>
</tr>
<tr>
<td></td>
<td>Default: 2 (seconds)</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
</tbody>
</table>

## E-mail configuration parameters

The following parameters are applicable to DOMAIL, -DOSHOUT (when shout destination is mail), ctmshout, and –SHOUT (when shout destination is mail).

**NOTE**

The SYSOUT of a job can be attached to an e-mail message only if the job has completed processing.
Table 93  CONTROL-M/Server e-mail configuration parameters (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ADD_SYSOOUT_TO_EMAIL</td>
<td>Determines whether the SYSOUT of a job can be attached to e-mail messages.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>▪ N – No. When specified, the SYSOUT of a job is not attached. This setting</td>
</tr>
<tr>
<td></td>
<td>overrides any specification made elsewhere.</td>
</tr>
<tr>
<td></td>
<td>▪ A – Attachment. When specified, the SYSOUT of a job is attached. This</td>
</tr>
<tr>
<td></td>
<td>setting overrides any specification made elsewhere.</td>
</tr>
<tr>
<td></td>
<td>Default: N</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
<tr>
<td>ADD_SYSOOUT_TO_EMAIL_LIMIT_SIZE</td>
<td>Determines the maximum size of the attachment SYSOUT file in kilobytes.</td>
</tr>
<tr>
<td></td>
<td>You can specify the value 0 for unlimited size.</td>
</tr>
<tr>
<td></td>
<td>Note: If the SYSOUT file is larger than the specified maximum size, the</td>
</tr>
<tr>
<td></td>
<td>SYSOUT will not be attached to the e-mail message.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 0–2^31</td>
</tr>
<tr>
<td></td>
<td>Default: 5120KB (5MB)</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
<tr>
<td>ADD_SYSOOUT_TO_EMAIL_TIMEOUT_LIMIT</td>
<td>When sending a mail request—with a SYSOUT file attached—to the SMTP server,</td>
</tr>
<tr>
<td></td>
<td>determines the maximum time to wait.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 1–300 (seconds)</td>
</tr>
<tr>
<td></td>
<td>Default: 30 (seconds)</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
<tr>
<td>MAIL_ADD_SUBJECT_PREFIX</td>
<td>Determines if the CONTROL-M/Server Shout by orderno prefix must be added</td>
</tr>
<tr>
<td></td>
<td>to the subject of the e-mail message.</td>
</tr>
<tr>
<td></td>
<td>Valid values: Y, N</td>
</tr>
<tr>
<td></td>
<td>Default: Y</td>
</tr>
<tr>
<td></td>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td>Refresh Type: Manual</td>
</tr>
</tbody>
</table>
Table 93  CONTROL-M/Server e-mail configuration parameters (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| MAIL_TIMEOUT           | Determines the maximum time to send the mail request to the SMTP server when no SYSOUT is attached.  
                          | **Valid values:** 1–30 (seconds)                                               |
|                        | **Default:** 5 (seconds)                                                    |
|                        | **How / where to set:** See “Editing the config.dat file” on page 408.       |
|                        | **Refresh Type:** Manual                                                    |
| SMTP_SERVER_NAME       | Specify the name of the SMTP server relay.                                  |
|                        | **Valid values:** 0 - 50 characters                                           |
|                        | **Default:** “” (During installation, this is overridden by a null value.)   |
|                        | **How / where to set:** In the CONTROL-M Main Menu, choose Parameter        |
|                        |   Customization => Simple Mail Transfer Protocol Parameters => SMTP          |
|                        |   Server (Relay) Name. For more information, see “Using the Main menu” on   |
|                        |   page 406.                                                                |
|                        | **Refresh Type:** Automatic                                                 |
| SMTP_SENDER_EMAIL      | Specify the e-mail address used by CONTROL-M/Server.                        |
|                        | **Valid values:** 0 - 99 characters                                          |
|                        | **Default:** “” (During installation, this is overridden by CONTROL@M.)     |
|                        | **How / where to set:** In the CONTROL-M Main Menu, choose Parameter        |
|                        |   Customization => Simple Mail Transfer Protocol Parameters => Sender        |
|                        |   Email. For more information, see “Using the Main menu” on page 406.        |
|                        | **Refresh Type:** Automatic                                                 |
| SMTP_PORT_NUMBER       | Specify the port number to which the service is assigned.                   |
|                        | **Valid values:** 1–2^31                                                    |
|                        | **Default:** 25                                                            |
|                        | **How / where to set:** In the CONTROL-M Main Menu, choose Parameter        |
|                        |   Customization => Simple Mail Transfer Protocol Parameters => Port         |
|                        |   Number. For more information, see “Using the Main menu” on page 406.       |
|                        | **Refresh Type:** Automatic                                                 |
### Table 93  CONTROL-M/Server e-mail configuration parameters (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP_SENDER_FRIENDLY_NAME</td>
<td>Specify the regular text name used to identify the sender.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0 - 99 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> CONTROL-M/Server (During installation, this is overridden by a null value.)</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> In the CONTROL-M Main Menu, choose Parameter Customization =&gt; Simple Mail Transfer Protocol Parameters =&gt; Sender Friendly Name. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Automatic</td>
</tr>
<tr>
<td>MAIL_REPLY_TO_EMAIL</td>
<td>Specify the email address to which messages are returned if a return address is not otherwise specified. If this parameter is null, the sender’s email address becomes the default.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0 - 99 characters</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> &quot;&quot; (During installation, this is overridden by a null value.)</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> In the CONTROL-M Main Menu, choose Parameter Customization =&gt; Simple Mail Transfer Protocol Parameters =&gt; Reply–To Email. For more information, see “Using the Main menu” on page 406.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Manual</td>
</tr>
</tbody>
</table>

### User exit parameters

Table 94 lists the CONTROL-M/Server user exit parameters.
Table 94  CONTROL-M/Server user exit parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTM_PRM_ENABLE_U</td>
<td>Indicates whether CONTROL-M user exits and Watchdog process exits are enabled. (See “Watchdog process parameters” on page 498.)</td>
</tr>
<tr>
<td></td>
<td>Valid values: ( Y, N )</td>
</tr>
<tr>
<td></td>
<td>Default: ( Y )</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>CTM_PRM_ENABLE_UExxx (101-106)</td>
<td>Indicates whether the associated UExxx user exit is enabled. For more information, see Appendix C, “Exits.”</td>
</tr>
<tr>
<td></td>
<td>Valid values: ( Y, N )</td>
</tr>
<tr>
<td></td>
<td>Default: ( N )</td>
</tr>
</tbody>
</table>
Table 94  CONTROL-M/Server user exit parameters (part 2 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CTM_PRM_SCRIPT_UExxx (101–106)</strong></td>
<td>Name of the UExxx user exit script. These scripts must reside in the ~&lt;controlm_owner&gt;/ctm_server/ue_exit directory.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values</strong>: 1024 characters</td>
</tr>
</tbody>
</table>
|                                                | **Default**:  ■ UE101 Job Ordering User Exit—ctm_exit101.sh  
|                                                | ■ UE102 Job Submission User Exit—ctm_exit102.sh  
|                                                | ■ UE103 Before New Day Procedure User Exit—ctm_exit103.sh  
|                                                | ■ UE104 After New Day Procedure User Exit—ctm_exit104.sh  
|                                                | ■ UE105 Before User Daily User Exit—Ctm_exit105.sh  
|                                                | ■ UE106 After User Daily User Exit—Ctm_exit106.sh  
|                                                | **How / where to set**: See “Editing the config.dat file” on page 408.                                                                      |
|                                                | **Refresh Type**:  ■ UE101 Job Ordering User Exit—Manual  
|                                                | ■ UE102 Job Submission User Exit—Manual  
|                                                | ■ UE103 Before New Day Procedure User Exit—Recycle  
|                                                | ■ UE104 After New Day Procedure User Exit—Recycle  
| **CTM_PRM_TIMEOUT_UExxx (101–106)**             | Time to wait for a user exit script to run before it is terminated.                                                                     |
|                                                | For UNIX: Time is measured in units of seconds  
|                                                | For Windows: Time is measured in units of milliseconds                                                                                     |
|                                                | **Valid values**: 20–2^31                                                                                                                     |
|                                                | **Default**: 20                                                                                                                            |
|                                                | **How / where to set**: See “Editing the config.dat file” on page 408.                                                                      |
|                                                | **Refresh Type**:  ■ UE101 Job Ordering User Exit—Manual  
|                                                | ■ UE102 Job Submission User Exit—Manual  
|                                                | ■ UE103 Before New Day Procedure User Exit—Recycle  
|                                                | ■ UE104 After New Day Procedure User Exit—Recycle  

**Watchdog process parameters**

The following parameters are used for the Watchdog Process. (For more information, see “Heartbeat monitor and Watchdog facility” on page 266 and “Implementing Heartbeat Monitors and the Watchdog facility” on page 275.) The CTM_PRM_ENABLE_UE parameter must be set to Y to enable the WD process.
The Watchdog Process parameters discussed in this section are:

- General parameters
- CONTROL-M/Server system exit parameters
- Watchdog user exit parameters

### General parameters

Table 95  General Watchdog Process parameters (part 1 of 2)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD_ALIVE_MSG</td>
<td>Indicates message to be sent in response to successful heartbeat checks.</td>
</tr>
<tr>
<td>Valid values: 1024 characters</td>
<td></td>
</tr>
<tr>
<td>Default: &quot;&quot;</td>
<td></td>
</tr>
<tr>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
<tr>
<td>WD_CTMEXIT_NUMBER</td>
<td>Total number of CONTROL-M/Server system exits to run.</td>
</tr>
<tr>
<td>Valid values: 0–2^31</td>
<td></td>
</tr>
<tr>
<td>Default: 0 (In the shipped config.dat, this is overridden by the value 2.)</td>
<td></td>
</tr>
<tr>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
<tr>
<td>WD_ERROR_HANDLE Script_FILE</td>
<td>Full path name of a user defined script called by the Watchdog process as an error handler. The error messages are included as arguments to the script.</td>
</tr>
<tr>
<td>Valid values: 1024 characters</td>
<td></td>
</tr>
<tr>
<td>Default: &quot;&quot; (In the shipped config.dat, the default is overridden by ./scripts/UE_handler.)</td>
<td></td>
</tr>
<tr>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
<tr>
<td>WD_ERROR_HANDLE S_TIMEOUT</td>
<td>Maximum time for the Watchdog facility to wait for the user-defined script to run.</td>
</tr>
<tr>
<td>Valid values: 5–2^31</td>
<td></td>
</tr>
<tr>
<td>Default: 5 (In the shipped config.dat, this is overridden by the value 10.)</td>
<td></td>
</tr>
<tr>
<td>How / where to set: See “Editing the config.dat file” on page 408.</td>
<td></td>
</tr>
<tr>
<td>Refresh Type: Recycle</td>
<td></td>
</tr>
</tbody>
</table>
**Table 95   General Watchdog Process parameters (part 2 of 2)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD_HEARTBEAT_INTERVAL</td>
<td>The Watchdog process checks CONTROL-M/Server processes by sending a message. If this parameter is set to 5, the Watchdog process sends a message to each of the primary CONTROL-M/Server processes every 5th interval and awaits a response.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 1–$2^{31}$</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 5 (In the shipped config.dat, this is overridden by the value 1.)</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>WD_HEARTBEAT_LIMIT</td>
<td>Maximum time (in seconds) to wait for a response from each of the CONTROL-M/Server processes, after issuing a Heartbeat check, before sending a message to the error handlers.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 1–$2^{31}$</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 360</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>WD_INTERVAL</td>
<td>Basic time unit interval, in minutes. When the value in either the WD_CTMEXIT_#<em>INTERVAL parameter or the WD_USEREXIT</em>#_INTERVAL parameter is multiplied by the value in this parameter, the resulting value is the number of minutes that must pass before reinvoking the exit script.</td>
</tr>
<tr>
<td></td>
<td>For example, if the value of this parameter is 6 (minutes), and the value of the WD_CTMEXIT_1_INTERVAL parameter is 20, the script for system exit 1 will run once every 120 minutes (20 x 6 minutes).</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 1–$2^{31}$</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 5 (In the shipped config.dat, this is overridden by the value 6.)</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
<tr>
<td>WD_USEREXIT_NUMBER</td>
<td>Total number of user exits to run.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> 0–$2^{31}$</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 0</td>
</tr>
<tr>
<td></td>
<td><strong>How / where to set:</strong> See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td></td>
<td><strong>Refresh Type:</strong> Recycle</td>
</tr>
</tbody>
</table>
### CONTROL-M/Server system exit parameters

The # used in each of the following CONTROL-M/Server system exit parameters represents the corresponding CONTROL-M/Server utility that can be included in the CONTROL-M/Server Watchdog process: Disk Space Utility (1) and Database Usage Utility (2). For more information, see “Enabling the Watchdog facility to run the ctmdiskspace or ctmdbspace utilities, or other scripts” on page 529.

#### Table 96  Watchdog parameters for CONTROL-M/Server system exits (part 1 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **WD_CTMEXIT_#_CMD_LINE** | Contains parameters to be passed to the exit script. Arguments must start with a ‘-’ sign. Values separated by either a space or a ‘-’ sign must be enclosed in double quotation. Mandatory.  
  **Valid values:** 1024 characters  
  **Default:** ""  
  In the shipped config.dat on UNIX, the default values are overridden as follows:  
  - **wd_ctmexit_1:** `-LIMIT "10 M" -PATH $HOME`  
  - **wd_ctmexit_2:** `-LIMIT "90 M"`  
  In the shipped config.dat on Windows, the default values are overridden as follows:  
  - **wd_ctmexit_1:** `-LIMIT 10M -PATH C:\`  
  - **wd_ctmexit_2:** `-LIMIT 90`  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  **Refresh Type:** Recycle |
| **WD_CTMEXIT_#_ERROR_MSG** | Error message string to be passed to the error handler(s) if the utility returns a “failed” status. Optional.  
  **Valid values:** 1024 characters  
  **Default:** ""  
  (In the shipped config.dat, for wd_ctmexit_1 and wd_ctmexit_2, the default is overridden by “Low on database space.”)  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  **Refresh Type:** Recycle |
Table 96  Watchdog parameters for CONTROL-M/Server system exits (part 2 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>WD_CTMEXIT_#_INTERVAL</strong></td>
<td>Number of basic time interval units that should pass before reinvoking the exit script. The basic time interval unit is defined in parameter WD_INTERVAL.</td>
</tr>
<tr>
<td></td>
<td>For example, if the value of this parameter is 20, and the basic time interval unit (as defined in parameter WD_INTERVAL) is 5 minutes, the exit script will be invoked every 100 minutes (20 x 5 minutes).</td>
</tr>
<tr>
<td><strong>Valid values</strong></td>
<td>1–2³¹</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>5 (In the shipped config.dat, this is overridden by the value 20.)</td>
</tr>
<tr>
<td><strong>How / where to set</strong></td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td><strong>Refresh Type</strong></td>
<td>Recycle</td>
</tr>
<tr>
<td><strong>WD_CTMEXIT_#_RUN_STATE</strong></td>
<td>Specify whether (Y) or not (N) to run the utility when CONTROL-M/Server is running. A Y must be specified for either this parameter or for parameter WD_CTMEXIT_#_SUSPEND_STATE for the utility to be run.</td>
</tr>
<tr>
<td><strong>Valid values</strong></td>
<td>Y, N</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>N (In the shipped config.dat, this is overridden by the value Y.)</td>
</tr>
<tr>
<td><strong>How / where to set</strong></td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td><strong>Refresh Type</strong></td>
<td>Recycle</td>
</tr>
<tr>
<td><strong>WD_CTMEXIT_#_SCRIPT_FILE</strong></td>
<td>Relative path of the script or binary from the ~controlm\ctm_server\exe_&lt;computer&gt; directory.</td>
</tr>
<tr>
<td><strong>Valid values</strong></td>
<td>1024 characters</td>
</tr>
<tr>
<td><strong>Default</strong></td>
<td>&quot;&quot; (In the shipped config.dat, for both wd_ctmexit_1 and wd_ctmexit_2, this is overridden by the value CTMDISKSPACE.)</td>
</tr>
<tr>
<td><strong>How / where to set</strong></td>
<td>See “Editing the config.dat file” on page 408.</td>
</tr>
<tr>
<td><strong>Refresh Type</strong></td>
<td>Recycle</td>
</tr>
</tbody>
</table>
### Table 96  Watchdog parameters for CONTROL-M/Server system exits (part 3 of 3)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD_CTMEXIT_#_SUSPEND_STATE</td>
<td>Specify whether (Y) or not (N) to run the utility in Suspend mode (that is, during New Day procedure or download, when the database inaccessible). A Y must be specified for either this parameter or for parameter WD_CTMEXIT_#_RUN_STATE for the utility to be run. Valid values: Y, N Default: N How / where to set: See “Editing the config.dat file” on page 408. Refresh Type: Recycle</td>
</tr>
<tr>
<td>WD_CTMEXIT_#_TIMEOUT</td>
<td>Time (milliseconds) allowed before the exit script is terminated. Valid values: 1–2^31 (ms) Default: 5 ms (In the shipped config.dat, this is overridden by the value 30.) How / where to set: See “Editing the config.dat file” on page 408. Refresh Type: Recycle</td>
</tr>
</tbody>
</table>

**Watchdog user exit parameters**

The # used in the following user exit parameters represents a separate number for each user exit that can be included in the CONTROL-M Watchdog process (see “Watchdog facility exits” on page 528). A user exit can be either a user supplied script/executable file or a CONTROL-M utility.
## Table 97  Watchdog parameters user exit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **WD_USEREXIT_#_CMD_LINE** | Contains parameters to be passed to the exit script. Arguments must start with a '-' sign. Values separated by either a space or a '-' sign must be enclosed in double quotation. Mandatory.  
  
  **Valid values**: 1024 characters  
  **Default**: ""  
  **How / where to set**: See “Editing the config.dat file” on page 408.  
  **Refresh Type**: Recycle |
| **WD_USEREXIT_#_ERROR_MSG** | Error message string to be passed to the error handler(s) if the check returns a “failed” status. Optional.  
  
  **Valid values**: 1024 characters  
  **Default**: ""  
  **How / where to set**: See “Editing the config.dat file” on page 408.  
  **Refresh Type**: Recycle |
| **WD_USEREXIT_#_INTERVAL** | Number of basic time interval units that should pass before reinvoking the exit script. The basic time interval unit is defined in parameter WD_INTERVAL.  
  
  For example, if the value of this parameter is 2, and the basic time interval unit (as defined in parameter WD_INTERVAL) is 5 minutes, the exit script will be invoked every 10 minutes (2 x 5 minutes).  
  
  **Valid values**: 1–2^31  
  **Default**: 5  
  **How / where to set**: See “Editing the config.dat file” on page 408.  
  **Refresh Type**: Recycle |
| **WD_USEREXIT_#_RUN_STATE** | Specify whether (Y) or not (N) to run the utility when CONTROL-M/Server is running. A Y must be specified for either this parameter or for parameter WD_USEREXIT_#_SUSPEND_STATE for the utility to be run.  
  
  **Valid values**: Y, N  
  **Default**: N  
  **How / where to set**: See “Editing the config.dat file” on page 408.  
  **Refresh Type**: Recycle |
### Table 97  Watchdog parameters user exit

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| WD_USEREXIT_#_SCRIPT_FILE | Relative path of the script or binary from the ~controlm\ctm_server\exe_<computer> directory.  
  **Valid values:** 1024 characters  
  **Default:** ""  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  **Refresh Type:** Recycle |
| WD_USEREXIT_#_SUSPEND_STATE | Specify whether (Y) or not (N) to run the script in Suspend mode (that is, during New Day procedure or download, when the database inaccessible). This parameter or WD_CTMEXIT_#_RUN_STATE must be set to Y for the script to be run.  
  **Valid values:** Y, N  
  **Default:** N  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  **Refresh Type:** Recycle |
| WD_USEREXIT_#_TIMEOUT | Time (milliseconds) allowed before the exit script is terminated.  
  **Valid values:** 1–2^31 (ms)  
  **Default:** 5 ms  
  **How / where to set:** See “Editing the config.dat file” on page 408.  
  **Refresh Type:** Recycle |

### CONTROL-M/Agent parameters

This section lists and describes the following categories of CONTROL-M/Agent parameters:

<table>
<thead>
<tr>
<th>Agent parameter category</th>
<th>Page reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>Agent configuration parameters</td>
<td>506</td>
</tr>
<tr>
<td>CM parameters (UNIX)</td>
<td>510</td>
</tr>
<tr>
<td>CM parameters (Windows)</td>
<td>514</td>
</tr>
<tr>
<td>Agent service parameters</td>
<td>520</td>
</tr>
</tbody>
</table>
In this section, the information in the tables is listed alphabetically according to the Agent system parameter names. Parameters that can be changed from the CONTROL-M Configuration Manager are indicated by including the descriptive names (as they appear in the CONTROL-M Configuration Manager) in parenthesis.

Parameter changes are implemented automatically.

**Agent configuration parameters**

Table 98 lists the Agent configuration parameters.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AGENT_STATUS</td>
<td></td>
</tr>
</tbody>
</table>
  
  *(UNIX only)* This parameter is read by the `rc.agent_user` startup script to determine whether the agent should be started.  
  
  **Valid values:**  
  
  ■ Started  
  
  ■ Stopped  
| AG_LOG_ON            | Indicates if the `ctmag_<year><month><day>.log` file is generated (Y) or not (N).  
  
  **Valid values:** Y, N  
  
  **Default:** Y  
| AGCMNDATA            |  
  
  `<Port number>/<Timeout>` for the Server-to-Agent port. Port number specifies agent computer port that receives data from the Server computer. Verify that this port is not used for any other purpose. Must match Server-to-Agent port number in CONTROL-M/Server. The timeout value is the `COMTIMOUT` communication job-tracking timeout in seconds. Mandatory. Example: `7006/30`  
  
  **Valid values:** between 1024 and 65533 inclusive  
  
  **Default:** 7006  
| AGENT_DIR            | Location of files used by CONTROL-M/Server.  
| ALLOW_COMM_INIT      | Determines if the agent can open a connection to the server when working in persistent connection mode.  
  
  **Valid values:** Y, N  
  
  **Default:** Y  
| AR_AG_COMM_PORT      | Internal port used only when the agent is working in persistent connection mode. This port is selected by the installation, which validates that it is free. If this port is not free when the agent is started in persistent connection mode, or when it is shifted from transient to persistent during runtime, the agent automatically finds a new free port and updates the parameter accordingly.  

---

506  

**CONTROL-M Administrator Guide**
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AR_AT_COMM_PORT</td>
<td>Internal port used only when the agent is working in persistent connection mode. This port is selected by the installation, which validates that it is free. If this port is not free when the agent is started in persistent connection mode, or when it is shifted from transient to persistent during runtime, the agent automatically finds a new free port and updates the parameter accordingly.</td>
</tr>
<tr>
<td>AR_UT_COMM_PORT</td>
<td>Internal port used only when the agent is working in persistent connection mode. This port is selected by the installation, which validates that it is free. If this port is not free when the agent is started in persistent connection mode, or when it is shifted from transient to persistent during runtime, the agent will automatically find a new free port and update the parameter accordingly.</td>
</tr>
<tr>
<td>ATCMNDATA</td>
<td>&lt;Port number&gt;/&lt;Timeout&gt; for the Agent-to-Server port. Port number specifies the Server computer port that receives data from the agent computer. Verify that this port is not used for any other purpose. This value must match the Agent-to-Server Port Number in CONTROL-M/Server. The Timeout value is the COMTIMOUT communication job-tracking timeout in seconds. Mandatory. Example: 7005/30. Note: Increasing the Timeout value reduces agent performance. Valid values: Between 1024 and 65533 inclusive Default: 7005</td>
</tr>
<tr>
<td>AUTOEDIT_INLINE</td>
<td>Flag that indicates whether all AutoEdit variables will be set as environment variables in the script. Valid values: Y (yes), N (no) Default: Y</td>
</tr>
<tr>
<td>CM_APPL_TYPE</td>
<td>Default control module. Default: OS</td>
</tr>
<tr>
<td>CMLIST</td>
<td>List of Control Modules. For internal use only.</td>
</tr>
<tr>
<td>COMM_TRACE</td>
<td>Flag indicating whether communication packets that CONTROL-M/Agent sends to and receives from CONTROL-M/Server are written to a file. If set to 1, separate files are created for each session (job, ping, and so forth). This parameter can only be changed after completing the installation. Valid values: 1 (on), 0 (off) Default: 0 (off) How / where to set: See the Set communication trace option in “Activating diagnostics for CONTROL-M/Server” on page 339 and “Activating diagnostics for CONTROL-M/Agent” on page 340.</td>
</tr>
</tbody>
</table>
### Table 98  Agent configuration parameters (part 3 of 4)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| COMMOPT                 | Determines if CONTROL-M communication is secured using the SSL protocol.  
  **Valid values:** SSL=Y, SSL=N  
  **Default:** SSL=N                                                                 |
| COMMRETSLP              | Time in seconds (integer value) to wait between each attempt to attach to the CONTROL-M/Server.  
  **Default:** 1                                                           |
| CTMPERMHOSTS            | <one or more TCP/IP addresses or DNS names separated by |>. Each value identifies an authorized CONTROL-M/Server host where a backup CONTROL-M/Server is installed.  
  (This parameter was previously called Mirror CONTROL-M/Server Host Name.) Specify this parameter if one or more CONTROL-M/Servers have been designated as backups and can connect to this agent in case of failover. For information about backup server configuration, see the CONTROL-M Administrator Guide.  
  Mandatory. At least one primary host name should be specified. Example: 192.138.28.121|aristo.isr.bmc.com/mybksys1|192.138.28.123 |
| CTMS_ADDR_MODE          | [IP]  
  If this parameter is set to IP, the IP address instead of the host name is saved in CTMS_HOSTNAME. Use this parameter when CONTROL-M runs on a computer with more than one network card. |
| CTMSHOST                | CONTROL-M/Server host name. Name of the primary host running CONTROL-M/Server.                                                                 |
| DBGLVL                  | CONTROL-M/Agent diagnostic level (for use by Technical Support). Determines types of diagnostic messages generated. This parameter is normally set to zero (no diagnostics).  
  **Valid values:** 0-4  
  **Default:** 0                                                                 |
| EVENT_TIMEOUT           | Job Tracking Timeout. Tracker event timeout in seconds.  
  **Default:** 120                                                                 |
| I18N                    | Determines CONTROL-M mode of support for foreign languages.  
  **Valid values:** Latin-1, CJK  
  **Default:** Latin-1                                                                 |
| LISTEN_INTERFACE        | The network interface the agent is listening on. It can be set to a specific hostname or IP address so that the agent port is not opened in the other interfaces.  
  **Default:** *ANY (the agent is listening on all available interfaces) |
### Table 98  Agent configuration parameters (part 4 of 4)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>LOCALE</td>
<td>(Locale (LATIN-1 mode only)) (UNIX only) Determines the locale under which the agent processes run. Valid only when the agent is working in Latin-1 mode. Supported locales are specified in.</td>
</tr>
<tr>
<td>LOGICAL_AGENT_NAME</td>
<td>Logical name of the agent. The value specified should match the name the agent is defined by in CONTROL-M/Server.</td>
</tr>
<tr>
<td>LOGKEEPDAYS</td>
<td>Number of days to retain agent proclog files. After this period, agent proclog files are deleted by the New Day procedure.</td>
</tr>
<tr>
<td>PERSISTENT_CONNECTION</td>
<td>Determines if the agent is working in persistent or transient communication mode.</td>
</tr>
<tr>
<td>PROTOCOL_VERSION</td>
<td>Server-Agent communication protocol version.</td>
</tr>
<tr>
<td>TCP_IP_TIMEOUT</td>
<td>The COMTIMOUT communication job-tracking timeout in seconds.</td>
</tr>
<tr>
<td>TRACKER_EVENT_PORT</td>
<td>Number of the port for sending messages to the Tracker process when jobs end</td>
</tr>
<tr>
<td>UTTIMEOUT</td>
<td>Maximum time (in seconds) the agent waits after sending a request to CONTROL-M/Server. This timeout interval should be longer than the TCP/IP Timeout.</td>
</tr>
</tbody>
</table>

**Default**

- Agent host name
- 1
- N
- 08
- 120
- 120 (recommended)
### CM parameters for UNIX

Table 99 lists the Control Module configuration parameters for Unix.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION_LOCALE (CJK Encoding)</td>
<td>Determines the CJK encoding used by CONTROL-M/Agent to run jobs. For more information, see the CONTROL-M Language Customization Guide.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> UTF-8, JAPANESE EUC, JAPANESE SHIFT-JIS, KOREAN EUC, SIMPLIFIED CHINESE GBK, SIMPLIFIED CHINESE GB, TRADITIONAL CHINESE EUC, TRADITIONAL CHINESE BIG5</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> UTF-8</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> Yes</td>
</tr>
<tr>
<td>CM_TEMP_SCRIPTS_DIR</td>
<td>Default path for saving temporary scripts.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> Any valid path on the Agent computer.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> $CONTROLM/runtime</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> Yes</td>
</tr>
<tr>
<td>CTM_PARM_ENC</td>
<td>Character used to enclose job processing parameters passed to jobs by CONTROL-M/Server. Any character or string can be specified. A blank space (in single or double quotes) is valid.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> Any character or string can be specified. A blank space (in single or double quotes) is also valid.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Double quotes</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
<tr>
<td>CTM_PRM_DONT_DELETE (Temporary Scripts Saving)</td>
<td>By default, temporary scripts generated from jobs are deleted at the end of job execution. If this value is set to <strong>YES</strong>, temporary scripts are not deleted.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> Yes and No</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> No</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> Yes</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CTM_PRM_KSH_FLAGS (Korn Shell Flags)</td>
<td>Indicates the shell flag that will be used to run the job script. For more information, see “Specifying the shell type” on page 131.</td>
</tr>
<tr>
<td></td>
<td>Default: -x</td>
</tr>
<tr>
<td>CTM_PRM_SH_FLAGS (Bourne Shell Flags)</td>
<td>Indicates the shell flag that will be used to run the job script. For more information, see “Specifying the shell type” on page 131.</td>
</tr>
<tr>
<td></td>
<td>Default: -x</td>
</tr>
<tr>
<td>CTM_SU_PATH</td>
<td>Alternative path that CONTROL-M/Server will use to look for the su command.</td>
</tr>
<tr>
<td></td>
<td>Default: /bin/su</td>
</tr>
<tr>
<td>PRINTER_NAME</td>
<td>Default printer for job output (SYSOUT).</td>
</tr>
<tr>
<td>PROCLOG_MODE</td>
<td>Octal value indicating file access mode of the Proclong (output) file. 777 indicates the highest level of access.</td>
</tr>
<tr>
<td></td>
<td>Default: 644</td>
</tr>
<tr>
<td>RJX_CONN_MODE</td>
<td>The RJX mode used in RJX jobs.</td>
</tr>
<tr>
<td>(AgentLess Connection Mode)</td>
<td>▪ 0 - The agent uses only the SSH protocol to upload and download files and to submit the job to the remote computer.</td>
</tr>
<tr>
<td></td>
<td>▪ 1 - The agent uses both SFTP and SSH protocols. Only one connection is opened during job execution.</td>
</tr>
</tbody>
</table>
### CM parameters for UNIX (part 3 of 5)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RJX_CONN_TRY</strong>&lt;br&gt;(AgentLess Connection Retries)</td>
<td>A maximum number of attempts to be made to restore the connection. &lt;br&gt;<strong>Default:</strong> 3&lt;br&gt;<strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
<tr>
<td><strong>RJX_CONN_TOUT</strong>&lt;br&gt;(Time Interval between Restore Connections)</td>
<td>The time interval, in seconds, between attempts to restore the connection. &lt;br&gt;<strong>Default:</strong> 120 seconds&lt;br&gt;<strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
<tr>
<td><strong>RJX_DETAILS_TO_SYSOUT</strong>&lt;br&gt;(Print Details to SYSOUT)</td>
<td>Determines whether to include details related to the remote connection in the job SYSOUT of jobs executed on a remote host. &lt;br&gt;<strong>Valid values:</strong> Y, N&lt;br&gt;<strong>Default:</strong> Y&lt;br&gt;<strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
<tr>
<td><strong>RJX_OVMS_DEFAULT_QUEUE</strong>&lt;br&gt;(Default Queue for OpenVMS Remote Host)</td>
<td>For a CONTROL-M/Agent submitting jobs to an OpenVMS remote host, the default batch queue to which the CONTROL-M/Agent submits jobs. &lt;br&gt;If this parameter is not specified, the CONTROL-M/Agent submits jobs to <code>sys$batch</code> (the system’s default batch queue). &lt;br&gt;<strong>Valid values:</strong> String consisting of 1 to 31 characters, including any uppercase and lowercase alphanumeric digits, the dollar sign ($), the underscore (_), and includes at least one alphabetic character. &lt;br&gt;<strong>Default:</strong> sys$batch&lt;br&gt;<strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
</tbody>
</table>
### Table 99 CM parameters for UNIX (part 4 of 5)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
</table>
| **RJX_OVMS_SETVERIFY**  <br>(Save Commands in the SYSOUT in OpenVMS Remote Host) | For a CONTROL-M/Agent submitting jobs to an OpenVMS remote host, this parameter specifies whether or not to print commands in the SYSOUT of a job.  
**Valid values:**  
- **Y** – Implements SET VERIFY, which prints commands in the job SYSOUT  
- **N** – Implements SET NOVERIFY, which does not print commands in the job SYSOUT  
- **E** – Specifies that the verification value is taken from the environment (account’s LOGIN.COM or SYLOGIN_VERIFY logical name)  
**Default:** Y |
| **RJX_SYSOUT_DIR**  <br>(AgentLess Temporary Directory) | A directory to store temporary files  
These files are automatically removed to CONTROL-M/Agent when the jobs end and the network connection is available or restored.  
**Default:** period (.), which means that the files are stored in the user home directory of the job’s owner in the remote host. |
| **SMTP_PORT_NUMBER**  <br>(Port Number) | The port number on which the SMTP server communicates.  
**Valid values:** 1024-65535  
**Default:** 25 |
| **SMTP_REPLY_TO_EMAIL**  <br>(Reply-To Email) | The e-mail address to which to send replies. If this field is left empty, the sender e-mail address is used. |
| **SMTP_SENDER_EMAIL**  <br>(Sender Email) | The e-mail address of the sender.  
**Default:** control@m |
| **SMTP_SENDER_FRIENDLY_NAME**  <br>(Sender Friendly Name) | The name or alias that appears on the e-mail sent. |
| **SMTP_SERVER_NAME**  <br>(SMTP Server (Relay) Name) | The name of the SMTP server. |
### Table 99   CM parameters for UNIX (part 5 of 5)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>SSH_VER_CMD</strong></td>
<td>SSH command to verify platform version.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> A valid command</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> cmd.exe /c ver</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
<tr>
<td><strong>SYSOUT_MODE</strong></td>
<td>Octal value indicating file access mode of the SYSOUT (output) file.</td>
</tr>
<tr>
<td></td>
<td>777 indicates the highest level of access.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> XXX, in which X is an integer between 0 an 7.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 660</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> No</td>
</tr>
<tr>
<td><strong>SYSOUT_NAME</strong></td>
<td>{JOBNAME</td>
</tr>
<tr>
<td>(Sysout Name)</td>
<td>If set to JOBNAME, parameter Jobname is used in the SYSOUT file instead of parameter Memname.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> JOBNAME, MEMNAME</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> MEMNAME</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> Yes</td>
</tr>
<tr>
<td><strong>TRANSLATE_$0</strong></td>
<td>For more information, see “Using the $0 Reserved Variable” on page 137.</td>
</tr>
<tr>
<td>(Replace $0 by File Name)</td>
<td></td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong></td>
</tr>
<tr>
<td></td>
<td>■ Y - Reserved variable $0 specifies whether instances of $0 in the</td>
</tr>
<tr>
<td></td>
<td>job script should be replaced before the script is run.</td>
</tr>
<tr>
<td></td>
<td>■ N - Functionality is disabled</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmunixcfg:</strong> Yes</td>
</tr>
</tbody>
</table>

### CM parameters for Windows

Table 100 lists the Control Module configuration parameters for Windows.
## Table 100  CM parameters for Windows (part 1 of 6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>APPLICATION_LOCALE</td>
<td>Determines the CJK encoding used by CONTROL-M/Agent to run jobs. For more information, see the CONTROL-M Language Customization Guide.</td>
</tr>
<tr>
<td>CJK Encoding</td>
<td><strong>Valid values:</strong> UTF-8, JAPANESE EUC, JAPANESE SHIFT-JIS, KOREAN EUC, SIMPLIFIED CHINESE GBK, SIMPLIFIED CHINESE GB, TRADITIONAL CHINESE EUC, TRADITIONAL CHINESE BIG5.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> UTF-8</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmwincfg:</strong> Yes</td>
</tr>
<tr>
<td>DFTPRT</td>
<td>Default printer for job SYSOUT files. Type a printer name in the field box or select a name from the list box.</td>
</tr>
<tr>
<td>Default Printer</td>
<td><strong>Valid values:</strong> Text</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Blank</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmwincfg:</strong> Yes</td>
</tr>
<tr>
<td>DOMAIN</td>
<td>The domain is determined by the value of this parameter if &lt;domain&gt; is not specified in &lt;domain&gt;&lt;username&gt; in the owner parameter of the job definition. If the domain is not specified in the owner parameter or this parameter, the user profile is searched in the trusted domains.</td>
</tr>
<tr>
<td>Logon Domain</td>
<td><strong>Note:</strong> BMC Software recommends that you do not specify a value for Logon Domain.</td>
</tr>
<tr>
<td></td>
<td><strong>Valid values:</strong> Text</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> Blank</td>
</tr>
<tr>
<td></td>
<td><strong>Modifiable by ctmwincfg:</strong> Yes</td>
</tr>
<tr>
<td>ECHO_SYSOUT</td>
<td>Specifies whether to print commands in the SYSOUT of a job.</td>
</tr>
</tbody>
</table>
| Echo Job Commands into Sysout | **Valid values:**  
  ■ Y – Implements ECHO_ON, which prints commands in the job SYSOUT  
  ■ N – Implements ECHO_OFF, which does not print commands in the job SYSOUT  
  **Default:** Y  
  **Modifiable by ctmwincfg:** Yes |
### Table 100 CM parameters for Windows (part 2 of 6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JOB_STATISTIC</td>
<td>Flag that indicates how to manage job object processing statistics.</td>
</tr>
<tr>
<td>(Add Job Object statistics to Sysout)</td>
<td></td>
</tr>
<tr>
<td>Valid values:</td>
<td></td>
</tr>
</tbody>
</table>
| ■ Y – Statistics are added to the end of the SYSOUT file.  
■ N – Statistics are not added to the SYSOUT file. |                                                                                                                                                                                                             |
| Default: Y                 |                                                                                                                                                                                                             |
| Modifiable by ctmwincfg:   | Yes                                                                                                                                                                                                        |
| JOB_WAIT                   | Flag that specifies if procedures invoked by a job can be run outside the Job Object. If so, this prevents a situation in which the original job remains in executing mode until the invoked procedure completes. |
| (Job children inside job object) |                                                                                                                                                                                                             |
| Valid values:              |                                                                                                                                                                                                             |
| ■ N – All procedures invoked by the job are run outside the job object.  
■ Y – All procedures invoked by the job are run inside the job object. |                                                                                                                                                                                                             |
| Default: Y                 |                                                                                                                                                                                                             |
| Modifiable by ctmwincfg:   | Yes                                                                                                                                                                                                        |
| LOGON_AS_USER              | Flag that specifies which user account is used for the services to log on to.                                                                                                                                 |
| (Logon As User)            |                                                                                                                                                                                                             |
| Valid values:              |                                                                                                                                                                                                             |
| ■ Y – Jobs are submitted with the permissions and environment variables of the specified user.  
■ N – Jobs are submitted with the permissions and environment variables of the local system account. |                                                                                                                                                                                                             |
| Default: Not selected      |                                                                                                                                                                                                             |
| Modifiable by ctmwincfg:   | Yes                                                                                                                                                                                                        |
### Table 100  CM parameters for Windows (part 3 of 6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJX_CONN_MODE</td>
<td>The RJX mode used in RJX jobs.</td>
</tr>
<tr>
<td>(AgentLess Connection Mode)</td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>■ 0 - The agent uses only the SSH protocol to upload and download files and to submit the job to the remote computer.</td>
</tr>
<tr>
<td></td>
<td>■ 1 - The agent uses both SFTP and SSH protocols. Only one connection is opened during job execution.</td>
</tr>
<tr>
<td></td>
<td>■ 2 - The agent used both SFTP and SSH protocols. Two connections are opened at the beginning of the job, but after a while the SSH connection is closed.</td>
</tr>
<tr>
<td></td>
<td>Default: 2</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: No</td>
</tr>
<tr>
<td>RJX_CONN_TRY</td>
<td>maximum number of attempts to be made to restore the connection</td>
</tr>
<tr>
<td>(AgentLess Connection Retries)</td>
<td>Valid values: Integer</td>
</tr>
<tr>
<td></td>
<td>Default: 3</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: No</td>
</tr>
<tr>
<td>RJX_CONN_TOUT</td>
<td>time interval, in seconds, between attempts to restore the connection</td>
</tr>
<tr>
<td>(Time Interval between Restore Connections)</td>
<td>Valid values: Integer</td>
</tr>
<tr>
<td></td>
<td>Default: 120 seconds</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: No</td>
</tr>
<tr>
<td>RJX_DETAILS_TO_SYSOUT</td>
<td>Determines whether to include details related to the remote connection in the job SYSOUT of jobs executed on a remote host.</td>
</tr>
<tr>
<td>(Print Details to SYSOUT)</td>
<td>Valid values: Y, N</td>
</tr>
<tr>
<td></td>
<td>Default: Y</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: No</td>
</tr>
</tbody>
</table>
Table 100  CM parameters for Windows (part 4 of 6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>RJX_OVMS_DEFAULT_QUEUE</td>
<td>For a CONTROL-M/Agent submitting jobs to an OpenVMS remote host, the default batch queue to which the CONTROL-M/Agent submits jobs. If this parameter is not specified, the CONTROL-M/Agent submits jobs to sys$batch (the system’s default batch queue). <strong>Valid values:</strong> String consisting of 1 to 31 characters, including any uppercase and lowercase alphanumeric digits, the dollar sign ($), the underscore (_), and includes at least one alphabetic character. <strong>Default:</strong> sys batch <strong>Modifiable by ctmwincfg:</strong> No</td>
</tr>
</tbody>
</table>
| RJX_OVMS_SETVERIFY | For a CONTROL-M/Agent submitting jobs to an OpenVMS remote host, this parameter specifies whether or not to print commands in the SYSOUT of a job. **Valid values:** ■ Y – Implements SET VERIFY, which prints commands in the job SYSOUT ■ N – Implements SET NOVERIFY, which does not print commands in the job SYSOUT ■ E – Specifies that the verification value is taken from the environment (acco)
**Modifiable by ctmwincfg:** No |
| RJX_SYSOUT_DIR | A directory to store temporary files These files are automatically removed to CONTROL-M/Agent when the jobs end and the network connection is available or restored. **Default:** period (.), which means that the files are stored in the user home directory of the job’s owner in the remote host. **Modifiable by ctmwincfg:** No |
| RUN_USER_LOGON_SCRIPT | Indication if a user-defined logon script should be run by the CONTROL-M/Agent before running the standard user logon script. **Valid values:** ■ Y – The user-defined logon script is run, if it exists. ■ N – The user-defined logon script is not run. **Default:** N **Modifiable by ctmwincfg:** Yes |
Table 100  CM parameters for Windows (part 5 of 6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SMTP_PORT_NUMBER (Port Number)</td>
<td>The port number on which the SMTP server communicates.</td>
</tr>
<tr>
<td></td>
<td>Valid values: 0-65535</td>
</tr>
<tr>
<td></td>
<td>Default: 25</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
<tr>
<td>SMTP_REPLY_TO_EMAIL (Reply-To Email)</td>
<td>The e-mail address to which to send replies. If this field is left empty, the sender e-mail address is used.</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
<tr>
<td>SMTP_SENDER_EMAIL (Sender Email)</td>
<td>The e-mail address of the sender.</td>
</tr>
<tr>
<td></td>
<td>Valid values: Text up to 99 characters</td>
</tr>
<tr>
<td></td>
<td>Default: control@m</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
<tr>
<td>SMTP_SENDER_FRIENDLY_NAME (Sender Friendly Name)</td>
<td>The name or alias that appears on the e-mail sent.</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
<tr>
<td>SMTP_SERVER_NAME (SMTP Server (Relay) Name)</td>
<td>The name of the SMTP server.</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
<tr>
<td>SSH_VER_CMD</td>
<td>SSH command to verify platform version.</td>
</tr>
<tr>
<td></td>
<td>Valid values: A valid command.</td>
</tr>
<tr>
<td></td>
<td>Default: cmd.exe /c ver</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: No</td>
</tr>
<tr>
<td>SYSOUT_NAME (Sysout Name)</td>
<td>Determines the prefix for the SYSOUT file name.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>- MEMNAME – the SYSOUT file prefix is the MEMNAME of the job.</td>
</tr>
<tr>
<td></td>
<td>- JOBNAME – the SYSOUT file prefix is the JOBNAME of the job.</td>
</tr>
<tr>
<td></td>
<td>Default: Memnam</td>
</tr>
<tr>
<td></td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
</tbody>
</table>
Table 100  CM parameters for Windows (part 6 of 6)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>WRAP_PARAM_QUOTES</td>
<td>Indication of how parameter values (%%PARMn,...,%%PARMx) are managed by CONTROL-M/Agent for Microsoft Windows.</td>
</tr>
<tr>
<td></td>
<td>Valid values:</td>
</tr>
<tr>
<td></td>
<td>1 – This parameter is no longer relevant.</td>
</tr>
<tr>
<td></td>
<td>2 – Parameter values are always passed to the operating system without quotes. If quotes were specified in the job definition, they are removed before the parameter is passed onward by the agent. This option is compatible with the way that these parameters were managed in version 6.0.0x, or 6.1.01 with Fix Pack 1, 2, 3, or 4 installed. In this case, if a parameter value contains a blank, the operating system may consider each string as a separate parameter.</td>
</tr>
<tr>
<td></td>
<td>3 – This parameter is no longer relevant.</td>
</tr>
<tr>
<td></td>
<td>4 – Parameters are passed to the operating system in exactly the same way that they were specified in the job definition. No quotes are added or removed in this case. This option is compatible with the way that parameters were managed by version 2.24.0x.</td>
</tr>
<tr>
<td>Default: 2</td>
<td>Modifiable by ctmwincfg: Yes</td>
</tr>
<tr>
<td>WMI_SETUP_SHARE</td>
<td>Indicates whether the agent will create a shared directory on a remote host.</td>
</tr>
<tr>
<td></td>
<td>Valid values: Y, N</td>
</tr>
<tr>
<td>Default: Y</td>
<td>Modifiable by ctmwincfg: No</td>
</tr>
</tbody>
</table>

CONTROL-M Agent services parameters

Table 101 lists parameters that affect the operation of the following CONTROL-M/Agent services:

- Agent service
- FileWatcher service
Table 101 System configuration for CONTROL-M/Agent services

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Log on as</td>
<td>User account under which CONTROL-M Agent service will run.</td>
</tr>
<tr>
<td>Valid values:</td>
<td></td>
</tr>
<tr>
<td>■ Local System Account – Service logs on as the system account.</td>
<td></td>
</tr>
<tr>
<td>— Allow Service to Interact with Desktop – This option is valid only if the service is running as a local system account. See “Defining a CONTROL-M/Agent account (Windows only)” on page 170.</td>
<td></td>
</tr>
<tr>
<td>Selected – the service provides a user interface on a desktop that can be used by whoever is logged in when the service is started. Default.</td>
<td></td>
</tr>
<tr>
<td>Unselected – the service does not provide a user interface.</td>
<td></td>
</tr>
<tr>
<td>■ This Account – User account under which CONTROL-M Agent service will run.</td>
<td></td>
</tr>
<tr>
<td>For more information, see “Defining a CONTROL-M/Agent account (Windows only)” on page 170.</td>
<td></td>
</tr>
<tr>
<td>Note: If the owner of any CONTROL-M/Server jobs has a “roaming profile” or if job output (SYSOUT) will be copied to or from other computers, the Logon mode must be set to This Account.</td>
<td></td>
</tr>
<tr>
<td>Default: Local System Account</td>
<td></td>
</tr>
<tr>
<td>Startup Type</td>
<td>How to install CONTROL-M/Agent service.</td>
</tr>
<tr>
<td>Valid values:</td>
<td></td>
</tr>
<tr>
<td>■ Automatic – Service should start when the system starts.</td>
<td></td>
</tr>
<tr>
<td>■ Manual – User or a dependent service can start service.</td>
<td></td>
</tr>
<tr>
<td>■ Disabled – User or a dependent service cannot start service.</td>
<td></td>
</tr>
<tr>
<td>Default: Automatic</td>
<td></td>
</tr>
</tbody>
</table>
Exits

This section presents the following topics:

User Exits ................................................................. 523
  Job Order Exit (CTMUE101) ........................................ 524
  Job Submission Exit (CTMUE102) ................................. 525
  Before New Day Procedure Exit (CTMUE103) .................... 527
  After New Day Procedure Exit (CTMUE104) ..................... 527
  Before User Daily Exit (CTMUE105) .............................. 528
  After User Daily Exit (CTMUE106) ................................ 528
Watchdog facility exits ................................................ 528
  Enabling the Watchdog facility to run the ctmdiskspace or ctmdbspace utilities, or other scripts ........................................ 529
  Enabling the Watchdog facility to run the user-defined scripts or CONTROL-M/Server utilities ........................................ 530
  Defining the error handler criteria for the Watchdog facility .......... 531

User Exits

This section describes the following topics:

  ■  Job Order Exit (CTMUE101)
  ■  Job Submission Exit (CTMUE102)
  ■  Before New Day Procedure Exit (CTMUE103)
  ■  After New Day Procedure Exit (CTMUE104)
  ■  Before User Daily Exit (CTMUE105)
  ■  After User Daily Exit (CTMUE106)
Job Order Exit (CTMUE101)

This exit is executed for each CONTROL-M job before it is ordered. The flat text file passed to the exit is a job record from the Scheduling definition table. User exit CTMUE101 can be used to alter the job information in this file after it is fetched from the database and before it is passed to the procedure that determines if the job will be ordered for the current day.

The following is a sample text file in the format that is passed to the CTMUE101 exit:

```
JOBNAME daily_job
JOBNO 30
DESCRIPT
APPLIC STRESS
APPLGROUP STRESS
SCHEDTAB STRESS
AUTHOR ctm600
OWNER ctm600
PRIORITY 0
CRITICAL N
CYCLIC N
RETRO N
AUTOARCH N
TASKCLASS
CYCLICINT 0
TASKTYPE C
DATEMEM
NODEGRP
computer
NODEID
DOCLIB
DOCMEM
MEMLIB
MEMNAME
OVERLIB
CMDLINE ./stress_cmd_spl.ctm600
MAXRERUN 0
MAXDAYS 0
MAXRUNS 0
FROMTIME
UNTIL
MAXWAIT 0
DAYSTR ALL
WDAYSTR
MONTHSTR YYYYYYYYYYYY
AJFSONSTR NNNNNNNNNNNN
CONF N
UNKNOWNTIM 0
DAYSCL
WEEKCAL
```
Example

The following exit script changes the Days parameter (DAYSTR) for jobs that were scheduled on the first day of the month, so that these jobs will be ordered on the second day of the month.

```bash
#!/bin/ksh
cp $1 /tmp/ue101.$$ 
sed -e 's/DAYSTR 1/DAYSTR 2/' /tmp/ue101.$$ > $1
```

Job Submission Exit (CTMUE102)

This exit is executed for each CONTROL-M job before it is submitted for execution. The flat text file passed to the exit contains a job record from the Active Job File table. User exit CTMUE102 can be used to alter job information in this record before it is passed to the CONTROL-M/Agent for job submission.

The following is a sample text file in the format that is passed to the CTMUE102 exit:

```
JOBNO 0
ORDERNO 19450
PRIORITY 1039
CRITICAL N
TASKTYPE C
CYCLIC N
CONFIRM_R N
CONFIRMED N
RETO N
AUTOARCH N
TASKCLASS
HOLDFLAG N
STATUS N
STATE E
CYCLICINT 0
```
Example

The following exit script checks if the job has a Owner of root and changes the Owner for these jobs to nobody.

```ksh
#!/bin/ksh
cp $1 /tmp/ue102.$$
sed -e 's/OWNER root/OWNER nobody/' /tmp/ue102.$$ > $1
```
Before New Day Procedure Exit (CTMUE103)

This exit is executed before the New Day procedure is run. The New Day Procedure performs automatic functions at the beginning of each new CONTROL-M working day. This procedure is used as a master scheduler for all CONTROL-M activities. For more information, see “Methods for automating daily job scheduling” on page 81.

The flat text file that is passed to the exit contains the name of the Daily (SYSTEM), time, and original scheduling date (Odate) of the procedure.

The following is a sample text file in the format that is passed to the CTMUE103 exit:

```
DAILY_NAME SYSTEM
TIME 1300
ODATE 20001121
```

Example

The following exit script runs a procedure that performs various actions before the New Day procedure is run.

```
#!/bin/ksh
/opt/controlm/scripts/run_pre_New_Day_proc
```

After New Day Procedure Exit (CTMUE104)

This exit is executed after each run of the CONTROL-M New Day procedure. The flat text file that is passed to the exit contains the name of the Daily (SYSTEM), time, and original scheduling date (Odate) of the procedure.

The following is a sample text file in the format that is passed to the CTMUE104 exit:

```
DAILY_NAME SYSTEM
TIME 1319
ODATE 20001121
```

Example

The following exit script runs a procedure that performs various actions after completion of the New Day procedure.

```
#!/bin/ksh
/opt/controlm/scripts/run_post_New_Day_proc
```
Before User Daily Exit (CTMUE105)

This exit is executed before each CONTROL-M User Daily job (except SYSTEM) is run. User Daily jobs can be used to order new jobs. For more information, see “Methods for automating daily job scheduling” on page 81.

The flat text file that is passed to the exit contains the name of the User Daily, time, and original scheduling date (Odate) of the User Daily job.

The following is a sample text file in the format that is passed to the CTMUE105 exit:

```
DAILY_NAME my_daily
TIME 1321
ODATE 20001121
```

After User Daily Exit (CTMUE106)

This exit is executed after each CONTROL-M User Daily job (except SYSTEM) is run. User Daily jobs can be used to order new jobs. For more information, see “Methods for automating daily job scheduling” on page 81.

The flat text file that is passed to the exit contains the name of the User Daily, time, and original scheduling date (Odate) of the User Daily job.

The following is a sample text file in the format that is passed to the CTMUE106 exit:

```
DAILY_NAME my_daily
TIME 1322
ODATE 20001121
```

**NOTE**

If the User Daily job fails, the User Exit 106 (UE106) will not be executed.

Watchdog facility exits

This section describes the following topics:

Enabling the Watchdog facility to run the ctmdiskspace or ctmdbspace utilities, or other scripts
Enabling the Watchdog facility to run the ctmdiskspace or ctmdbspace utilities, or other scripts

1 Determine which utilities you want the Watchdog process to run, and set the # value in the WD_CTMEXIT_# system parameter accordingly:

- To run only the ctmdiskspace utility, set the # to 1 (enables WD_CTMEXIT_1).
- To run both the ctmdiskspace and ctmdbspace utilities, set the # to 2 (enables both WD_CTMEXIT1 and CTMEXIT2).
- (To disable the exits, set the # to 0).

2 If the facility should run a user-defined script:

A Specify the file name of the script or binary that resides in the ctm_server/exe_<operatingSystem> directory in the WD_CTMEXIT_#_SCRIPT_FILE parameter.

B Define the parameters to be passed to the exit script in the WD_CTMEXIT_#_CMD_LINE parameter.

C Define the message to be sent if the exit script fails in the WD_CTMEXIT_#_ERROR_MSG parameter.

3 Define the number of basic time interval units that should pass before re-invoking the exit script in the WD_CTMEXIT_#_INTERVAL parameter. Range: 1-1440. Default: 20

The basic time interval unit is defined in parameter WD_INTERVAL. For example, if the value of this parameter is 20, and the basic time interval unit (as defined in parameter WD_INTERVAL) is 6 minutes, the exit script will be invoked every 120 minutes (20 x 6 minutes).

4 Define the number of minutes that should be allowed to pass before the exit script is terminated in the WD_CTMEXIT_#_TIMEOUT parameter.

5 Define situation under which the exit script should or should not run, as follows:
Enabling the Watchdog facility to run the user-defined scripts or CONTROL-M/Server utilities

- If the exit script should be run when CONTROL-M/Server is running, set the value of the WD_CTMEXIT_#_RUN_STATE parameter to Y. Otherwise, set the value to or N.

- If the exit script should be run when CONTROL-M/Server is suspended, set the value of the WD_CTMEXIT_#_SUSPEND_STATE parameter to Y. Otherwise, set the value to or N.

Enabling the Watchdog facility to run the user-defined scripts or CONTROL-M/Server utilities

1. Specify the number of user exit to be enabled in the WD_USEREXIT_# system parameter by replacing the # with that number. (Specify 0 to disable all user-defined Watchdog user exits.)

2. Specify the file name of the script or binary that resides in the ctm_server/exe_<computer> directory in the WD_USEREXIT_#_SCRIPT_FILE parameter.

3. Define the parameters to be passed to the exit script in the WD_USEREXIT_#_CMD_LINE parameter.

4. Define the message to be sent if the exit script fails in the WD_USEREXIT_#_ERROR_MSG parameter.

5. Define the number of basic time interval units that should pass before rerunning the exit script in the WD_USEREXIT_#_INTERVAL parameter. Range: 1-1440. Default: 20

   The basic time interval unit is defined in parameter WD_INTERVAL. For example, if the basic time interval unit (as defined in parameter WD_INTERVAL) is 6 minutes, and you set the value of this parameter to 20, the exit script will be run every 120 minutes (20 x 6 minutes).

6. Define the number of minutes that should be allowed to pass before the exit script is terminated in the WD_USEREXIT_#_TIMEOUT parameter.

7. Define situation under which the exit script should or should not run, as follows:

   - If the exit script should be run when CONTROL-M/Server is running, set the value of the WD_USEREXIT_#_RUN_STATE parameter to Y. (Otherwise, set the value to or N.)
If the exit script should be run when CONTROL-M/Server is suspended, set the value of the WD_USEREXIT_#_SUSPEND_STATE parameter to Y. (Otherwise, set the value to or N.)

**Example**

CONTROL-M/Server **ctmping** utility can be added to the Watchdog facility to automatically test the communication link between CONTROL-M/Server and agent computers and update the available agent list. Add the following parameters to the *config.dat* file:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>WD_USEREXIT_1_CMD_LINE</td>
<td><code>~&lt;controlm_owner&gt;/ctm_server/ctmuser/agntlist</code></td>
</tr>
<tr>
<td>WD_USEREXIT_1_ERROR_MSG</td>
<td>Agent not available</td>
</tr>
<tr>
<td>WD_USEREXIT_1_INTERVAL</td>
<td>5</td>
</tr>
<tr>
<td>WD_USEREXIT_1_RUN_STATE</td>
<td>Y</td>
</tr>
<tr>
<td>WD_USEREXIT_1_SCRIPT_FILE</td>
<td><code>$HOME/ctm_server/exe_AIX/ctmping</code></td>
</tr>
<tr>
<td>WD_USEREXIT_1_SUSPEND_STATE</td>
<td>N</td>
</tr>
<tr>
<td>WD_USEREXIT_1_TIMEOUT</td>
<td>5</td>
</tr>
</tbody>
</table>

---

**Defining the error handler criteria for the Watchdog facility**

If the error handler should be a user-defined script, define the following:

1. Define the full path and script name in the WD_ERROR_HANDLER_SCRIPT_FILE parameter.

2. Define the maximum time the Watchdog facility should wait for the user defined script to run in the WD_ERROR_HANDLER_TIMEOUT parameter.
This appendix presents the following topics:

Overview ................................................................. 533
CONTROL-M/EM and SNMP traps .................................. 534
   SNMP trap format ................................................. 534
Customization .......................................................... 535

One of the most powerful components in the CONTROL-M/Enterprise Manager “management by exception” arsenal is the use of Alerts. By having jobs issue alert messages when an abnormal situation is encountered, CONTROL-M/EM enables you to focus attention on those areas requiring human intervention, while allowing other production jobs to continue.

CONTROL-M/EM carries this concept one step further by enabling alerts to be directed to a Network Management application, allowing the network manager to be included in the list of alert recipients.

Overview

The Simple Network Management Protocol (SNMP) helps network managers locate and correct network problems (usually in a TCP/IP network). Managers invoke an SNMP client (usually under a network management application) on their local computer and use the client to contact one or more SNMP servers (or agents) that execute on remote computers.

A special SNMP message type, called a trap message, is the only type that is initiated by a server. A trap message informs the client about an event that has occurred at the server computer, usually a failure event (hardware or software, permanent or temporary). Customization at the client site determines, according to the trap codes, whether an Alert message appears on the manager’s screen or whether the recording of an event log message is sufficient. The trap message can carry additional MIB variables, thereby providing additional information to the client application.
CONTROL-M/EM and SNMP traps

When an alert is posted to the Alerts window or an existing alert is changed by a CONTROL-M/EM user, a standard SNMP trap message can optionally be issued to the host of the relevant network management application.

CONTROL-M/EM functioning, including the generation of a trap message, is not affected in any way if the management application is not active.

The generated SNMP traps are enterprise-specific traps (that is, field generic-trap is set to 6).

SNMP trap format

The trap consists of 20 distinct SNMP variables (described in Table 102). There is one specific trap type: Specific-trap 10: CONTROL-M/EM alerts.

SNMP traps issued using CONTROL-M/EM consist of the following fields:

Table 102  SNMP trap format (part 1 of 2)

<table>
<thead>
<tr>
<th>#</th>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| 1  | UPDATE TYPE   | Single character indicating the type of event that triggered the alert:  
■ I — A new alert was issued.  
■ U — An existing alert was updated.                      |
| 2  | ALERT ID      | Numeric value used as a key (index) to identify the alert.                                                                               |
| 3  | CONTROLM      | Name of the data center to which the job belongs.                                                                                          |
| 4  | MEMNAME       | Mem Name of the job.                                                                                                                        |
| 5  | ORDER ID      | Order ID of the job.                                                                                                                        |
| 6  | SEVERITY      | Severity of the alert:  
■ V — Very urgent  
■ U — Urgent  
■ R — Regular                                                        |
| 7  | STATUS        | Values: Not noticed, Noticed, or Handled.                                                                                                  |
| 8  | TIME          | Time and date that the alert was issued. Format: yyyy:mmddhhmss                                                                        |
| 9  | USER          | Name of the user who last modified the status or text of the alert                                                                       |
| 10 | UPDATE TIME   | Time and date that the alert was last modified by the user                                                                               |
| 11 | MESSAGE       | Full text of the alert                                                                                                                      |
| 12 | OWNER         | Owner of the job                                                                                                                           |
| 13 | GROUP         | Group of the job                                                                                                                           |
The customization procedures, described below, are required to support SNMP traps issued by CONTROL-M/EM.

The Services file may need to be updated to include the SNMP monitor trap port. The following entry must be added to the /etc/services file (on UNIX) or WINDIR\system32\drivers\etc\Services file (on Microsoft Windows), if not already present. After adding the line, verify that the host of the relevant network management application is listening to the port number indicated in this line:

```
snmp-trap 162/udp # snmp monitor trap port
```

In addition, the following parameters must be modified using the CONTROL-M Configuration Manager:

- SnmpSendActive
- SnmpHost
- SendSnmp

For more information about these system parameters, see Table 70 on page 414.

## Modifying each SNMP parameter

SNMP parameters are accessed from the System Parameters window of the CONTROL-M Configuration Manager. For information about modifying system parameters, see “Modifying CONTROL-M/Server system parameters” on page 406.
The network management application must first be customized so that it recognizes the Enterprise ID (1031) of CONTROL-M/EM alert. Next, the corresponding trap codes must be defined.

**MIB file location**

The SNMP format is described in a MIB (Management Information Base) file. The file name is CONTROLMEM-MIB.txt, and can be found in the `<emHome\Data>` directory.
Mass conversion of agents and remote hosts

The following topic describes how to perform a mass conversion of CONTROL-M/Agents to remote hosts:

Converting multiple CONTROL-M/Agents to remote hosts . . . . . . . . . . . . . . . . . . . . . . . 537

For instructions on converting individual agents to remote hosts, see page 70.
For instructions on converting a remote host to a CONTROL-M/Agent, see page 67.

Converting multiple CONTROL-M/Agents to remote hosts

1 Ensure that no jobs have been submitted or are running on the required agents.

2 Determine all the owners that are used on the agent computers, as follows:

   Log onto the database server and run the following SQL commands to determine all the owners used on the agent computer:

   ```sql
   select OWNER from CMR_AJF where lower(NODEID)='<agentNameToBeConverted>'
   union
   select OWNER from CMS_JOBDEF where lower(NODEGRP)= '<agentNameToBeConverted>' or exists
   (select 1 from CMS_NODGRP where GRPNAME=CMS_JOBDEF.NODEGRP and lower(NODEID)= '<agentNameToBeConverted>')
   ```

   Add one of the following on a separate line at the end of the commands:

   - For Oracle or PostgreSQL: ;
   - For Sybase or MSSQL: go
The `<agentNameToBeConverted>` variable must be specified in lower case.

--- EXAMPLE ---
To convert a node with the name cyborg on Oracle, log onto the sql database server and run the following commands to determine all the owners used on cyborg:

```sql
select OWNER from CMR_AJF where lower(NODEID)='cyborg'
union
select OWNER from CMS_JOBDEF where lower(NODEGRP)='cyborg' or exists
(select 1 from CMS_NODGRP where GRPNAME=CMS_JOBDEF.NODEGRP and
lower(NODEID)='cyborg')
```

---

3 Define all the owners, and their authentication settings, that you identified in step 2. You can do this using either of the following tools:

- CONTROL-M Configuration Manager—for instructions, see “Defining job owner and authentication settings for CONTROL-M/Agents and remote hosts” on page 173.

- `ctmsetown` utility—you can run a script using the `ctmsetown` utility to define all the owners used on the agent computers. For more information, see the `CONTROL-M Utility Guide`.

4 For each agent, verify once more that no jobs have been submitted or are running.

5 Using the CONTROL-M/Configuration Manager, shut down the agents.

6 Redefine each relevant agent as a remote host, using either of the following methods:

- Run the `ctmhostmap` utility with the `-force` option. For more information, see `CONTROL-M Utility Guide`.

- Use the CONTROL-M Configuration Manager to perform one of the following:
  
  — If the remote host should be connected using default communication settings, delete the agents. Once a job is scheduled on the node, the remote host will be automatically configured.

  — If the remote host should be connected using non-default communication settings, use the Convert to Remote Host option in the CONTROL-M Configuration Manager.

The remote hosts are now configured.
Working with Remedy

The following topics in this section describe how to configure the connection to the Remedy server:

- Configuring the connection to the Remedy server ........................................ 539
- Refining Remedy incident information ...................................................... 540

Configuring the connection to the Remedy server

The connection to the Remedy server is configured using the remedy_configure interactive utility. The utility enables you to set connection parameters to the Remedy server, and to test the connection using the new parameters.

Setting basic connection parameters

To set the basic connection parameters

1. Enter remedy_configure.

2. Select the appropriate menu items, and enter the required information.

3. Enter s, to save the configuration.

The utility sets the Remedy server host name, port, user name, and password. The configuration parameters, except for the encrypted password, are saved in the RemedyConf.xml file.

For the location of the utility and the configuration file, see Table 103 and Table 104.
Refining Remedy incident information

NOTE
When Remedy Server is configured to use a “port mapper” the Remedy port should be set to 0 (default), otherwise the port is the Remedy server port.

Testing the connection to the Remedy server

The test option, provided by the utility, creates a low urgency incident in the Remedy server using default values. The incident is only used to test the configuration parameters.

Table 103 Location of the Remedy configuration utility - remedy_configure

<table>
<thead>
<tr>
<th>Environment</th>
<th>Windows</th>
<th>UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-EM</td>
<td>&lt;EM home&gt;\bin</td>
<td>&lt;EM home&gt;/scripts</td>
</tr>
<tr>
<td>CONTROL-M</td>
<td>&lt;CTM server home&gt;\Exe</td>
<td>&lt;CTM server home&gt;/scripts</td>
</tr>
</tbody>
</table>

Table 104 Location of the Remedy configuration file - RemedyConf.xml

<table>
<thead>
<tr>
<th>Environment</th>
<th>Windows</th>
<th>UNIX</th>
</tr>
</thead>
<tbody>
<tr>
<td>CONTROL-EM</td>
<td>&lt;EM home&gt;\data\REMEDY</td>
<td>&lt;EM home&gt;/appl/ecs/cli/data/REMEDY</td>
</tr>
<tr>
<td>CONTROL-M</td>
<td>&lt;CTM server home&gt;\data\REMEDY</td>
<td>&lt;CTM server home&gt;/data/REMEDY</td>
</tr>
</tbody>
</table>

Refining Remedy incident information

The Remedy configuration file consists of three sections. The first section contains the connection settings, which are set using the remedy_configure interactive utility (see “Setting basic connection parameters” on page 539).

The other two sections contain configuration settings that are specific for each Remedy server version. The first section is for Remedy 6, while the second is for Remedy 7.

Each Remedy server version contains two Action configurations; one for opening the incidents and one for closing them. Each Action configuration contains the form name used for the specific action as shown in the following table. The schema name is used for the form name.

Table 105 Form names used for opening and closing incidents (part 1 of 2)

<table>
<thead>
<tr>
<th>Server</th>
<th>Action</th>
<th>Form name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Remedy 6</td>
<td>open</td>
<td>HPD:HelpDesk</td>
</tr>
<tr>
<td></td>
<td>close</td>
<td>HPD:HelpDesk</td>
</tr>
</tbody>
</table>
An incident form can either be created directly (the default process for Remedy 6) or indirectly (the default process for Remedy 7) by the Remedy server. When the indirect process is used to create an incident form, the Remedy server first creates an intermediate form that contains an ID number that identifies the real (target) form. The intermediate form must be resolved to obtain the real form ID.

To use the indirect process

1. For the ResolveRealFormID, specify Yes.

2. For the RealFormFieldID, specify a field ID number, that will contain the real form ID.

When Remedy incidents are created, default values are used for each of the Remedy incident fields. The default values are listed in the RemedyConf.XML file (for the location of the configuration file, see Table 104). Each Remedy incident field consists of the following attributes:

- **Name** - field description
- **ID** - Remedy field identification number
- **Data Type** - either a string field (indicated by the number 4) or a selection field (indicated by the number 6)
- **Value** - default value used

The Remedy field ID values for additional Remedy fields must be obtained from the Remedy administrator.

The configuration file contains the following built-in Remedy fields that are automatically populated by BMC Batch Manager and CONTROL-M/Server.

- **Summary**
- **Note**
- **Urgency**

**NOTE**

The built-in fields are used to resolve the field ID in the Remedy form. When BMC Batch Manager or CONTROL-M/Server creates an incident, the built-in fields are automatically resolved, overwriting any values that may have been manually specified. For more information about Remedy fields and parameters, see the Remedy documentation.
Index

Symbols

"Context" parameter
  DIAG ini file 334
# ! statement 135
$0 reserved variable 137
%errorlevel%
  exit code 141
*default parameter
  DIAG ini file 333
.bat
  DOS batch files 142
.cmd
  REXX-language 142
cshrc file 134
.login file 134
.profile file 134
_sleep utility 141

A

Action code field
  GCS_LOG record 374, 375
Action_OrderForce__AuthLevel system parameter 439
Active Jobs file
  downloading 368, 369
  erasing contents 369
  forcing download 368
  time zones 111
Active shout table
  system parameter 454
ACU
  CONTROL-M Agent Check utility 344
diagnostic data 344
Add Backup Device option
  Database Maintenance 294
ADD_SYSOUT_TO_EMAIL
  e-mail configuration parameter 494
ADD_SYSOUT_TO_EMAIL_LIMIT_SIZE
  e-mail configuration parameter 494
ADD_SYSOUT_TO_EMAIL_TIMEOUT_LIMIT
  e-mail configuration parameter 494
adding
  backup devices 294
AddJobsChunkSize system parameter 439
  address policy
  Domain Settings panel 389
ADJUST_COND
  parameter 484
Advanced button
  Summary Panel 400
Advanced settings panel
  actions 401
tree format 400
AG_LOG_ON
  configuration parameter 506
AGCMNDATA
  configuration parameter 506
Agent communication parameters
  description 464
Agent platforms
  communication parameters 464
  Shout messages to 118
AGENT_DIR
  configuration parameter 506
AGENT_STATUS
  configuration parameter 506
agentless job submission 52
AGENTS_CLEANUP_IN_NEWDAY
  Server parameter 480
Agent-to-Server
  port number 459
Agent-to-Server Port Number parameter 459
ALARM_DEST
  Server parameter 480
Alert data processing facility 88
ALERT ID
  SNMP trap 534
  alert processing
description 88
  SNMP interface 533
  SNMP trap or script 88
AlertOnAbend system parameter 425
AlertReaderRetries system parameter 433
Alerts window
  DIAG component prefix 372
AlertsMapRefreshInterval system parameter 433
APPLICATION_LOCALE
  configuration parameter 510, 515
applications
  SNMP trap 535
AR_AG_COMM_PORT
configuration parameter 506
AR_AT_COMM_PORT
configuration parameter 507
AR_UT_COMM_PORT
configuration parameter 507
assigning ports 222, 391
ATCMNDATA
configuration parameter 507
Audit facility overview 211
audit records 307
auth_userpassword function 158
authentication task summary 184, 213, 268
workflow 179, 212, 218, 264
authentication settings 173
AuthenticationLevel system parameter 439
AuthenticationMethod system parameter 159, 415
Author parameter authorization to modify 197
authorization checking
CONTROL-M clients 214
Authorization facility 179
AuthorSecurity system parameter 197, 199, 440
AUTOEDIT_INC_SEC parameter 481
AUTOEDIT_INLINE
configuration parameter 507
automated job scheduling 81

backup
Oracle 293
Sybase 292
backup device dropping 295
Backup Socket port number Sybase 470
bidirectional communication disabling 390
IIOP 389, 395
BMC Software, contacting 2
Browse access level communication 189
Prerequisite Conditions panel 195
Scheduling Tables panel 192, 196
bulk_act_cond system parameter 440
bulk_act_grp system parameter 440
bulk_act_job system parameter 441
bulk_act_res system parameter 441
bulk_def_size system parameter 415
bulk_def_storage_len system parameter 415
bulk_send_int parameter Defaults.rsc file 429
bulk_send_max parameter

Defaults.rsc file 429

C

CALL TYPE SNMP trap 534
Callback mechanism firewall penetration 389
catior utility stringified IORs 388
CD_MAX_DBU communication parameter 460
CDROM name Oracle parameter 472
ChallengeResponseTimeout system parameter 415
CHANGE_LOG command ctl utility 337
ChangePassword system parameter 438
character set
Sybase SQL server 242
Check Kernel Configuration parameter 368
clean_old_int parameter
Defaults.rsc file 429
client cannot connect to server troubleshooting 360
CloseOldDownloads system parameter 441
CM_APL_TYPE configuration parameter 507
CM_LIST configuration parameter 507
CM_TEMP_SCRIPTS_DIR configuration parameter 510
cnd data flag
GCS_LOG file 375
Code field
CONTROL-M Definition window 59
collecting diagnostic data 343
comchkn data flag
GCS_LOG file 375
COMM_TRACe configuration parameter 507
comm_userid parameter Defaults.rsc file 202
COMMLOPT configuration parameter 508
COMMRETSLP configuration parameter 508
communication
Agent platforms 464
bidirectional 389
gateway log file 372
parameter descriptions 459
Timeout parameter 465
Communication Protocol parameter 459
Communication Protocol Version parameter 465
Comp. Name field
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

ViewpointPolicy system parameter 126
component state
down 265
hanging 265
up 265
ComponentRestartInterval system parameter 435
ComponentShowState system parameter 435
compound name
sequence of names 384
computer aliases
support for 360
Computer System parameter 454
COMTIMOUT
Agent parameter 462
COMTRYNO
Server parameter 462
ConcurrentCollections system parameter 441
config.dat file
parameters 478
watchdog parameters 498
Configuration Agent Port
Server parameter 460
Configuration agents
DIAG component prefix 372
configuration files
CORBA 383
scopes 391
configuration parameters
Watchdog 498
connection technologies 62
continue_not_responding parameter
Defaults.rsc file 452
Control resources
deleting 369
Control Shell 273, 337, 338
CONTROL-M
main menu 406
menu system 103
CONTROL-M Agent Check utility
ACU 344
CONTROL-M Configuration Manager
Security database maintenance 181
CONTROL-M database
Oracle parameters 236, 471
owner parameter (Sybase) 234, 239, 468
parameters 467
Sybase parameter 234, 240, 468
CONTROL-M date
Day Time parameter 455
CONTROL-M Date parameter 454
CONTROL-M for z/OS 273
CONTROL-M log
Shout utility 118
CONTROL-M Mirror database parameters 477
CONTROL-M security 147
CONTROL-M SYSTEM tablespace parameters 471
CONTROL-M Version parameter 454
CONTROL-M/Agent
advantages 61
multiple agents 65
CONTROL-M/Desktop
DIAG component prefix 372
CONTROL-M/EM
release version 463
Shout messages 118
TCP/IP port number 463
CONTROL-M/EM client components 72
CONTROL-M/EM clients
authorization checking 214
CONTROL-M/EM database dialog box 302
CONTROL-M/EM GUI
DIAG component prefix 372
CONTROL-M/EM Release Version parameter 463
CONTROL-M/EM server
listening ports 386
CONTROL-M/EM TCP/IP Port Number parameter 463
CONTROL-M/Server
host name 462
Shout messages 118
TCP/IP port number 463
CONTROL-M/Server database
backing up 292
ControlResource LoadLimit system parameter 441
conventions, documentation 22
CORBA 357
TIMEOUT system exception 390
CORBA communication
NAT environment 361
CORBA server listening on port X 357
cryptocli utility 170
c
DIAG component prefix 372
CTM_ADJUST_COND_SCOPE
Server parameter 481
CTM_CONFIG_AGENT_AGENT_UNAVAIL_THRESHOLD
Server parameter 482
CTM_CONFIG_AGENT_MODE
Server parameter 482
CTM_CONFIG_AGENT_PORT_NUMBER
Server parameter 483
CTM_CONFIG_AGENT_SSL_ENBL 457
CTM_DB_TIMEOUT
Server parameter 483
CTM_GD_FORWARD configuration parameter 488
CTM_GROUP_ADJUST Dummy
Server parameter 484
CTM_GROUP_RECHECK
Server parameter 484
cmt_menu command 406
CTM_MULTIP_LIB_REPLACE
server parameter 485
CTM_PARM_ENC
configuration parameter 510
CTM_PRM_DONT_DELETE
configuration parameter 510
CTM_PRM_ENABLE_UExxx
user exit parameter 497
CTM_PRM_KPA_ACTIVE
communication parameter 461
CTM_PRM_KPA_ROUNDTRIP_TIMEOUT
communication parameter 461
CTM_PRM_KSH_FLAGS
configuration parameter 511
CTM_PRM_SCRIPT_UExxx
user exit parameter 498
CTM_PRM_SH_FLAGS
configuration parameter 511
CTM_PRM_TIMEOUT_UExxx
user exit parameter 498
CTM_RT_PORT_NUMBER
operational parameter 460
CTM_SLP_SUSPEND
Server parameter 485
CTM_SNMP_SEND_FORMAT
Server parameter 486
CTM_SU_PATH
configuration parameter 511
CTM_WRITE_CONSOLE
Server parameter 486
CTMBAT2UNC utility
summary 142
ctmdiskspace utility
disk space check 266
CTMFW utility
execution log file 128
ctmjsa utility
job statistics 124
CTMLOG_DEL_CHK configuration parameter 486
CTMORDER_FORCE
Server parameter 487
CTMPERMHOSTS
configuration parameter 508
ctmping utility
Watchdog facility 531
CTMS_ADDR_MODE
configuration parameter 508
CTMSHOST
configuration parameter 508
CTMUE101 user exit
job ordering 524
CTMUE102 user exit
job submission 525
CTMUE103 user exit
New Day procedure 527
CTMUE104 user exit
New Day procedure 527
CTMUE105 user exit
User Daily jobs 528
CTMUE106 user exit
User Daily jobs 528
cto utility 126
Custom Export/Import option
Database Maintenance menu 288
customer support 3
CYCLIC_MAXWAIT
Server parameter 488
CYCLIC_RERUN
Server parameter 488

dal_insert_max_bulksize parameter
Defaults.rsc file 452
dal_insert_min_bulksize parameter
Defaults.rsc file 452
dal_rel_cache_size parameter
Defaults.rsc file 452
dal_select_max_bulksize parameter
Defaults.rsc file 452
dal_select_min_bulksize parameter
Defaults.rsc file 452
Data field
GCS_LOG record 375
Data Flag field
GCS_LOG record 375
Data flags
GCS_LOG file 375
database
log files 472
parameters 467
size 233, 235, 469
Sybase SQL server 470
synchronization 257
Database Administrator Login
Sybase parameter 234
Database Administrator Password
Sybase parameter 234, 239
Database Administrator password
Sybase 469
Database Maintenance menu
options 288
Root menu 288, 289
Database Size parameter
Sybase 233, 235, 469
Database version
system parameter 454
Day Time * parameter 455
db_diag parameter
Defaults.rsc file 431
dbghelp.dll file
correct version 357
DBGLVL
   configuration parameter 508
DBO password
   Oracle parameter 478
   Sybase parameter 234, 239, 469, 478
dc data flag
   GCS_LOG file 375
Debug_Module parameter
   Defaults.rsc file 336
debugging
   Keep Alive messages 337
Default access level
   communication 190
default scope
   configuration file 391
defaults
   Default ctm agent 65
Defaults.rsc file
   comm_userid parameter 202
   limit_gcs_distrib parameter 88
DefaultUserTimeoutSec system parameter 433
DelayBeforePinning system parameter 441
deleting
   audit data 307
   prerequisite conditions 83, 369
   statistics 83
deleting a backup device 295
DeltaMaxActMinutes system parameter 425
Description field
   GCS_LOG record 375
device, backup
dropping 295
DFTPRT
   configuration parameter 515
DIAG diagnostics facility
   commands 331
   description 331
   DIAGL command 332
   DIAGOFF command 332
   DIAGON command 332
   log files 371
DIAGL command 332
DIAGOFF command 332
DIAGON command 332
DiagStacksOn parameter
   DIAG ini file 334
DirectoryServerHostPort system parameter 416
Disconnect from GUI Server option
   CONTROL-M/Desktop 198
Do Forcejob
   scheduling table action 192
DO_NOT_COPY_LOG_TO_MIRROR
   configuration parameter 487
documentation information 22
DOMAIN
   configuration parameter 515
Domain Configuration window
   Domain Settings panel 389
   Ports panel 222, 391
Domain Settings panel
   Domain Configuration window 389, 393
DownCreAlerts system parameter 426
downloading
   Active Jobs file 368, 369
drop a backup device 295
dst data flag
   GCS_LOG file 375
DUMMY jobs 484
E
EBCDIC_cp system parameter 426
ECHO_SYSOUT
   configuration parameter 515
ecs_dbg_lvl parameter
   Defaults.rsc file 336
electronic documentation 22
e-mail configuration
   attached SYSOUT messages 494
   ctmshout 493
   DOMAIL 493
   -DOSHOUT 493
   parameters 493
   -SHOUT 493
empackui.exe 73
EMThreadPool IdleTime system parameter 442
EMThreadPool MaxSize system parameter 442
EMThreadPool MinSize system parameter 442
encrypted password
   mcs.ini file 170
entities
   start 39
   stop 39
environment
   runtime 134
Erase Audit Data option
   Database Maintenance menu 289
Erase Old Nets option
   Database Maintenance menu 289
erase_audit_data script 308
EVENT_TIMEOUT
   configuration parameter 508
ExcludeJobFields system parameter 442
ExcludeJobControlRes system parameter 443
ExcludeJobQuantRes system parameter 443
executable path
   system parameter 454
Executable Path parameter 455
Exit 7
   CONTROL-M security 206
exit codes
   %errorlevel% 141
CONTROL-M scripts 136
  distinguishing between 140
  scripts 140
exits
  CTMUE101 524
  CTMUE102 525
  CTMUE103 527
  CTMUE104 528
  CTMUE105 528
  CTMUE106 528
Export Database option
  Database Maintenance menu 288
exporting
  audit records 301
Extend Database Size option
  Database Maintenance menu 288

F
FailCheckDBTimeOut system parameter 433, 444
File Watcher utility
  service trace 128
filename debug_level parameter
  DIAG ini file 333
Filenames
  component prefixes 372
  filtering
    group scheduling tables 125
firewall
  affect on communication 219
firewalls
  bidirectional IIOP 398
  communication through 389
  configuring 361
  ports for CORBA components 391
  Ports panel 398
first database log file
  Oracle parameter 472
flow
  security 147
FlushBufferSize parameter
  DIAG ini file 334
forcing download
  Active Jobs file 368
FTP
  send generated reports 344
Full access level
  communication 190
  Prerequisite Conditions panel 195
  Scheduling Tables panel 192, 196
Full Security * parameter 455
Full Security parameter
  usage 182

gateway communication
  log file 372
Gateway log file
  location 372
Gateway parameters
  system parameters 425
gc_done_wait parameter
  Defaults.rsc file 429
gc_handle_multiple parameter
  Defaults.rsc file 430
gc_max_retry parameter
  Defaults.rsc file 430
gc_retry_int parameter
  Defaults.rsc file 430
gc_unsent_wait parameter
  Defaults.rsc file 430
GCS_LOG files
  Action codes 375
  Data flags 375
  sample 373
GCS_LOG record 374
gcs_log_size parameter
  Defaults.rsc file 432
GCSERV user
  changing 202
  Global Conditions server user ID 202
General panel
  User Authorizations window 167
  General system parameters 413
get_auth_plugin_info function 158
get_plugin_info function 158
gethostbyaddr() system call 395
GLOBAL
  value for AUTOEDIT_INC_SEC 481
Global Alerts Server
  DIAG component prefix 372
  logical name 55
  system parameters 432
Global conditions
  distribution 88, 108
  traffic trace log 374
Global Conditions Distribution facility 88, 108
GROUP
  SNMP trap 534
  value for AUTOEDIT_INC_SEC 481
group scheduling tables
  filtering 125
gsr_DiagLvl.ini file 335
gtw_send_ctl_timeout parameter
  Defaults.rsc file 452
GtwCondDispatchErr system parameter 426
GUI Server
  DIAG component prefix 372
  logical name 55
  system parameters 439
GUI system parameters 438

H
HandleAlertsOnRerun system parameter 417
Health Check utility  
scanning and collecting information 343
Help, online 22
HERE documents  
CONTROL-M scripts 136
Host Interface Name  
database parameter 239
HostPort system parameter 417
HostPortList system parameter 427
How to reset the Naming repository  
CORBA troubleshooting 354

I
I18N  
configuration parameter 508
ID data flag  
GCS_LOG file 375
Ignore New Day Conditions parameter  
description 456
Import Database option  
Database Maintenance menu 288
Index tablespace file  
Oracle parameter 471
init_prflag 369
Input process communication port number  
operational parameter 463
InsertAlertTries system parameter 427
int_diag parameter  
Defaults.rsc file 432
Inter Process Communication Port Number  
operational parameter 460
interfaces file  
directory 234
Internet Inter-ORB Protocol  
addresses 389
Interoperable Object Reference  
decoding 388
definition 386
element 385
Invalid IIOP reference  
CORBA troubleshooting 355
Invalid listening port  
CORBA troubleshooting 355
Invalid process ID file name  
CORBA troubleshooting 354
Invalid repository directory  
CORBA troubleshooting 354
IOALOG_DEL_INT  
Server parameter 489
IOR IP address 127.0.0.1  
troubleshooting 360
IsBufer parameter  
DIAG ini file 333
IsCyclic parameter 333
IsPIDUsed parameter  
DIAG ini file 334
javaw.exe error message  
Enter Point Not Found 357
jetty 75
JO_STATISTIC  
configuration parameter 516
JOB NAME  
SNMP trap 535
job owner settings 173
JOB_WAIT  
configuration parameter 516
jobs  
CTMUE101 user exit 524
CTMUE102 user exit 525
ordering 524
submitting 525
Kernel Configuration parameter, Check 368
Key Authentication 173
Key name 173
Language system parameter 418
LAST TIME  
SNMP trap 534
LAST USER  
SNMP trap 534
level, Restricted security 182
LifeCheckRespTimeOut system parameter 435
LifeCheckRetries system parameter 435
LifeCheckRetryTime system parameter 436
limit_gcs_distrib parameters 88
limit_gcs_distrib_activate 88
limit_gcs_distrib_disable_dates 88
limit_gcs_distrib_max_days 88
LimitArchiveJobsInMem system parameter 444
LISTEN_INTERFACE  
configuration parameter 508
listener port number  
Oracle parameter 236, 471
listening ports  
CONTROL-M/EM Server 386
CORBA components 391
LMGUI_Communication_Cfg system parameter 418
load balancing
  overview 90
loader
  DIAG component prefix 372
LOCAL
  value for AUTOEDIT_INC_SEC 481
local agent 52
Local IP Host Interface Name parameter 460
Local System account option
  CONTROL-M Agent service 171
LOCALE
  configuration parameter 509
LockAccountForMinutes system parameter 165, 418
Locked account feature 165
Log device name
  Sybase parameter 235, 468
Log device type
  Sybase parameter 469
Log files
  naming convention 371
log physical device
  Sybase parameter 235, 469
LogCleanInterval system parameter 436
LogCleanLevel system parameter 436
LogHistoryDays system parameter 436
login process
  scripts 134
LogInfoLevel system parameter
  description 436
LOGKEEPDAYS
  configuration parameter 509
Logon As
  Agent
    configuration parameter 521
LOGON_AS_USER
  configuration parameter 516
logs
  cyclical files 371
  single-file 371

M
MAIL_ADD_SUBJECT_PREFIX
  e-mail configuration parameter 494
MAIL_TIMEOUT
  e-mail configuration parameter 495
maintaining
  Sybase SQL server 304, 311
maintenance
  CONTROL-M menu 406
Maintenance system parameters 435
Master Device Type
  Sybase parameter 470
Master physical device
  Sybase parameter 470
Max Wait parameter
  New Day procedure 83
max_gcs_logs parameter
  Defaults.rsc file 432
MaxDownHistDays system parameter 427
Maximum Days Retained by CONTROL-M Log
  system parameter 82, 456
Maximum Days Retained by CONTROL-M Log parameter
  456
Maximum Days to Retain Sysout Files
  system parameter 82
Maximum job state changes
  operational parameter 463
Maximum Number of Worker Threads parameter 464
Maximum Retries parameter 466
  description 456, 466
Maximum server processes
  operational parameter 463
Maximum Server Processes parameter 463
MaxOldDay system parameter
  description 427
MaxOldTotal system parameter
  description 427
MaxPasswordLength system parameter 419
MaxUpdatedJobsToAudit parameter 419
MaxUploadBufferMPM system parameter 427
MaxUploadBufferMVS system parameter 427
MaxUserTimeoutSec system parameter 433, 444
mcs.ini file
  administrator user name 170
MemBufferSize parameter
  DIAG ini file 333
MEMNAME
  SNMP trap 534
menus
  CONTROL-M main menu 406
Minimum server processes
  operational parameter 463
Minimum Server Processes parameter 463
MinimumDbgLvl parameter
  DIAG ini file 333
MinPasswordLength system parameter 419
mirror database
  Oracle 478
  parameters 476
  port numbers 478
  Sybase 478
  synchronization 257
mirror database data device
  Sybase parameter 477
mirror database log device
  Sybase parameter 477
Modify Database Name option
  Database Maintenance menu 289
Modify Interfaces File option
  Database Maintenance menu 289
modifying
passwords 170
pinned data 126
msg_diag parameter
    Defaults.rsc file 432
multiple agents 65
multiple scripts 142
multiple sessions
    port assignment 222, 391

N
ame binding 384
Name field
    CONTROL-M Definition window 59
name resolution 384
names
    multiple agents 65
name-to-object association 384
naming conventions
    DIAG log files 371
    log files 371
naming graph 384
Naming Service
    CORBA troubleshooting 354
    description 384
    directory 385
    listening port not free 354
    problems 353, 355
    repository 385
    updating 384
Network Address Translation environment 361
network interface detection 389
New Day procedure
    CTMUE103 user exit 527
    CTMUE104 user exit 527
    restarting 368
New Day time 82
New Domain dialog box 394
NEW_DAY_ASYNC_SP_EXECUTION
    cleanup parameter 489
Node group
    load balancing 90
    usage 90
Node ID
    SNMP trap 535
nonBlockTimeout parameter
    Defaults.rsc file 453
None access level
    communication 189
NOT_ORDERED_JOB_ALERT parameter 489
NrHandledAlarms system parameter 419
Number of Worker Threads parameter 464
NumberOfMyWorldJobs system parameter 444
NumberOfFailedLogins system parameter 165, 419
NumberOfPasswordReplacements system parameter 162, 420
NumOfFiles parameter
    DIAG ini file 333
NumOfMessages parameter
    DIAG ini file 333

O
object key 387
odat data flag
    GCS_LOG file 375
On code parameter scripts 139
On statement parameter scripts 139
On Statement/Code parameter 135
online Help 22
op data flag
    GCS_LOG file 375
operational parameters
    description 462
Oracle
    backing up 293
    database logs 285
Oracle SQL server
    home directory 472
    host parameter 236, 472
    listener port number 236, 471
    parameters 233, 236, 471
ORBListenEndpoints parameter
    CORBA troubleshooting 355
OrbShutdownWait system parameter 438
ORBSvcConf parameter
    CORBA troubleshooting 357
Order ID
    SNMP trap 534
ordering
    jobs for time zones 488
OS.dat file
    configuration parameters 510
OS_DIAG_LIMIT_LOG_FILE_SIZE
    prolog parameter 313
OS_DIAG_LIMIT_LOG_VERSIONS
    prolog parameter 313
OS_PRM_HOSTNAME
    Agent parameter 462
    Server parameter 462
OWNER
    SNMP trap 534

P
parameter scripts
    On code 139
    On statement 139
parameters
    database 467
    On Statement/Code 135

Index 551
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

A

performance 478
Sybase database 467
system 454, 496
Passphrase 173
password
new users 167
password authentication
external 158
return codes 158
Password will expire every n days option
User Authorizations 163
PasswordComplexityOnOff system parameter 420
PasswordComplexityRules system parameter 420
PasswordEncode system parameter 159, 420
PasswordExpirationOnOff system parameter 164, 421
PasswordHistoryOnOff system parameter 162, 421
PasswordLifetimeDays system parameter 164, 421
passwords
cryptocli utility 170
Permissive mode
Author parameter modification 197
persistent connection
Agent Router 224
description 224
pin_collection.ini configuration file 126
pinned data 126
Platform field
  CONTROL-M Definition window 59
plugin-sdk.zip
  software development kit 158
Polling interval parameter
communication 467
description 467
port assignment
  multiple sessions 222, 391
port numbers
  Agent-to-Server 459
  backup socket 470
  CONTROL-M components 398
  CONTROL-M/EM TCP/IP 463
  mirror database 477, 478
  multiple CTM agents 65
  query socket 470
  Server-to-Agent 467
  SNMP monitor trap 535
Ports panel
  Domain Configuration window 222, 391
PostgreSQL 239
post-processing
  performance parameters 478
predefined time zones
  TimeZone.dat file 110
PrereqConditions LoadLimit system parameter 444
prerequisite conditions
  deleting 83, 369
  security 202
PRINTER_NAME

R

RBS tablespace file
  Oracle parameter 471
REFRESH_SECURITY_PARAMS command string 158, 160, 411
Relative Round-trip Timeout policy 390
release version
  CONTROL-M/EM parameter 463
REM comment 142
RemedyCloseTicketMode system parameter 434
remote disk resources 142
remote host
  advantages 61
  deciding to configure 61
  job owner and authentication settings 173
Remote Sybase host name
  database parameter 234, 470
Reports
  FTP 344
Repository files
  Naming Service 385, 397
  repository ID 386
request-reply interval
  relative round-trip timeout policy 390
reserved variable $0 137
Resolve job's Author Field conflict
CONTROL-M/Desktop 199
Restricted security level 182
Restrictive mode
Author parameter modification 197
Retry Interval parameter 467
description 467
return codes
password authentication 158
REXX-language scripts 133
RJX_CONN_MODE
configuration parameter 511, 517
RJX_CONN_TOUT
configuration parameter 512, 517
RJX_CONN_TRY
configuration parameter 512, 517
RJX_DETAILS_TO_SYSOUT
configuration parameter 512, 517
RJX_OVMS_DEFAULT_QUEUE
configuration parameter 512, 518
RJX_OVMS_SETVERIFY
configuration parameter 513, 518
RJX_SYSOUT_DIR
configuration parameter 513, 518
Rollback segment tablespace file
Oracle parameter 471
rsi utility 126
RTTimeoutPolicy parameter 390
RUN_USER_LOGON_SCRIPT
configuration parameter 518
RUNINF_CUTOFF_NUMBER parameter 490
RUNINF_CUTOFF_RATIO parameter 490
RUNINF_PURGE_LIMIT
Server parameter 83, 490
RUNINF_PURGE_MODE
Server parameter 491
runtime environment 134

S
scanning information 343
scheduling jobs
performance parameters 478
scopes
configuration file 391
default 391
scripts
exit codes 136, 140
guidelines for writing 138
HERE documents 136
length 139
login process 134
On code 139
On statement 139
On Statement/Code parameter 135
run-time environment 134
Shell type 131
startup process 134
utilities 140
working directory 135
Secure Sockets Layer parameter 457
SecuredExcludedFields system parameter 445
security 147
authorizations 182
flow 147
levels 182
prerequisite conditions 202
Restricted security level 182, 455
task summary for authentication 184, 213, 268
Unrestricted security level 182, 455
workflow for authentication 179, 212, 218, 264
Security database
CONTROL-M Configuration Manager 181
maintenance 181
security flow 147
security level, Restricted 182
SEND TIME
SNMP trap 534
SendAlarmToScript system parameter 422
SendSnmp system parameter 423
Server-to-Agent
port numbers 467
Server-to-Agent Port Number parameter 467
service trace
File Watcher utility 128
set_gc_multiple_handling parameter
Defaults.rsc file 431
set_pwd_def_lifetime script 163, 164
SEVERITY
SNMP trap 534
shell type
CONTROL-M scripts 131
Shout Destination tables
description 91
specifying destinations 92
Shout facility
description 91
Shout messages
Agent platforms 118
CONTROL-M/EM 118
shut down
CONTROL-M/Server entities 39
shut_ca
closing CONTROL-M/Server Configuration Agent 39
shut_ctm
closing CONTROL-M/Server 39
shutdb
closing the SQL database server 39
SID mirror
Oracle parameter 478
siid data flag
GCS_LOG file 375
size of database log files
Oracle parameter 472
Sleep Time
considerations 479
resetting 369
sleep utility 141
SMTP_PORT_NUMBER
configuration parameter 513, 519
SMTP_REPLY_TO_EMAIL
configuration parameter 513, 519
SMTP_SENDER_EMAIL
configuration parameter 513, 519
SMTP_SENDER_FRIENDLY_NAME
configuration parameter 513, 519
SMTP_SERVER_NAME
configuration parameter 513, 519
SNMP
alerts 533
CONTROL-M/EM parameters 535
description 533
interfacing with CONTROL-M/EM 533
MIB file 536
monitor trap port 535
network manager 533
trap format 534
trap message 533
traps 534
SNMP customization
CONTROL-M/EM 535
SsmtpHost system parameter 423
SsmtpSendActive system parameter 423
SockRecrMaxAtmp system parameter 434, 436, 446
SockRecrWtIntr system parameter 434, 436, 446
srvers_poll_int parameter
Defaults.rsc file 431
SSH connections 62
SSH_VER_CMD
configuration parameter 514, 519
SSL 151
SSLRetries system parameter 428
SSLSyncTime system parameter 428
StandartCheckDBTimeOut system parameter 434
start
CONTROL-M/Server entities 39
entities 39
Start Day of the Week parameter 458
start_ca
starting CONTROL-M/Server Configuration Agent 39
start_ctm
starting CONTROL-M/Server 39
startdb
starting the SQL server 39
starting
CONTROL-M scripts 134
DIAG for GUI server 331
gateway debug message truncation 337
gateway host debug messages 337
Startup Type
Agent
configuration parameter 521
STATISALG
Server parameter 491
Statistical Details table
ctmj sa utility 124
statistics
ctmj sa utility 124
deleting 83
summary mode 464
Statistics Mode parameter 464
description 123, 464
Statistics parameter 458
Statistics Summary table
ctmj sa utility 124
STATS_TIME
Server parameter 492
STATUS
SNMP trap 534
StdoutLogInfoLevel system parameter 437
stop
entities 39
StopGracePeriodSec system parameter 437
StopIfDBConnectionFail system parameter 434, 446
stopping
DIAG for GUI server 331
gateway debug message truncation 337
output of gateway host debug messages 337
StopTries system parameter 437
stringified IORs 388
summary, task
authentication 184, 213, 268
support for computer aliases 360
support, customer 3
svc.conf file
cannot be found error message 357
TAO internal configuration 396
Sybase
backing up 292
Sybase Interface Directory
Sybase parameter 234
Sybase interface directory
database parameter 470
Sybase parameter
log physical device 235, 469
Master physical device 470
owner 234, 239, 468
Sybase SQL server
character set 242
database name 470
database parameters table 467
maintenance 304, 311
synchronization
database 257
mirror database 257
syntax statement conventions 23
SYSOUT
  attach to an e-mail message 494
Sysout directory
  WMI connection 69
sysout log directory
  system parameter 454
SYSOUT_LIMIT_SIZE parameter 492
SYOUTH_MODE
  configuration parameter 514
SYSOUT_NAME
  configuration parameter 514, 519
SYSOUT_WINDOW_SIZE parameter 493
SYSTEM
  value for AUTOEDIT_INC_SEC 481
system parameters
  description 454, 496
System user password
  Oracle parameter 472

Tablespace
  data file 472
  Oracle SQL server 242
  size 472
  user 473
TAO internal configuration file
  Domain Settings panel 396
task summary
  authentication security 184, 213, 268
TCP/IP
  CONTROL-M host name 59
TCP/IP port number
  CONTROL-M/EM 463
TCP_IP_TIMEOUT
  Agent
    configuration parameter 509
technical support 3
Time Zone field
  CONTROL-M Definition window 59
time zones
  enabling early job ordering 488
  TimeZone.dat file 110
Timeout for Agent utilities
  Agent configuration parameter 509
Timeout parameter
  description 465
timeout policy
  RTTimeoutPolicy parameter 390
TIMEOUT system exception
  CORBA 390
Timestamp field
  GCS_LOG record 375
TimeZone.dat
  file with predefined time zones 110
trace file
  File Watcher utility 128
  TRACE_CLIENT off command
    ctl utility 338
  TRACE_CLIENT on command
    ctl utility 338
  TRACE_CTM off command
    ctl utility 337
  TRACE_CTM on command
    ctl utility 337
  TRACE_DB command
    ctl utility 337
  TRACE_DISABLE_ALL command
    ctl utility 337
  TRACE_JOB_MESSAGE off command
    ctl utility 338
  TRACE_JOB_MESSAGE on command
    ctl utility 338
  TRACE_KLIVE off command
    ctl utility 337
  TRACE_KLIVE on command
    ctl utility 337
  TRACE_LINK_CLIENT off command
    ctl utility 338
  TRACE_LINK_CLIENT on command
    ctl utility 338
  TRACE_LINK_CTM off command
    ctl utility 338
  TRACE_LINK_CTM on
    ctl utility 338
  TRACE_TRUNC off command
    ctl utility 337
  TRACE_TRUNC on command
    ctl utility 337
  Tracker Port
    Agent
      configuration parameter 509
  TRACKER_EVENT_PORT
    Agent
      configuration parameter 509
  TRACKER_MAX_WORKERS_NUM parameter 464
  TRACKER_WORKERS_NUM parameter 464
  TRANSALATE_S0
    configuration parameter 514
  Translate_S0 flag 137
troubleshooting
  z/OS scheduling table not assigned to user daily 101, 102
truncating
  gateway debugging messages 337
tryno data flag
  GCS_LOG file 375

UDLY_PARTCOPY_ERR parameter 493
ue_exit directory
user exits 95
UNC
  description 142
  path 143
  Universal Naming Convention 142
Unlock option
  Scheduling Table Manager 198
  unlock_user script 166
Unrestricted security level
  description 182
upd_comm_int parameter
  Defaults.rsc file 431
Update access level
  communication 189
  Prerequisite Conditions panel 195
  Scheduling Tables panel 192, 196
UpdatesQueueLimit system parameter 447
UpdatesQueueMaxLimit system parameter 447
Use TAO internal configuration file
  Domain Settings panel 396
useNonBlock parameter
  Defaults.rsc file 453
UseQueryedCollectionForFind system parameter 446
User Daily
  CTMUE105 user exit 528
  CTMUE106 user exit 528
user exits
  configuration parameters 497
User password
  Oracle parameter 473
USER_NOT_FOUND exception 391
UserAuditContext system parameter 168
UserAuditOn system parameter 168
UserChangePassword system parameter 168
utilities
  clean_ajf 259
  ctm_clean_db 258
  ctm_cleanlog 258
  ctm_db_extend 258
  ctm_logdb_extend 258
  ctm_rollback_extend 258
  ctm_tempdb_extend (Oracle) 258
  ctm_tempdb_extend (Sybase) 258
  ctmdbrst 258
  ctmfw 128
  make_db 258
  scripts 140
UTTIMEOUT parameter
  configuration file 509
CORBA troubleshooting 358
ViewpointPolicy system parameter 125, 447
ViewPointTimeoutForBIM system parameter 447
virtual hostname 395

W
WarningPasswordExpirationDays system parameter 164, 425
WarningSSLExpirationDays system parameter 425
Watchdog facility
  configuration parameters 498
  description 266
  parameters 498
WD_CTMEXIT__ERROR_MSG parameter
  Watchdog exit 529, 530
WD_CTMEXIT_NUMBER parameter
  Watchdog facility 529, 530
WD_USEREXIT_#_SUSPEND_ STATE parameter 505
Web Launch 52
  deploying new packages 76
  requirements 53
Web Launch package 72
Web Launch Package Builder 73
WMI connections 62
WMI_SETUP_SHARE
  configuration parameter 520
workflow
  authentication security 179, 212, 218, 264
Working directory
  CONTROL-M scripts 135
workstation gateway
  log file 372
WRAP_PARAM_QUOTES
  configuration parameter 520

V
-v flag 137
verify user
  DIAG component prefix 372
ViewPoint is empty