



Command Line Interface Reference Guide for Cisco Unified Communications Solutions, Release 14SU1

First Published: 2021-10-27

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

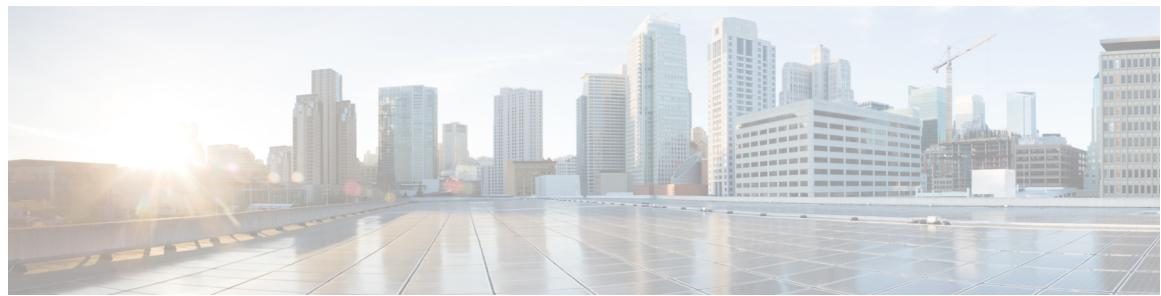
Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2021 Cisco Systems, Inc. All rights reserved.



CONTENTS

PREFACE

Preface xxiii

Purpose xxiii

Audience xxiii

Organization xxiii

Related Documents xxiv

CHAPTER 1

About CLI 1

CLI Privilege Levels 1

Start CLI session 1

Tab completes command 3

Command help 3

Ctrl-C exits command 4

Quit CLI session 5

CHAPTER 2

Delete Commands 7

delete account 7

delete cuc futuredelivery 7

delete cuc locale 8

delete dns 9

delete dscp 9

delete ipsec policy_group 10

delete ipsec policy_name 10

delete process 11

delete smtp 11

CHAPTER 3

File Commands 13

| | |
|---------------------------------|----|
| file build log | 13 |
| file check | 17 |
| file delete | 18 |
| file delete tftp | 18 |
| file delete dir tftp | 19 |
| file dump | 20 |
| file dump sftpdetails | 20 |
| file dump tftp | 21 |
| file fragmentation sdi | 21 |
| file fragmentation sdi file | 22 |
| file fragmentation sdi all | 22 |
| file fragmentation sdl | 23 |
| file fragmentation sdl file | 23 |
| file fragmentation sdl all | 24 |
| file get | 24 |
| file get salog | 25 |
| file get tftp | 26 |
| file list | 27 |
| file list salog | 28 |
| file list tftp | 29 |
| file search | 29 |
| file search tftp | 30 |
| file tail activelog | 31 |
| file tail tftp | 32 |
| file view | 32 |
| file view activelog | 33 |
| file view inactivelog | 34 |
| file view system-management-log | 35 |
| file view tftp | 35 |

CHAPTER 4

License Commands 37

| | |
|--|----|
| license smart deregister | 37 |
| license smart register idtoken <token> [force] | 38 |
| license smart renew auth | 38 |

| | |
|---|----|
| license smart renew ID | 38 |
| license smart transport direct | 39 |
| license smart transport gateway <URL> | 39 |
| license smart transport proxy <proxy-server> <proxy-port> | 40 |
| license smart factory reset | 40 |
| license smart reservation enable | 41 |
| license smart reservation disable | 41 |
| license smart reservation request | 41 |
| license smart reservation cancel | 42 |
| license smart reservation install "<authorization-code>" | 42 |
| license smart reservation install-file <url> | 42 |
| license smart reservation return | 43 |
| license smart reservation return authorization "<authorization-code>" | 43 |
| license smart reservation set license_count | 44 |
| license smart export request local <exportfeaturename> | 44 |
| license smart export return local <exportfeaturename> | 45 |
| license smart export cancel | 45 |

CHAPTER 5**Run Commands** 47

| | |
|-------------------------|----|
| run cuc dbquery | 47 |
| run cuc preupgrade test | 48 |
| run cuc smptest | 50 |
| run cuc sysagent task | 50 |
| run cuc vui rebuild | 51 |
| run loadcsv | 52 |
| run loadxml | 52 |
| run sql | 53 |
| run pe sql | 53 |

CHAPTER 6**Set Commands** 55

| | |
|----------------------------------|----|
| set account enable | 57 |
| set account name | 57 |
| set account ssorecoveryurlaccess | 59 |
| set account ssouidvalue | 60 |

| | |
|--|----|
| set cert bulk consolidate | 61 |
| set cert bulk export | 61 |
| set cert bulk import | 62 |
| set cert bulk sftp | 62 |
| set cert default-ca-list disable | 63 |
| set cert default-ca-list enable | 64 |
| set cert delete | 66 |
| set cert import | 66 |
| set cert regen | 67 |
| set cert regen ITLRecovery | 67 |
| set cli pagination | 68 |
| set cli session timeout | 69 |
| set commandcount | 70 |
| set csr gen | 70 |
| set cuc jetty stderrlog | 71 |
| set cuc jetty stdoutlog | 72 |
| set cuc jetty requestlog | 73 |
| set cuc speechview registration certificate size | 73 |
| set cuc srsv timeout | 74 |
| set cuc trace | 74 |
| set date | 75 |
| set dscp defaults | 76 |
| set dscp | 76 |
| set dscp marking | 77 |
| set ipsec policy_group | 78 |
| set ipsec policy_name | 78 |
| set key regen authz encryption | 79 |
| set key regen authz signing | 79 |
| set logging | 79 |
| set Login Grace Timeout | 80 |
| set network cluster publisher | 80 |
| set network cluster subscriber details | 81 |
| set network cluster subscriber dynamic-cluster-configuration | 82 |
| set network dhcp eth0 | 82 |

| | |
|---|-----|
| set network dns | 83 |
| set network dns options | 83 |
| set network domain | 84 |
| set network failover | 85 |
| set network gateway | 85 |
| set network hostname | 86 |
| set network ip eth0 | 88 |
| set network ipv6 dhcp | 89 |
| set network ipv6 gateway | 89 |
| set network ipv6 service | 90 |
| set network ipv6 static_address | 90 |
| set network max_ip_conntrack | 91 |
| set network mtu | 91 |
| set network name-service hosts cache-enable | 92 |
| set network name-service hosts max-db-size | 93 |
| set network name-service hosts negative-time-to-live | 93 |
| set network name-service hosts persistent | 94 |
| set network name-service hosts positive-time-to-live | 94 |
| set network name-service hosts suggested-size | 94 |
| set network name-service services cache-enable | 95 |
| set network name-service services max-db-size | 95 |
| set network name-service services negative-time-to-live | 96 |
| set network name-service services persistent | 96 |
| set network name-service services positive-time-to-live | 97 |
| set network name-service services suggested-size | 97 |
| set network nic eth0 | 98 |
| set network ntp option | 98 |
| set network pmtud state | 99 |
| set network restore | 99 |
| set network status eth0 | 101 |
| set network name-service | 101 |
| set password complexity minimum-length | 102 |
| set password age | 102 |
| set password change-at-login | 103 |

| | |
|--|-----|
| set password complexity character | 103 |
| set password complexity character difference | 105 |
| set password complexity character max-repeat | 105 |
| set password expiry maximum-age | 106 |
| set password expiry user maximum-age configure | 107 |
| set password expiry minimum-age | 107 |
| set password expiry user maximum-age | 108 |
| set password expiry user minimum-age | 109 |
| set password history | 110 |
| set password inactivity | 110 |
| set password system bootloader encryptHash | 111 |
| set password user admin | 111 |
| set password user security | 112 |
| Set replication-sync monitor | 113 |
| set samltrace level | 113 |
| set session maxlimit | 114 |
| set smtp | 114 |
| set strace enable | 115 |
| set strace disable | 115 |
| set timezone | 115 |
| set tls min-version | 116 |
| set trace disable | 117 |
| set trace enable | 118 |
| set tlresumptiontimeout | 118 |
| set tltrace* | 119 |
| set tltrace disable | 119 |
| set tltrace enable | 120 |
| set web-security | 120 |
| set webapp session timeout | 121 |
| set webapp session maxlimit | 122 |
| set workingdir | 125 |

| | |
|---|-----|
| show accountlocking | 131 |
| show cert default-ca-list | 132 |
| show cert list | 133 |
| show cert list type | 134 |
| show cert own | 134 |
| show cert trust | 135 |
| show cli pagination | 135 |
| show cli session timeout | 136 |
| show csr list | 136 |
| show csr list type | 137 |
| show csr own | 137 |
| show csr own name | 138 |
| show ctl | 139 |
| show cuc cluster status | 139 |
| show cuc config groups | 139 |
| show cuc config settings | 140 |
| show cuc dbconsistency | 141 |
| show cuc dbcontents | 142 |
| show cuc dbschema | 143 |
| show cuc dbserver disk | 144 |
| show cuc dbserver session | 144 |
| show cuc dbserver sessions all | 145 |
| show cuc dbserver sessions list | 145 |
| show cuc dbserver user list | 146 |
| show cuc dbserver user waiting | 146 |
| show cuc dbtable contents | 146 |
| show cuc dbtable list | 147 |
| show cuc dbtable schema | 148 |
| show cuc dbview contents | 150 |
| show cuc dbview list | 151 |
| show cuc dbview schema | 152 |
| show cuc jetty ssl status | 153 |
| show cuc locales | 153 |
| show cuc speechview registration certificate size | 154 |

| | |
|---------------------------------------|-----|
| show cuc sysagent task list | 154 |
| show cuc sysagent task results | 155 |
| show cuc sysinfo | 156 |
| show cuc tech dbschemaversion | 157 |
| show cuc tech dbserver all | 158 |
| show cuc tech dbserver integrity | 158 |
| show cuc tech dbserver log diagnostic | 159 |
| show cuc tech dbserver log message | 159 |
| show cuc tech dbserver status | 160 |
| show cuc trace levels | 160 |
| show cuc version | 161 |
| show date | 162 |
| show diskusage | 162 |
| show dscp all | 163 |
| show dscp defaults | 163 |
| show dscp marking | 163 |
| show dscp status | 164 |
| show environment fans | 165 |
| show environment power-supply | 165 |
| show environment temperatures | 165 |
| show fileserver transferspeed | 166 |
| show haproxy client-auth | 166 |
| show haproxy num-threads | 167 |
| show hardware | 168 |
| show ipsec information | 168 |
| show ipsec policy_group | 169 |
| show ipsec policy_name | 170 |
| show ipsec status | 170 |
| show itl | 170 |
| show logins | 171 |
| show logins successful | 171 |
| show logins unsuccessful | 171 |
| show key authz encryption | 172 |
| show key authz signing | 172 |

show license all **173**
show license status **173**
show license summary **173**
show license tech support **174**
show license trace **174**
show license UDI **174**
show license usage **175**
show Login Grace Timeout **175**
show media streams **175**
show memory **177**
show myself **177**
show network all **178**
show network cluster **178**
show network dhcp eth0 **178**
show network eth0 **179**
show network failover **179**
show network ip_conntrack **180**
show network ipprefs **180**
show network ipv6 **181**
show network max_ip_conntrack **181**
show network ntp option **182**
show network route **182**
show network status **182**
show network name-service attributes **183**
show network name-service cache-stats **184**
show network name-service {hosts|services} attributes **184**
show open files all **185**
show open files process **185**
show open files regexp **186**
show open ports all **186**
show open ports process **186**
show open ports regexp **187**
show packages **187**
show password **188**

show password change-at-login 188
show password complexity character 189
show password complexity length 189
show password expiry 189
show password expiry user 190
show password expiry user list 190
show perf counterhelp 191
show perf list categories 191
show perf list classes 192
show perf list counters 192
show perf list instances 193
show perf query class 193
show perf query counter 194
show perf query instance 194
show perf query path 195
show process list 195
show process load 196
show process name 197
show process name process-name 197
show process open 198
show process open-fd 198
show process pid 199
show process search 199
show process user 200
show process using-most cpu 200
show process using-most memory 201
show registry 201
show risdb list 202
show risdb query 203
show samltrace level 203
show session maxlimit 204
show smtp 204
show stats io 204
show status 205

show tech activesql 206
show tech all 206
show tech ccm_service 206
show tech database 207
show tech dberrcode 207
show tech dbhighcputasks 208
show tech dbintegrity 208
show tech dbschema 208
show tech dbinuse 209
show tech dbstateinfo 209
show tech devdefaults 210
show tech dumpCSVandXML 210
show tech gateway 210
show tech locales 211
show tech network all 211
show tech network hosts 212
show tech network interfaces 212
show tech network resolv 213
show tech network routes 213
show tech network sockets 214
show tech notify 214
show tech params 215
show tech prefs 215
show tech procedures 216
show tech repltimeout 216
show tech routepatterns 217
show tech routeplan 217
show tech runtime 217
show tech sqlhistory 218
show tech systables 218
show tech system 219
show tech table 220
show tech triggers 220
show tech version 220

| | |
|-----------------------------|-----|
| show timezone config | 221 |
| show timezone list | 221 |
| show tlstrace | 222 |
| show tls min-version | 222 |
| show tlsresumptiontimeout | 222 |
| show trace | 223 |
| show ups status | 223 |
| show version active | 224 |
| show version inactive | 224 |
| show vos version | 224 |
| show web-security | 225 |
| show webapp session timeout | 226 |
| show workingdir | 226 |
| show logins unsuccessful | 226 |

CHAPTER 8**Unset Commands** 229

| | |
|--|-----|
| unset ipsec policy_group | 229 |
| unset ipsec policy_name | 229 |
| unset network cluster subscriber details | 230 |
| unset network cluster subscriber dynamic-cluster-configuration | 230 |
| unset network dns options | 231 |
| unset network domain | 231 |
| unset network ntp options | 232 |
| unset network ipv6 gateway | 232 |
| unset network ipv6 static_address | 233 |

CHAPTER 9**Utils Commands** 235

| | |
|--------------------------|-----|
| utils auditd | 240 |
| utils BE6000Mode enable | 240 |
| utils BE6000Mode disable | 241 |
| utils BE6000Mode status | 241 |
| utils branding enable | 241 |
| utils branding disable | 241 |
| utils branding status | 242 |

| | |
|---|-----|
| utils contactsearchauthentication disable | 242 |
| utils contactsearchauthentication enable | 242 |
| utils contactsearchauthentication status | 243 |
| utils core analyze | 243 |
| utils core list | 244 |
| utils capf cert import | 244 |
| utils capf set keep_alive | 244 |
| utils capf stale-lsc | 245 |
| utils create report | 245 |
| utils create report database | 246 |
| utils ctl | 246 |
| utils ctl reset localkey | 247 |
| utils cuc activate CUSRSP | 248 |
| utils cuc auto ITL download | 248 |
| utils cuc cluster activate | 249 |
| utils cuc cluster deactivate | 249 |
| utils cuc cluster makeprimary | 249 |
| utils cuc cluster overwritedb | 250 |
| utils cuc cluster renegotiate | 250 |
| utils cuc create report | 251 |
| utils cuc dbreplication 01_tear_down | 251 |
| utils cuc dbreplication 02_define_servers | 252 |
| utils cuc dbreplication 03_define_db_template | 253 |
| utils cuc dbreplication 04_sync_database | 253 |
| utils cuc dbreplication reset_all | 254 |
| utils cuc encryption | 255 |
| utils cuc hwconfig update | 256 |
| utils cuc jetty ssl disable | 257 |
| utils cuc jetty ssl enable | 257 |
| utils cuc networking clear_replication | 258 |
| utils cuc networking dscep | 258 |
| utils cuc odbc non-secure enable | 259 |
| utils cuc odbc non-secure disable | 259 |
| utils cuc odbc non-secure status | 260 |

| | |
|---|-----|
| utils cuc reset password | 260 |
| utils cuc set PinExpiry_PromptTime “Authentication Rule Name” | 260 |
| utils container-engine start | 261 |
| utils container-engine stop | 261 |
| utils container-engine restart | 261 |
| utils container-engine status | 262 |
| utils dbreplication dropadmindb | 262 |
| utils dbreplication forcedatasyncsub | 263 |
| utils dbreplication quickaudit | 264 |
| utils dbreplication rebuild | 264 |
| utils dbreplication repair | 265 |
| utils dbreplication repairreplicate | 265 |
| utils dbreplication repairtable | 266 |
| utils dbreplication reset | 267 |
| utils dbreplication runtimestate | 267 |
| utils dbreplication setprocess | 268 |
| utils dbreplication setrepltimeout | 269 |
| utils dbreplication status | 269 |
| utils dbreplication stop | 270 |
| utils imbd_replication replication status | 271 |
| utils diagnose | 271 |
| utils disaster_recovery backup network | 272 |
| utils disaster_recovery cancel_backup | 272 |
| utils disaster_recovery device add network | 273 |
| utils disaster_recovery device delete | 274 |
| utils disaster_recovery device list | 274 |
| utils disaster_recovery estimate_tar_size | 274 |
| utils disaster_recovery history | 275 |
| utils disaster_recovery jschLogs operation | 275 |
| utils disaster_recovery prepare restore pub_from_sub | 276 |
| utils disaster_recovery restore network | 276 |
| utils disaster_recovery schedule add | 277 |
| utils disaster_recovery schedule | 278 |
| utils disaster_recovery schedule delete | 278 |

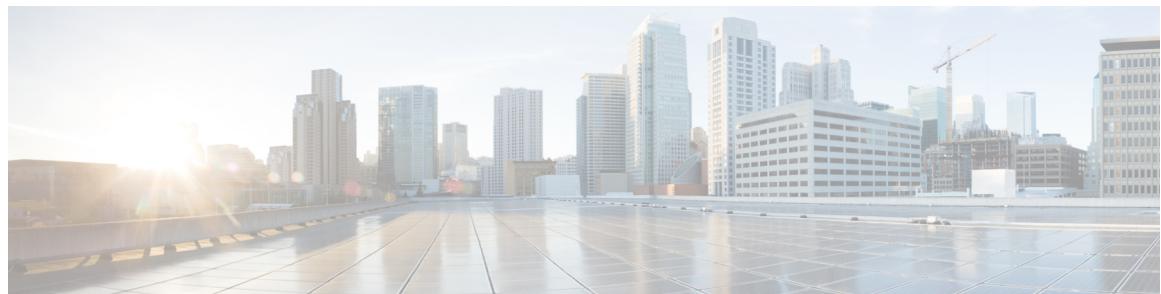
utils disaster_recovery schedule disable **279**
utils disaster_recovery schedule list **279**
utils disaster_recovery show_backupfiles **279**
utils disaster_recovery show_registration **280**
utils disaster_recovery status **280**
utils EnhancedSecurityMode disable **281**
utils EnhancedSecurityMode enable **281**
utils EnhancedSecurityMode status **281**
utils filebeat config **282**
utils filebeat disable **282**
utils filebeat enable **283**
utils filebeat status **283**
utils filebeat tls **283**
utils fior **284**
utils fior disable **284**
utils fior enable **285**
utils fior list **285**
utils fior start **286**
utils fior status **286**
utils fior stop **286**
utils fior top **287**
utils fips **287**
utils fips_common_criteria **288**
utils firewall ipv4 debug **289**
utils firewall ipv4 **290**
utils firewall ipv4 list **290**
utils firewall ipv4 status **291**
utils firewall ipv6 debug **291**
utils firewall ipv6 **292**
utils firewall ipv6 list **292**
utils firewall ipv6 status **293**
utils ha failover **293**
utils ha fallback **294**
utils haproxy set {required|optional|disable} client-auth **294**

| | |
|--|-----|
| utils haproxy set num-threads | 296 |
| utils ha recover | 298 |
| utils ha status | 298 |
| utils ils showpeerinfo | 299 |
| utils import config | 300 |
| Execute utils import config in Vmware Deployment | 300 |
| utils iostat | 301 |
| utils iothrottle | 301 |
| utils itl reset | 302 |
| utils ipsec restart | 303 |
| utils ldap config | 303 |
| utils ldap config status | 304 |
| utils managementAgent alarms minpushLevel | 304 |
| utils managementAgent alarms pushfrequency | 305 |
| utils managementAgent alarms pushnow | 305 |
| utils network arp delete | 305 |
| utils network arp set | 306 |
| utils network arp list | 307 |
| utils network capture | 307 |
| utils network capture-rotate | 308 |
| utils network connectivity | 309 |
| utils network host | 311 |
| utils network ipv6 host | 311 |
| utils network ipv6 traceroute | 312 |
| utils network ipv6 ping | 312 |
| utils network ping | 312 |
| utils network traceroute | 313 |
| utils network name-service {hosts services} cache invalidate | 313 |
| utils ntp auth symmetric-key | 314 |
| utils ntp auth auto-key | 316 |
| utils ntp server add | 319 |
| utils ntp server delete | 320 |
| utils ntp config | 321 |
| utils ntp restart | 322 |

utils ntp server list 322
utils ntp start 322
utils ntp status 323
utils os kerneldump 323
utils os kerneldump ssh 324
utils os kerneldump status 325
utils os secure 325
utils os secure dynamic-policies compile 326
utils os secure dynamic-policies list 326
utils os secure dynamic-policies load 326
utils os secure dynamic-policies remove 327
utils os secure dynamic-policies show 327
utils os secure dynamic-policies start-recording 328
utils os secure dynamic-policies stop-recording 329
utils PlatformWebAccess disable 329
utils PlatformWebAccess enable 330
utils PlatformWebAccess status 330
utils processCoreDumps disable 330
utils processCoreDumps enable 331
utils processCoreDumps status 331
utils remote_account create 331
utils remote_account disable 332
utils remote_account enable 332
utils remote_account status 332
utils remotesyslog set protocol tcp 333
utils remotesyslog set protocol udp 333
utils remotesyslog set protocol tls 333
utils remotesyslog show protocol 334
utils reset_application_ui_administrator_name 334
utils reset_application_ui_administrator_password 335
utils restore_application_ui_administrator_account 335
utils rosters list limited 336
utils rosters list full 336
utils rosters list watchers 336

| | |
|---|-----|
| utils rosters list contacts | 337 |
| utils rosters delete | 337 |
| utils scheduled-task disable | 337 |
| utils scheduled-task enable | 338 |
| utils scheduled-task list | 338 |
| utils set urlpattern disable | 339 |
| utils set urlpattern enable | 339 |
| utils service | 339 |
| utils service list | 340 |
| utils service auto-restart | 341 |
| utils service start | 341 |
| utils service stop | 342 |
| utils snmp config 1/2c community-string | 342 |
| utils snmp config 1/2c inform | 343 |
| utils snmp config 1/2c trap | 343 |
| utils snmp config 3 inform | 344 |
| utils snmp config mib2 | 345 |
| utils snmp config 3 trap | 345 |
| utils snmp config 3 user | 346 |
| utils snmp get | 346 |
| utils snmp get 1 | 347 |
| utils snmp get 2c | 348 |
| utils snmp get 3 | 348 |
| utils snmp hardware-agents | 349 |
| utils snmp test | 350 |
| utils snmp walk | 350 |
| utils snmp walk 1 | 352 |
| utils snmp walk 2c | 352 |
| utils snmp walk 3 | 353 |
| utils soap realserviceservice test | 354 |
| utils sso | 354 |
| utils sso recovery-url | 355 |
| utils system restart | 355 |
| utils system shutdown | 356 |

| | |
|--|-----|
| utils system switch-version | 356 |
| utils system boot | 356 |
| utils system upgrade | 357 |
| utils system upgrade cluster | 360 |
| utils system enableAdministration | 363 |
| utils update dst | 364 |
| utils users validate | 364 |
| utils vmtools refresh | 365 |
| utils vmtools status | 365 |
| utils vmtools switch open | 366 |
| utils vmtools switch native | 366 |
| utils system boot status | 366 |
| utils system upgrade dataexport initiate | 367 |
| utils system upgrade dataexport status | 368 |
| utils system upgrade dataexport cancel | 368 |



Preface

- [Purpose, on page xxiii](#)
- [Audience, on page xxiii](#)
- [Organization, on page xxiii](#)
- [Related Documents, on page xxiv](#)

Purpose

The *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* provides information about all the commands supported on the IM and Presence service, Cisco Unified Communications, and Cisco Unity Connection. Every command includes an "Applies to" section identifying applicable products.

Audience

The *Command Line Interface Reference Guide for Cisco Unified Communications Solutions* provides information to execute specific commands for network administrators responsible for managing and supporting IM and Presence, Cisco Unified Communications Manager, and Cisco Unity Connection.

Organization

The following table shows the organization for this guide:

Table 1: Organization of Command Line Interface Reference Guide for Cisco Unified Communications Solutions

| Chapter | Description |
|------------------|---|
| About CLI | Provides information about the CLI and tips to help make the management of the products easier to navigate. |
| Delete commands | Lists all commands relating to the removal of specific information. |
| File commands | Lists all commands relating to the management of files and logs. |
| License commands | Lists all commands relating to licensing. |

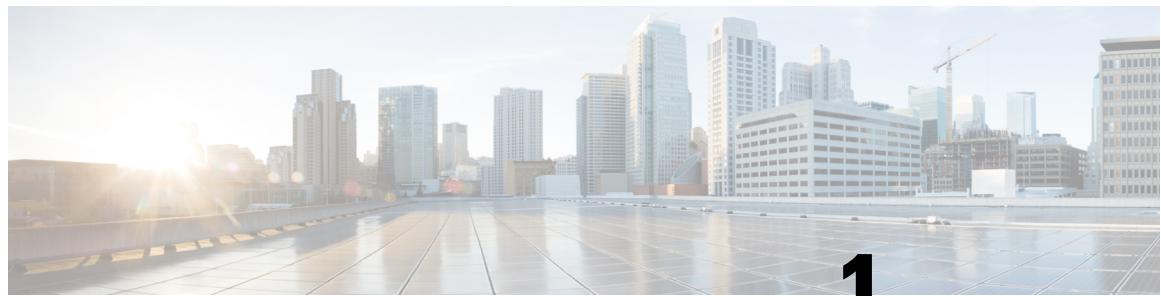
Related Documents

| | |
|----------------|---|
| Run commands | Lists all commands relating to the execution of sql queries, various tests, and tasks. |
| Set commands | Lists all commands relating to the tasks such as enabling, disabling, importing, and exporting. |
| Show commands | Lists all commands relating to the display of specified information. |
| Unset commands | Lists all commands relating to the disabling of specified network and ipsec options. |
| Utils commands | Lists all commands relating to utilities. |

Related Documents

See the *Cisco Unified Communications Manager Documentation Guide* to learn about the documentation for Unified Communications Manager and IM and Presence Service.

For the latest IM and Presence Service and Unified Communications Manager requirements, see the *Release Notes for Cisco Unified Communications Manager*.



CHAPTER 1

About CLI

- [CLI Privilege Levels, on page 1](#)
- [Start CLI session, on page 1](#)
- [Tab completes command, on page 3](#)
- [Command help, on page 3](#)
- [Ctrl-C exits command, on page 4](#)
- [Quit CLI session, on page 5](#)

CLI Privilege Levels

During installation of Unified Communications Manager, an administrator with level 4 privilege is created at the platform level. This administrator has all privileges to execute all the command line interface (CLI) commands. Through the CLI commands, the administrator with level 4 privilege creates the following administrators:

- Administrator with level 0 privilege—This administrator has read-only access privilege on the interface.
- Administrator with level 1 privilege—This administrator has both read and write access privilege on the interface.



Note Administrators can execute CLI commands based on the privileges defined for each of them.

After the administrators with the various privileges are created, you can start the CLI session.

Start CLI session



Note This procedure applies to both Unified Communications Manager and the IM and Presence Service. The Operating System for Unified Communications Manager is called the Cisco Unified Operating System. The Operating System for the IM and Presence Service is called the Unified IM and Presence Operating System. To start a CLI session for the IM and Presence Service, you must use the Unified IM and Presence Operating System.

You can access the Cisco Unified Operating System (or, for the IM and Presence Service, the Unified IM and Presence Operating System) remotely or locally:

- From a web client workstation, such as the workstation that you use for Cisco Unified Operating System Administration, you can use SSH to connect securely to the Cisco Unified Operating System.
- You can access the Cisco Unified Operating System CLI directly by using the monitor and keyboard that you used during installation or by using a terminal server that is connected to the serial port. Use this method if a problem exists with the IP address.

Before you begin

Ensure you have the following information that is defined during installation:

- A primary IP address and hostname
- An administrator ID
- A password

You will need this information to log in to the Cisco Unified Operating System.

Procedure

Step 1

Perform one of the following actions depending on your method of access:

- From a remote system, use SSH to connect securely to the Cisco Unified Operating System. In your SSH client, enter

`ssh adminname@hostname`

where *adminname* specifies the Administrator ID and *hostname* specifies the hostname that was defined during installation.

For example, **`ssh admin@ipt-1`**.

- From a direct connection, you receive this prompt automatically:

ipt-1 login:

where *ipt-1* represents the host name of the system.

Enter the administrator ID that was defined during installation.

Step 2

Enter the password that was defined at installation.

The CLI prompt displays. The prompt represents the Administrator ID; for example:

admin:

You can now use any CLI command.

Tab completes command

To complete commands, use Tab:

- Enter the start of a command and press **Tab** to complete the command. For example, if you enter se and press **Tab**, set is completed.
- Enter a full command name and press **Tab** to display all the commands or subcommands that are available. For example, if you enter set and press **Tab**, you see all the set subcommands. An * identifies the commands that have subcommands.
- If you reach a command, keep pressing **Tab**, and the current command line repeats; this indicates that no additional expansion is available.

Command help

You can get two kinds of help about any command:

- Detailed help that includes a definition of the command and an example of its use
- Short query help that includes only command syntax

| If you want to: | At the CLI prompt: |
|---------------------------|--|
| Get detailed help | Enter help command Where <i>command</i> specifies the command name or the command and parameter. See “Detailed Help Example.” |
| Query only command syntax | Enter <i>command?</i> Where <i>command</i> represents the command name or the command and parameter. See “Query Example.” |

Troubleshooting Tips

If you enter a ? after a menu command, such as set, it acts like the **Tab** key and lists the commands that are available.

Detailed Help Example:

```
admin:help file list activelog
activelog help:
This will list active logging files
options are:
```

Ctrl-C exits command

```

page      - pause output
detail    - show detailed listing
reverse   - reverse sort order
date      - sort by date
size      - sort by size

file-spec can contain '*' as wildcards

Example:
admin:file list activelog platform detail
02 Dec,2004 12:00:59      <dir>    drf
02 Dec,2004 12:00:59      <dir>    log
16 Nov,2004 21:45:43      8,557    enGui.log
27 Oct,2004 11:54:33      47,916   startup.log
dir count = 2, file count = 2

```

Query Example:

```

admin:file list activelog?Syntax:
file list activelog file-spec [options]
file-spec   mandatory   file to view
options     optional    page|detail|reverse|[date|size]

```

Ctrl-C exits command

You can stop most interactive commands by entering the **Ctrl-C** key sequence, as shown in the following example:

Exiting a Command with Ctrl-C

```

admin:utils system upgrade initiateWarning: Do not close this window without first
      exiting the upgrade command.
Source:
1) Remote Filesystem
2) DVD/CD
q) quit
Please select an option (1 - 2 or "q" ):
Exiting upgrade command. Please wait...
Control-C pressed
admin:

```



Note If you execute the command **utils system switch-version** and enter **Yes** to start the process, entering **Ctrl-C** exits the command but does not stop the switch-version process.

Quit CLI session

At the CLI prompt, enter **quit**. If you are logged in remotely, you get logged off, and the ssh session is dropped. If you are logged in locally, you get logged off, and the login prompt returns.

[Quit CLI session](#)



CHAPTER 2

Delete Commands

- [delete account, on page 7](#)
- [delete cuc futuredelivery, on page 7](#)
- [delete cuc locale, on page 8](#)
- [delete dns, on page 9](#)
- [delete dscp, on page 9](#)
- [delete ipsec policy_group, on page 10](#)
- [delete ipsec policy_name, on page 10](#)
- [delete process, on page 11](#)
- [delete smtp, on page 11](#)

delete account

This command allows you to delete an administrator account.

delete account *account-name*

| Syntax Description | Parameters | Description |
|--------------------|---------------------|---|
| | <i>account-name</i> | Specifies the name of an administrator account. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

delete cuc futuredelivery

This command deletes all messages that have been marked for future delivery.

delete cuc locale**delete cuc futuredelivery****Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

The following example deletes two messages that have been marked for future delivery.

```
admin: delete cuc futuredelivery

Deleting File : UmssMtaFutureDelivery/UnityMbxDb1/5C56C086-E64B-11DC-9BAF-41FC55D89593.eml
Deleting File : UmssMtaFutureDelivery/UnityMbxDb1/6D7DD796-E64B-11DC-A0E6-D1FD55D89593.eml
Files : Found = 2, Deleted = 2

Note: Files that are in use cannot be deleted
```

delete cuc locale

This command deletes the specified locale and all of the associated files and settings from Connection.

delete cuc locale *locale-id***Syntax Description****Parameters Description***locale-id* Specifies the ID of the locale that you want to delete.**Command Modes**

Administrator (admin:)

Usage Guidelines

Before you run this command, you must stop the Connection Conversation Manager and Connection Mixer services. After you run this command, you must restart the Connection Conversation Manager and Connection Mixer services. While running "delete cuc" locale command, you can choose to retain or not retain the locale mappings at your Unity Connection System.

If you choose to retain locale mapping, then after re-install of same locale, all objects like Subscribers and Call handlers are automatically mapped to retained locale. If you choose not to retain the locale mapping, then after uninstall all locale mappings are lost.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

The following example deletes the en-GB locale and all of the associated files and settings.

```
admin:delete cuc locale en-GB
```

```
en-GB uninstalled
```

delete dns

This command allows you to delete the IP address for a DNS server.

delete dns *addr*

Syntax Description

Parameters Description

| | |
|-------------|--|
| <i>addr</i> | Represents the IP address of the DNS server that you want to delete. |
|-------------|--|

Command Modes

Administrator (admin:)

Usage Guidelines

After you execute this command, the system asks whether you want to continue.



Caution

If you continue, this command causes a temporary loss of network connectivity.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

delete dscp

This command deletes a DSCP port tag.

delete dscp *port-tag*

delete ipsec policy_group

| Syntax Description | Parameters Description |
|--------------------|--|
| | <p><i>port-tag</i> Represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. This value is for the portTag field displayed when you use the command show dscp defaults. The set of port tags is predefined.</p> |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | <p>After you delete an enabled port tag, DSCP marking on that port tag stops. You can recreate a deleted port tag when you use the set dscp marking command; enter the name of the port tag that you previously deleted.</p> |
| Tip |  Use the command show dscp defaults to list the configured port tags. |

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager, Cisco Unity Connection

delete ipsec policy_group

This command deletes all policies within the specified group or all groups.

delete ipsec policy_group {group | all}

| Syntax Description | Parameters Description |
|--------------------|---|
| | <p><i>group</i> Represents a specific group name.</p> |
| | <p>all Deletes all groups.</p> |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, Cisco Unity Connection

delete ipsec policy_name

This command deletes an Ipsec policy with given policy name.

delete ipsec policy_name {policy_name | all}

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>policy_name</i> Represents the policy name. |
| | all Deletes policies within all policy names. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, Cisco Unity Connection

delete process

This command allows you to delete a particular process.

delete process *process-id* [{force | terminate | crash}]

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>process-id</i> Represents the process ID number. |
| | force Causes the process to stop. |
| | terminate Causes the operating system to terminate the process. |
| | crash Crashes the process and produces a crash dump. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

| | |
|------------------|--|
| Usage Guidelines | Use the force option only if the command alone does not delete the process; use the terminate option only if force does not delete the process. |
|------------------|--|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

delete smtp

This command allows you to delete the SMTP host.

delete smtp

```
delete smtp
```

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection



CHAPTER 3

File Commands

- [file build log](#), on page 13
- [file check](#), on page 17
- [file delete](#), on page 18
- [file delete tftp](#), on page 18
- [file dump](#), on page 20
- [file dump sftpdetails](#), on page 20
- [file dump tftp](#), on page 21
- [file fragmentation sdi](#), on page 21
- [file fragmentation sdl](#), on page 23
- [file get](#), on page 24
- [file get tftp](#), on page 26
- [file list](#), on page 27
- [file list tftp](#), on page 29
- [file search](#), on page 29
- [file search tftp](#), on page 30
- [file tail activelog](#), on page 31
- [file tail tftp](#), on page 32
- [file view](#), on page 32
- [file view tftp](#), on page 35

file build log

This command collects log information by service or feature and duration.

file build log *service/feature duration*

| Syntax Description | Parameters | Description |
|----------------------|------------------------|---|
| | <i>service/feature</i> | specifies the component or functional area from which to retrieve log information |
| | <i>duration</i> | specifies the time period, measured in days, from which the log information is retrieved. |
| Command Modes | Administrator (admin:) | |

Usage Guidelines**Requirements**

Command privilege level:

Allowed during upgrade:

Examples

This command collects logs for the Client Profile Agent.

```
admin: file build log cpa 10
Collecting logs

Collecting: logname1.txt
Collecting: logname2.txt

To retrieve run the following command:
  file get epas/trace/acdc_2012-06-28-111258.tar.gz
```

This command collects all logs defined in the xml config.

```
admin:file build log all
Collecting logs

Collecting: logname1.txt
Collecting: logname2.txt

To retrieve run the following command:
  file get epas/trace/acdc_2012-06-28-111258.tar.gz
```

This command collects logs for multiple services.

```
admin:file build log dbmon cpa
Collecting logs

Collecting: logname1.txt
Collecting: logname2.txt

To retrieve run the following command:
  file get epas/trace/acdc_2012-06-28-111258.tar.gz
```

This command shows help.

```
admin:file build log ?
Syntax:
  file build log [serviceName [serviceName] ...]

Service Names:
  FullName                      ShortName
  cisco_client_profile_agent     cpa
  cisco_database_layer_monitor   dbmon
  cisco_audit_logs                audit
  cisco_ris_dat_collector        risdc
```

This command shows information for the deployment.

```
admin: file build log deployment info 0

DB Queries may take up to 5 minutes to complete. Please be patient...
About to start queries for deployment data... please wait...
-----
Gathering CUCM Version...
ccmversion
11.0.1.100000 (9)
```

```
-----  
Gathering CUCM Publisher Node  
ccmpublisherhostname  
gwydlg050498vm1  
-----  
Gathering Rosters table...  
rosters  
3032681  
-----  
Gathering Groups table...  
groups  
1518966  
-----  
Gathering Non-Presence contacts...  
nonpresencecontacts  
502573  
-----  
Gathering Number of inter-cluster users...  
enduser  
0  
-----  
Gathering CUCM Nodes in cluster...  
processnode  
2  
-----  
Gathering CUCM Node names in cluster...  
name  
EnterpriseWideData  
processnode  
gwydlg050408vm1  
-----  
Gathering IM&P nodes in cluster...  
processnode  
2  
-----  
Gathering XCP Routing Node...  
paramvalue  
t  
-----  
Gathering Exchange Calendaring...  
pebackendgateway  
-----  
Gathering SIP Inter-domain Federation...  
domainname  
paramvaluegwydlg050408vm2-public.cisco.com  
-----  
Gathering XMPP Inter-domain Federation...  
xmpps2ssnodes  
0  
-----  
Gathering Intra-domain Partitioned Federation...  
enablepartitionedfedwithacs  
f  
-----  
Gathering Inter-cluster Peering...  
cupsinterclusterpeers  
-----  
Gathering Message Archiver...  
pkid  
8fede7a9-b6a6-4ad4-8da6-b8ea4c8d5411  
databasetype  
Postgres
```

file build log

```
datbasename
tcmadb
name
gwydlg050408vm2
tknodeusage
0
tkprocessnoderole
2
nodeid
3
-----
Gathering Third-party compliance...
ftextdbprocessnodemap
0
-----
Gathering Persistent Chat...
enablepersistentgear
t
datbasetype
Postgres
datbasename
tcmadb
name
gwydlg050408vm2
tknodeusage
0
tkprocessnoderole
2
nodeid
2
-----
Gathering Advanced File Transfer...
tkfiletransfer
2
datbasetype
Postgres
datbasename
tcmadb
name
gwydlg050408vm2
tknodeusage
0
tkprocessnoderole
2
nodeid
3
-----
Gathering AD Groups...
paramvalue
t
-----
Gathering XEP-198...
paramvalue
t
-----
Gathering DB Replication Status...
replicationdynamic
2
Services on this node that currently have debug logging enabled are:
Cisco Presence Engine
Cisco DRF Local
Cisco XCP File Transfer Manager
```

```

Collecting Logs for deployment_info

Collected: platformConfig.xml
Collected: deployment_info.xml
Collected: system_info.txt

To retrieve the logs, run the following CLI Command:
  file get activelog epas/trace/log_2015-08-17-154010.tar.gz
To maintain a stable system it is recommended that you remove the file after retrieval.
  To do this run the CLI Command:
    file delete activelog epas/trace/log_2015-08-17-154010.tar.gz
Please Note: Debug logging is not enabled for any of the files you have retrieved

```

file check

This command checks the /usr directory tree to see whether files or directories have been added, removed, or changed in size since the last fresh installation or upgrade and shows the results.

file check [*detection-size-kb*]

| Syntax Description | Parameters | Description |
|--------------------|--------------------------|---|
| | <i>detection-size-kb</i> | Specifies the minimum file size change that is required for the command to display the file as changed. Default value: 100 KB. |

Command Modes Administrator (admin:)

Usage Guidelines The command notifies you about a possible impact to system performance and asks you whether you want to continue. The display includes both deleted and new files.



Caution

Because this command can affect system performance, Cisco recommends that you run the command during off-peak hours.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file delete

This command deletes a log on the active or inactive side.

file delete { activelog | inactivelog } [file-spec] [detail] [noconfirm]

| Syntax Description | Parameters | Description |
|--------------------|--------------------|--|
| | activelog | Specifies a log on the active side. |
| | inactivelog | Specifies a log on the inactive side. |
| | file-spec | Specifies the path and filename of the log or logs to delete (includes install log files). |
| | detail | Shows a listing of deleted files with the date and time. |
| | noconfirm | Deletes files without asking you to confirm each deletion. |

Command Modes Administrator (admin:)

Usage Guidelines You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.



Caution

You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file delete tftp

This command deletes a TFTP file.

file delete tftp [file-spec] [detail] [noconfirm]

| Syntax Description | Parameters | Description |
|--------------------|------------------|--------------------------------|
| | file-spec | Represents the TFTP file name. |

| Parameters | Description |
|------------------|--|
| detail | Shows a listing of deleted files with the date and time. |
| noconfirm | Deletes files without asking you to confirm each deletion. |

Command Modes

Administrator (admin):

Usage Guidelines

You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.

**Caution**

You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file delete dir tftp

This command deletes the TFTP directory.

file delete dir tftp *dir-name* [**detail**]**Syntax Description****Parameters***dir-name* Specifies the TFTP directory to delete.**detail** Shows a listing of deleted files with the date and time.**Command Modes**

Administrator (admin):

Usage Guidelines

You get prompted for confirmation after you enter the command. You cannot delete directories or files that are in use.

**Caution**

You cannot recover a deleted file, but you may be able to with The Disaster Recovery System.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file dump

This command dumps the contents of a log, a page at a time.

file dump {activelog | inactivelog | install} file-spec [hex] [recent] [regexp expression]

| Syntax Description | Parameters | Description |
|--------------------|--------------------------|---|
| | activelog | Specifies a log on the active side. |
| | inactivelog | Specifies a log on the inactive side. |
| | install | Specifies an installation log. |
| | <i>file-spec</i> | Represents the log file to dump. |
| | hex | Shows output in hexadecimal. |
| | recent | Dumps the most recently changed file in the directory. |
| | regexp expression | Displays only the lines in the file that match the regular expression <i>expression</i> . |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

This command dumps contents of file `_cdrIndex.idx`.

```
admin: file dump activelog cm/cdr/_cdrIndex.idx
```

file dump sftpdetails

This command specifies the list of files that can be dumped in the SFTP context and allows you to choose which file to dump.

file dump sftpdetails

Command Modes Administrator (admin:)

Usage Guidelines Enter a to dump all SFTP-related files. Enter q to exit this command.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file dump tftp

This command dumps the contents of a TFTP file to the screen, a page at a time.

file dump tftp *file-spec* [*page*] [*detail*] [*hex*]

Syntax Description

| Parameters Description | |
|------------------------|--|
| <i>file-spec</i> | Represents the name of a TFTP file. |
| page | Displays the output one screen at a time. |
| detail | Displays the listing with the date and time. |
| hex | Displays the output in hexadecimal. |

Command Modes

Administrator (admin:)

Usage Guidelines



Note *file-spec* must resolve to a single file.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file fragmentation sdi

This command shows file fragmentation information about SDI log files.

file fragmentation sdi **most** {**fragmented** | **recent**} [*number*]

Syntax Description

| Parameters | Description |
|------------------------|---|
| most fragmented | Represents the most fragmented log files. |

file fragmentation sdi file

| Parameters | Description |
|--------------------|---|
| most recent | Represents the most recent logs files. |
| number | Represents the number of files to list. |

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file fragmentation sdi file

This command shows file fragmentation information about an SDI log file.

file fragmentation sdi file *filename* [verbose]**Syntax Description**

| Parameters | Description |
|-----------------|--|
| <i>filename</i> | Represents the SDI log file name. |
| verbose | Shows more detailed information on the screen. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level:1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file fragmentation sdi all

This command shows file fragmentation information about all SDI log files in the directory.

file fragmentation sdi all *filename***Syntax Description**

| Parameters | Description |
|-----------------|---|
| <i>filename</i> | Specifies the SDI log file name for which you want to show all fragmentation details. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

file fragmentation sdl

This command shows file fragmentation information about the most fragmented SDL log files.

file fragmentation sdl most {fragmented | recent} [number]

| Syntax Description | Parameters | Description |
|--------------------|------------------------|---|
| | most fragmented | Represents the most fragmented log files. |
| | most recent | Represents the most recent log files. |
| | <i>number</i> | Represents the number of files to list. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection.

file fragmentation sdl file

This command displays file fragmentation information about an SDL log file.

file fragmentation sdl file *filename* [verbose]

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | <i>filename</i> | Represents the file name of the SDL log file. |
| | verbose | Shows more detailed information on the screen. |

Command Modes Administrator (admin:)

file fragmentation sdl all**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection.

file fragmentation sdl all

This command shows file fragmentation information about all SDL log files in the directory.

file fragmentation sdl all *filename***Syntax Description****Parameters Description***filename* Represents the file name for which you want to show all fragmentation details.**Command Modes**

Administrator (admin):

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection.

file get

This command sends a log to another system by using SFTP.

file get {activelog|inactivelog|install} *file-spec* [{*reltimeabstime*}] [match *regex*] [recurs] [compress]**Syntax Description**

| Parameters | Description |
|--------------------|---|
| activelog | Specifies a log on the active side. |
| inactivelog | Specifies a log on the inactive side. |
| install | Specifies an installation log. |
| <i>file-spec</i> | Specifies the name of the file to transfer. |
| <i>reltime</i> | The relative time period, specified in minutes hours days weeks months time value |

| Parameters | Description |
|---------------------------|---|
| <i>abstime</i> | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| match <i>regex</i> | Match a particular string in the filename, specified as <i>regex</i> . |
| recurs | Get all files, including subdirectories. |
| compress | Transfer files as compressed file. |
| tftp | |

Command Modes

Administrator (admin:)

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

This example gets all files in the activelog operating system directory that match the string "plat."

admin: file get activelog platform match plat

This example gets all operating system log files for a particular time period.

admin: file get activelog platform/log abstime 18:00:10/20/13 18:00:10/21/13

file get salog

This command sends the partBsalog or salog directory to another system by using SFTP.

file get {partBsalog | salog} file-spec [{reltimeabstime}] [match regex] [recurs] [compress]

| Syntax Description | Parameters | Description |
|--------------------|-------------------|-------------------------------------|
| | partBsalog | Specifies the partBsalog directory. |
| | salog | Specifies the salog directory. |

| Parameters | Description |
|---------------------------|---|
| <i>file-spec</i> | Specifies the name of the file to transfer. |
| <i>reltime</i> | The relative time period, specified in minutes hours days weeks months time value |
| <i>abstime</i> | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| match <i>regex</i> | Match a particular string in the filename, specified as <i>regex</i> . |
| recurs | Get all files, including subdirectories. |
| compress | Transfer files as compressed file. |

Command Modes

Administrator (admin:)

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file get tftp

This command sends a TFTP file to another system by using SFTP.

file get tftp *file-spec* [{*reltimeabstime*}] [**match** *regex*] [**recurs**] [**compress**]

| Syntax Description | Parameters | Description |
|--------------------|------------------|---|
| | <i>file-spec</i> | Specifies the name of the TFTP file to transfer. |
| | <i>reltime</i> | The relative time period, specified in minutes hours days weeks months time value |

| Parameters | Description |
|---------------------------|---|
| <i>abstime</i> | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| match <i>regex</i> | Match a particular string in the filename, specified as <i>regex</i> . |
| recur | Get all files, including subdirectories. |
| compress | Transfer files as compressed file. |

Command Modes

Administrator (admin):

Usage Guidelines

After the command identifies the specified files, you get prompted to enter an SFTP host, username, and password.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file list

This command lists the log files in an available log directory.

file list {activelog | inactivelog | install} file-spec [{page | detail | reverse}] [{date | size}]

| Syntax Description | Parameters | Description |
|--------------------|--------------------|--|
| | activelog | Specifies a log on the active side. |
| | inactivelog | Specifies a log on the inactive side. |
| | install | Specifies an installation log. |
| | <i>file-spec</i> | Specifies the name of the log file . |
| | page | Shows the output one screen at a time. |
| | detail | Shows a detailed listing with date and time. |
| | reverse | Reverses the sort direction. |
| | date | Sorts files by date. |

file list salog

| Parameters | Description |
|------------|----------------------|
| size | Sorts files by size. |

Command Modes Administrator (admin:)**Usage Guidelines Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example: Log Files with Details

This example lists operating system log files with details.

admin: file list activelog platform/log page detail

Example: Directories in the CDR Repository

This example lists directories in CDR repository.

admin: file list activelog cm/cdr_repository

Example: CDR Files by Size

This example lists CDR files in a specified directory by size.

admin: file list activelog cm/cdr_repository/processed/20050812 size

file list salog

This command lists the partBsalog or salog directory.

file list {partBsalog | salog} file-spec [{page | detail | reverse}] [{date | size}]

| Syntax Description | Parameters | Description |
|--------------------|-------------------|--|
| | partBsalog | Specifies the partBsalog log directory. |
| | salog | Specifies the salog log directory. |
| | file-spec | Specifies the path to the file or files to list. |
| | page | Shows the output one screen at a time. |
| | detail | Shows a detailed listing with date and time. |
| | reverse | Reverses the sort direction. |
| | date | Sorts files by date. |

| Parameters | Description |
|------------|----------------------|
| size | Sorts files by size. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file list tftp

This command lists TFTP files.

file list tftp *file-spec* [{page | detail | reverse}] [{date | size}]

| Syntax Description | Parameters | Description |
|--------------------|------------------|--|
| | <i>file-spec</i> | Specifies the name of the TFTP file |
| | page | Shows the output one screen at a time. |
| | detail | Shows a detailed listing with date and time. |
| | reverse | Reverses the sort direction. |
| | date | Sorts files by date. |
| | size | Sorts files by size. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file search

This command searches the content of a log and shows the matching lines a page at a time.

file search {activelog | inactivelog | install} file-spec [{reltimeabstime}] [ignorecase]

| Syntax Description | Parameters | Description |
|--------------------|--------------------|--|
| | activelog | Specifies a log on the active side. |
| | inactivelog | Specifies a log on the inactive side. |
| | install | Specifies an installation log. |
| | file-spec | Specifies the name of the file to search. |
| | reltime | The relative time period, specified in minutes hours days weeks months time value |
| | abstime | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| | ignorecase | Ignores case in a search. |

Command Modes Administrator (admin:)

Usage Guidelines Write the search term in the form of a regular expression, which is a special text string to describe a search pattern.

If the search term is found in only one file, the filename appears at the top of the output. If the search term is found in multiple files, each line of the output begins with the filename in which the matching line was found.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

file search tftp

This command searches the content of a TFTP file and shows the matching lines a page at a time.

file search tftp file-spec [{reltimeabstime}] [ignorecase]

| Syntax Description | Parameters | Description |
|--------------------|------------------|--|
| | file-spec | Specifies the name of the TFTP file to search. |

| Parameters | Description |
|-------------------|---|
| <i>reltime</i> | The relative time period, specified in minutes hours days weeks months time value |
| <i>abstime</i> | The absolute time period, specified as hh:mm:MM/DD/YY hh:mm:MM/DD/YY |
| ignorecase | Ignores case in a search. |

Command Modes

Administrator (admin:)

Usage Guidelines

Write the search term in the form of a regular expression, which is a special text string to describe a search pattern.

If the search term is found in only one file, the filename appears at the top of the output. If the search term is found in multiple files, each line of the output begins with the filename in which the matching line was found.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

file tail activelog

This command tails (prints the last few lines) of a log file.

file tail {activelog | inactivelog | install} filespec [hex] [lines] [regexp expression]

Syntax Description

| Parameters | Description |
|------------------------------------|---|
| activelog | Specifies a log on the active side. |
| inactivelog | Specifies a log on the inactive side. |
| install | Specifies an installation log. |
| filespec | Specifies the path to the file. You can use the wildcard character, *, for filename as long as it resolves to one file. |
| hex | Show the listing in hexadecimal. |
| lines | Specifies the number of lines to display. |
| regexp <i>expression</i> | Tails log files that match <i>expression</i> |

Command Modes

Administrator (admin:)

file tail tftp

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

This example tails the operating system CLI log file.

admin: file tail activelog platform/log/cli00001.log

file tail tftp

This command tails (prints the last few lines) of a TFTP file.

file tail tftp *filespec* [**detail**] [**hex**] [**lines**]

| Syntax Description | Parameters | Description |
|--------------------|-----------------|---|
| | filespec | Specifies the path to the file. You can use the wildcard character, *, for filename as long as it resolves to one file. |
| | detail | Long listing with date and time |
| | hex | Show the listing in hexadecimal. |
| | lines | Specifies the number of lines to display. |

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file view

This command shows the contents of log files.

file view {activelog/inactivelog/install} **file-spec**

| Syntax Description | Parameters | Description |
|--------------------|------------------|--|
| | activelog | Shows the contents of an active side logging files |

| Parameters | Description |
|--------------------|--|
| inactivelog | Shows the contents of an inactive side logging files |
| install | Shows the contents of an install logging file |
| <i>file-spec</i> | Specifies the path to the file to view. You can use the wildcard character, *, as long as it resolves to one file. |

Command Modes Administrator (admin:)

Usage Guidelines



Caution Do not use this command to view binary files because this can corrupt the terminal session.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

Example

This example shows a particular CDR log on the active side.

```
admin: file view activelog /cm/cdr_repository/processed/20058012/{filename}
```

file view activelog

This command shows the contents of log files.

file view activelog file-spec

| Syntax Description | Parameters | Description |
|--------------------|------------------|--|
| | activelog | Shows the contents of an active side logging files |
| | <i>file-spec</i> | Specifies the path to the file to view. You can use the wildcard character, *, as long as it resolves to one file. |

Command Modes Administrator (admin:)

Usage Guidelines



Caution Do not use this command to view binary files because this can corrupt the terminal session.



Note This command may use a considerable amount of I/O and running it may impact system performance. It is highly recommended that this command be run off-hours.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

Example

This example shows a particular log on the active side.

```
admin:file view activelog cm/trace/ccm/sdl/{filename}
```

file view inactivelog

This command displays the contents of a log on the inactive side.

file view inactivelog {file-spec}

Syntax Description

Parameters Description

file-spec Specifies the path to the file to view. You can use the wildcard character, *, for **file-spec** as long as it resolves to one file.

Command Modes

Administrator (admin:)

Usage Guidelines



Caution Do not use this command to view binary files because this can corrupt the terminal session.



Note This command may use a considerable amount of I/O and running it may impact system performance. It is highly recommended that this command be run off-hours.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified CM, Unified CM with IM and Presence, Cisco Unity Connection

Example

This example shows a particular log on the inactive side.

```
admin:file view inactivelog cm/trace/ccm/sdl/{filename}
```

file view system-management-log

This command shows the contents of the Integrated Management Logs (IML).

file view system-management-log

Command Modes Administrator (admin:)

Usage Guidelines

Caution Do not use this command to view binary files because this can corrupt the terminal session.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

file view tftp

This command displays the contents of the installation log.

file view tftp *file-spec*

Syntax Description**Parameters Description**

file-spec Specifies the path to the file to view. You can use the wildcard character, *, as long as it resolves to one file.

Command Modes

Administrator (admin:)

Usage Guidelines

Caution Do not use this command to view binary files because this can corrupt the terminal session.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection



CHAPTER 4

License Commands

- [license smart deregister](#), on page 37
- [license smart register idtoken <token> \[force\]](#), on page 38
- [license smart renew auth](#), on page 38
- [license smart renew ID](#), on page 38
- [license smart transport direct](#), on page 39
- [license smart transport gateway <URL>](#), on page 39
- [license smart transport proxy <proxy-server> <proxy-port>](#), on page 40
- [license smart factory reset](#), on page 40
- [license smart reservation enable](#), on page 41
- [license smart reservation disable](#), on page 41
- [license smart reservation request](#), on page 41
- [license smart reservation cancel](#), on page 42
- [license smart reservation install "<authorization-code>"](#), on page 42
- [license smart reservation install-file <url>](#), on page 42
- [license smart reservation return](#), on page 43
- [license smart reservation return authorization "<authorization-code>"](#), on page 43
- [license smart reservation set license_count](#), on page 44
- [license smart export request local <exportfeaturename>](#), on page 44
- [license smart export return local <exportfeaturename>](#), on page 45
- [license smart export cancel](#), on page 45

license smart deregister

Use this command to unregister smart licensing on Unified Communications Manager and remove the product from Cisco Smart Software Manager.

license smart deregister

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

```
license smart register idtoken <token> [force]
```

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart register idtoken <token> [force]

Use this command to register Unified Communications Manager with Cisco Smart Software Manager using an ID token.

license smart register idtoken <token> [force]

Command Modes Administrator (admin):

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart renew auth

Use this command to manually renew the license usage information .

license smart renew auth

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart renew ID

Use this command to manually renew the license registration.

license smart renew ID

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart transport direct

Use the following command to configure the Smart Licensing feature to send license usage information directly to Cisco Smart Software Manager. This is a default setting.

license smart transport direct

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager



Note The following command is executed when Unified Communications Manager is unregistered with Cisco Smart Software Manager or satellite.

license smart transport gateway <URL>

Use the following command to configure the Smart Licensing feature to send license usage information to Cisco Smart Software Manager through an on-premise Transport Gateway or Smart Software Manager satellite. The setting is used when the product does not have internet access.

license smart transport gateway <URL>

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager



Note The following command is executed when Unified Communications Manager is unregistered with Cisco Smart Software Manager or satellite.

license smart transport proxy <proxy-server> <proxy-port>

license smart transport proxy <proxy-server> <proxy-port>

Use the following command to configure the Smart Licensing feature to communicate with Cisco Smart Software Manager through an HTTP or HTTPS Proxy:

<proxy-server> - Proxy Server IP Address/HostName

<proxy-port> - Proxy Server Port

license smart transport proxy <proxy-server> <proxy-port>

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager



Note The following command is executed when Unified Communications Manager is unregistered with Cisco Smart Software Manager.



Note When user gets the prompt **Do you want to enable Authentication based proxy? Yes/No**

Enter "Yes" if you want to register Unified Communication Manager with Cisco Smart Software Manager using authentication based proxy server.

Example

```
admin:license smart transport proxy <proxy-server> <proxy-port>
Do you want to enable Authentication based proxy ? y/n y
User Name : xyz
Password: *****
```

Result: Transport settings updated successfully.

license smart factory reset

Use this command to clear all licensing information from the trusted store and memory, except the evaluation period count down and the Specific License Reservation (SLR) sequence number.

license smart factory reset

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unified Communications Manager

license smart reservation enable

Use this command to enable the license reservation feature.

license smart reservation enable

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart reservation disable

Use this command to disable the license reservation feature.

license smart reservation disable

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart reservation request

Use this command to generate reservation request code from Unified Communications Manager product.

license smart reservation request

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

license smart reservation cancel

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart reservation cancel

Use this command to cancel the reservation process before the authorization code obtained from Cisco Smart Software Manager against the Product request code is installed.

license smart reservation cancel**Command Modes** Administrator (admin)**Requirements**

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart reservation install "<authorization-code>"

Use this command to install the license reservation authorization-code generated on the Cisco Smart Software Manager.

license smart reservation install "<authorization-code>"**Command Modes** Administrator (admin)**Requirements**

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart reservation install-file <url>

Use this command to install the license reservation authorization-code file generated on the Cisco Smart Software Manager.

license smart reservation install-file <url>**Command Modes** Administrator (admin)**Requirements**

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection



Note

url is mandatory Path to the authorization-code file on SFTP server in below format:

sftp://<HostName/IP>:<port>/<Path to Authorization-Code file>

license smart reservation return

Use this command to generate a return code that must be entered into the Cisco Smart Software Manager to return the licenses to the virtual account pool.

license smart reservation return

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

license smart reservation return authorization "**<authorization-code>**"

Use this command to generate a return code using the authorization code specified on the command line. The return code must be entered into the Cisco Smart Software Manager to return the licenses to the virtual account pool.

license smart reservation return authorization "<authorization-code>"

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

```
license smart reservation set license_count
```

license smart reservation set license_count

Use this command to configure or update the license count for the system to operate within when Permanent License Reservation is enabled. License count configured using this CLI does not affect compliance status and is for administrator reference only. The license count set by admin using the CLI will be displayed on the Unified Communications Manager License Management UI screen.

license smart reservation set license_count

Command Modes Administrator (admin):

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager , Cisco Emergency Responder, and Cisco Unity Connection

license smart export request local <exportfeaturename>

Use this command to allow user with Smart Account for whom Export Restrictions apply, to request a regulatory export license from Cisco Smart Software Manager or satellite.

The command returns an export authorization key if regulatory Export License is available from Cisco Smart Software Manager or satellite and enable export-controlled functionality on the product.

license smart export request local <exportfeaturename>



Note

- Export restricted feature name for Unified Communications Manager is <CUCM_Export_Restricted_Authorization_Key>
- Export restricted feature name for Cisco Unity Connection is <CUC_Export_Restricted_Authorization_Key>

Command Modes Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unified Communications Manager, Cisco Unity Connection.

license smart export return local <exportfeaturename>

Use this command to allow a return, previously requested export restricted license to Cisco Smart Software Manager or satellite. The export authorization key for the export restricted feature is removed from the system.

license smart export return local <exportfeaturename>

**Note**

- Export restricted feature name for Unified Communications Manager is <CUCM_Export_Restricted_Authorization_Key>
- Export restricted feature name for Cisco Unity Connection is <CUC_Export_Restricted_Authorization_Key>

Command Modes

Administrator (admin)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unified Communications Manager, Cisco Unity Connection.

license smart export cancel

Use this command to allow user with Smart Account for whom Export Restrictions apply, to cancel the automatic retry of previously failed export request or return from Cisco Smart Software Manager or satellite.

license smart export cancel

Command Modes

Administrator (admin)

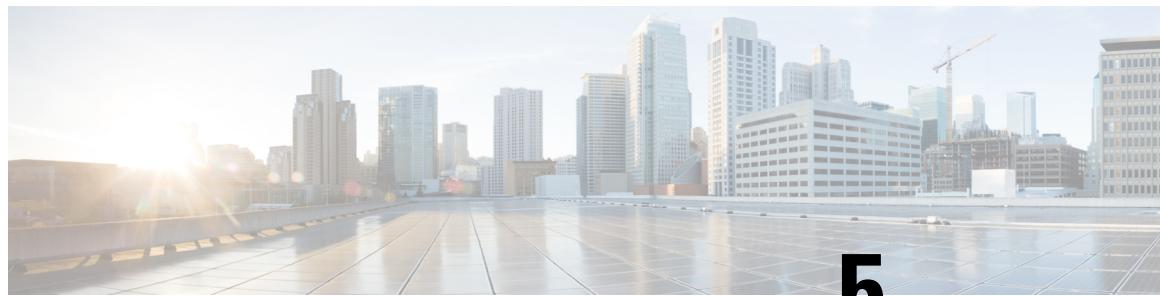
Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unified Communications Manager, Cisco Unity Connection.

```
license smart export cancel
```



CHAPTER 5

Run Commands

- [run cuc dbquery, on page 47](#)
- [run cuc preupgrade test, on page 48](#)
- [run cuc smptest, on page 50](#)
- [run cuc sysagent task, on page 50](#)
- [run cuc vui rebuild, on page 51](#)
- [run loadcsv, on page 52](#)
- [run loadxml, on page 52](#)
- [run sql, on page 53](#)
- [run pe sql, on page 53](#)

run cuc dbquery

This command runs an SQL query and displays the results.

run cuc dbquery *database_name* *sql_query* [page]

| Syntax Description | Parameters | Description |
|--------------------|----------------------|---|
| | <i>database_name</i> | Specifies the database that <i>sql_statement</i> operates on. Note Be aware that database names are case sensitive. Connection databases include: unitydirdb : Contains the directory and configuration data. unitydyndb : Contains dynamic data that Connection uses internally. unitymbxdb1 to unitymbxdb5 : Contains the data about the current voice messages in the corresponding mailbox store. This data includes pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1 . unityrptdb : Contains audit log data. |
| | <i>sql_query</i> | Specifies the SQL query that you want to run. |

run cuc preupgrade test

| Parameters | Description |
|-------------|--|
| page | Shows the output one page at a time. |
| Note | Be aware that page is case sensitive. |

Command Modes Administrator (admin:)**Usage Guidelines** You can also use the **run cuc dbquery** command with the **csp_ConfigurationModify** procedure, which configures the Wait for Blind Transfer Ringing timer. The command usage for this timer is as follows:

```
run cuc dbquery unitydirdb execute procedure
csp_ConfigurationModify(pFullName='System.Telphony.WaitForBlindTransferLongTimeoutMs',pvalueulong="new
value"
```

where, *new value* specifies the value of the Wait for Blind Transfer Ringing Timer parameter. The default and minimum value of this parameter is 500ms. The maximum value of this parameter can be 5000ms.

-

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

The following example runs the SQL query **select alias from vw_usertemplate** on the **unitydirdb** database.

```
admin: run cuc dbquery unitydirdb select alias from vw_usertemplate

alias
-----
AdministratorTemplate
VoiceMailUserTemplate
```

run cuc preupgrade test

This command verifies the state of the connection server on which the upgrade process is to be performed and specifies the actions that can be taken before upgrading the system.

run cuc preupgrade test

Command Modes Administrator (admin:)

| | |
|-------------------------|------|
| Usage Guidelines | None |
|-------------------------|------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only.

Example

```
admin:run cuc preupgrade test
=====
DISCLAIMER :::
This cli command should be executed from publisher before upgrade to
check system health. This cli command is not intended to correct the
system state , rather it aims at informing the administrator what all
actions are advised to be taken before running upgrade.
=====
Checking connection db. Please wait...Done
Checking critical services. Please wait...Done
Checking cluster state. Please wait...Done
Checking cop file installation. Please wait...Done
Checking locales installation. Please wait...Done
Checking drs backup history. Please wait...Done
=====
R E P O R T      C A R D
=====
Locales Installation Test: PASS
Connection DB Test: PASS
DRS Backup History Test: FAIL
Cluster State Test: SKIPPED
Critical Services Test: PASS
Cop File Installation Test: SKIPPED
=====
A C T I O N      S U M M A R Y
=====
ACTION : Connection DB is online.
          NO constraints were found disabled in :unitydirdb,NO ACTION required before upgrade.

          NO indexes were found disabled in :unitydirdb,NO ACTION required before upgrade.
          NO constraints were found disabled in :unitydyndb,NO ACTION required before upgrade.

          NO indexes were found disabled in :unitydyndb,NO ACTION required before upgrade.
          NO constraints were found disabled in :unitymbxdb1,NO ACTION required before
upgrade.
          NO indexes were found disabled in :unitymbxdb1,NO ACTION required before upgrade.
          NO constraints were found disabled in :unityrptdb,NO ACTION required before upgrade.

          NO indexes were found disabled in :unityrptdb,NO ACTION required before upgrade.
          Connection DB state is GOOD,NO ACTION required before upgrade.
ACTION : All Critical services are running ,NO ACTION required before upgrade.
ACTION : Standalone/Cores detected , excluding cluster state checking
ACTION : Skipping COP installation check, product version detected :'8.6.2.21018-1',NO
ACTION required before upgrade.
ACTION : No locales were found installed ,NO ACTION required before upgrade.
ACTION : Make Sure DRS backup is taken atleast a day before upgrade.
Check report /var/log/active/cuc/cli/preupgrade_120325-224523.txt for details.
```

run cuc smptest

run cuc smptest

This command initiates a test that helps to verify the outgoing or incoming SMTP configuration for SpeechView transcriptions.

run cuc smptest *email-address*

| Syntax Description | Parameters | Description |
|--------------------|----------------------|------------------------------|
| | <i>email-address</i> | Specifies the email address. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

| | |
|------------------|--|
| Usage Guidelines | The test sends a test message to a specified email address. You then access the email account and reply to the test message without changing the subject line. The test passes after the Cisco Unity Connection server receives the response. The success or failure of parts of the test help to pinpoint problems in the outgoing or incoming SMTP configuration for transcriptions. |
|------------------|--|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection.

Example

The following example runs the Sysagent task **CleanDeletedMessagesTask**.

```
admin: run cuc sysagent task CleanDeletedMessagesTask
```

run cuc sysagent task

This command runs a Sysagent task.

run cuc sysagent task *task_name*

| Syntax Description | Parameters | Description |
|--------------------|------------------|---|
| | <i>task_name</i> | Specifies the name of the Sysagent task that you want to run. |

In an HTTP(S) network, you need to provide the HTTP(S) link display name as a parameter in the command to run directory synchronization (Data.LocalNetworkSync) and voice name synchronization (Data.LocalNetworkSync.Voicename) tasks. The syntax is shown below:

run cuc sysagent task *task_name* *HTTP(S)LinkDisplayName*

The following example runs the **Data.LocalNetworkSync** task:

```
admin: run cuc sysagent task Data.LocalNetworkSync HTTP(S)LinkDisplayName1
```

```
Data.LocalNetworkSync started
```

Where HTTP(S)LinkDisplayName is the display name of the HTTP(S) link with which you want to synchronize the directory information.



Note

Before running the command, make sure that the scheduled task for directory or voice name synchronization is disabled for the specified HTTP(S) link "HTTP(S)LinkDisplayName" to avoid any issues in synchronization.

Command Modes

Administrator (admin:)

Usage Guidelines

For a list of Sysagent tasks, run the command **show cuc sysagent task list** (Cisco Unity Connection only). Be aware that sysagent task names are case sensitive.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

The following example runs the Sysagent task **Umss.CleanDeletedMessagesTask**.

```
admin: run cuc sysagent task Umss.CleanDeletedMessagesTask
```

```
Umss.CleanDeletedMessagesTask started
```

run cuc vui rebuild

This command instructs the voice recognition transport utility to immediately rebuild the voice recognition name grammars with pending changes.

run cuc vui rebuild

Command Modes

Administrator (admin:)

Usage Guidelines

This command rebuilds only grammars that have changes flagged in the database. This command ignores name grammar update blackout schedules and executes immediately. Due to the overhead of retrieving potentially large amounts of name-related data from the database, you should use this command sparingly and only when absolutely necessary.

run loadcsv

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

run loadcsv

This command is used on the publisher node to install the csv files that are available on a server.

run loadcsv**Command Modes**

Administrator (admin:)

Usage Guidelines**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

run loadxml

This command is a workaround for when service parameters or product-specific information does not appear in the administration window as expected.

run loadxml**Command Modes**

Administrator (admin:)

Usage Guidelines**Note**

This command is processor intensive, and you may need to restart some services after you run this command.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

run sql

This command allows you to run an SQL command.

run sql *sql_statement*

Syntax Description

Parameters Description

sql_statement Specifies the SQL command to run.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection



Note

Users with ordinary privileges can run read-only SQL commands.

Example

This example runs an SQL command.

```
admin: run sql select name from device
```

run pe sql

This command allows you to run an input SQL statement against the specified presence datastore.

run pe sql *datastore_name* *sql_statement*

Syntax Description

Parameters Description

datastore_name Represents the name of the datastore.

sql_statement Represents the SQL command to run.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: IM and Presence service on Unified Communications Manager

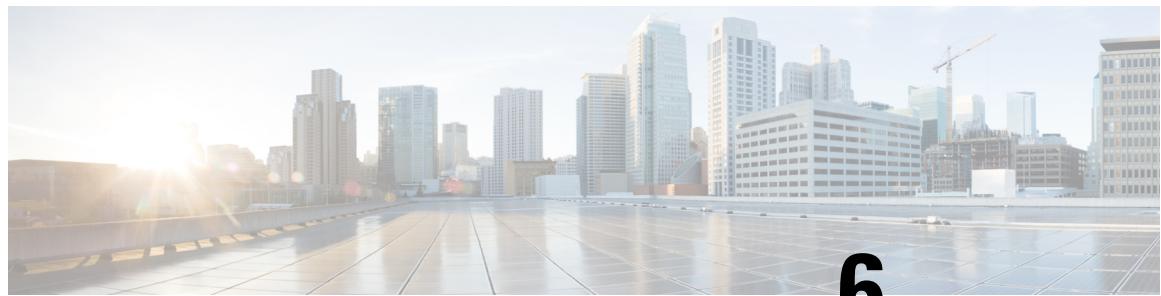


Note Users with ordinary privileges can run read-only SQL commands.

Example

This example runs an SQL command against the datastore.

```
admin: run pe sql ttsoft select * from presenceeventtable
```



CHAPTER 6

Set Commands

- [set account enable](#), on page 57
- [set account name](#), on page 57
- [set account ssorecoveryurlaccess](#), on page 59
- [set account ssuidvalue](#), on page 60
- [set cert bulk consolidate](#), on page 61
- [set cert bulk export](#), on page 61
- [set cert bulk import](#), on page 62
- [set cert bulk sftp](#), on page 62
- [set cert default-ca-list disable](#), on page 63
- [set cert default-ca-list enable](#), on page 64
- [set cert delete](#), on page 66
- [set cert import](#), on page 66
- [set cert regen](#), on page 67
- [set cert regen ITLRecovery](#), on page 67
- [set cli pagination](#), on page 68
- [set cli session timeout](#), on page 69
- [set commandcount](#), on page 70
- [set csr gen](#), on page 70
- [set cuc jetty stderrlog](#), on page 71
- [set cuc jetty stdoutlog](#), on page 72
- [set cuc jetty requestlog](#), on page 73
- [set cuc speechview registration certificate size](#), on page 73
- [set cuc srsv timeout](#), on page 74
- [set cuc trace](#), on page 74
- [set date](#), on page 75
- [set dscp defaults](#), on page 76
- [set dscp](#), on page 76
- [set dscp marking](#), on page 77
- [set ipsec policy_group](#), on page 78
- [set ipsec policy_name](#), on page 78
- [set key regen authz encryption](#), on page 79
- [set key regen authz signing](#), on page 79
- [set logging](#), on page 79

- [set Login Grace Timeout, on page 80](#)
- [set network cluster publisher, on page 80](#)
- [set network cluster subscriber details, on page 81](#)
- [set network cluster subscriber dynamic-cluster-configuration, on page 82](#)
- [set network dhcp eth0, on page 82](#)
- [set network dns, on page 83](#)
- [set network dns options, on page 83](#)
- [set network domain, on page 84](#)
- [set network failover, on page 85](#)
- [set network gateway, on page 85](#)
- [set network hostname, on page 86](#)
- [set network ip eth0, on page 88](#)
- [set network ipv6 dhcp, on page 89](#)
- [set network ipv6 gateway, on page 89](#)
- [set network ipv6 service, on page 90](#)
- [set network ipv6 static_address, on page 90](#)
- [set network max_ip_conntrack, on page 91](#)
- [set network mtu, on page 91](#)
- [set network name-service hosts cache-enable, on page 92](#)
- [set network name-service hosts max-db-size, on page 93](#)
- [set network name-service hosts negative-time-to-live, on page 93](#)
- [set network name-service hosts persistent, on page 94](#)
- [set network name-service hosts positive-time-to-live, on page 94](#)
- [set network name-service hosts suggested-size, on page 94](#)
- [set network name-service services cache-enable, on page 95](#)
- [set network name-service services max-db-size, on page 95](#)
- [set network name-service services negative-time-to-live, on page 96](#)
- [set network name-service services persistent, on page 96](#)
- [set network name-service services positive-time-to-live, on page 97](#)
- [set network name-service services suggested-size, on page 97](#)
- [set network nic eth0, on page 98](#)
- [set network ntp option, on page 98](#)
- [set network pm tud state, on page 99](#)
- [set network restore , on page 99](#)
- [set network status eth0, on page 101](#)
- [set network name-service, on page 101](#)
- [set password complexity minimum-length, on page 102](#)
- [set password age, on page 102](#)
- [set password change-at-login, on page 103](#)
- [set password complexity character, on page 103](#)
- [set password complexity character difference, on page 105](#)
- [set password complexity character max-repeat, on page 105](#)
- [set password expiry maximum-age, on page 106](#)
- [set password expiry user maximum-age configure, on page 107](#)
- [set password expiry minimum-age, on page 107](#)
- [set password expiry user maximum-age, on page 108](#)

- [set password expiry user minimum-age](#), on page 109
- [set password history](#), on page 110
- [set password inactivity](#), on page 110
- [set password system bootloader encryptHash](#), on page 111
- [set password user admin](#), on page 111
- [set password user security](#), on page 112
- [Set replication-sync monitor](#), on page 113
- [set samltrace level](#), on page 113
- [set session maxlimit](#), on page 114
- [set smtp](#), on page 114
- [set strace enable](#), on page 115
- [set strace disable](#), on page 115
- [set timezone](#), on page 115
- [set tls min-version](#), on page 116
- [set trace disable](#), on page 117
- [set trace enable](#), on page 118
- [set tlsresumptiontimeout](#), on page 118
- [set tlstrace*](#), on page 119
- [set web-security](#), on page 120
- [set webapp session timeout](#), on page 121
- [set webapp session maxlimit](#), on page 122
- [set workingdir](#), on page 125

set account enable

This command enables the OS user account that was disabled because of password inactivity.

set account enable *user-id*

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>user-id</i> Specifies the user ID of the account that was disabled. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

set account name

This command sets up a new account on the operating system.

set account name

set account name *name***Syntax Description****Parameters Description**

name Represents the username for the new account.

Enter a name comprised of only alphabets or characters comprised of alphanumeric characters (a-z, A-D, 0-9).

Command Modes

Administrator (admin:)

Usage Guidelines

After you enter the username, the system prompts you to enter the privilege level (0 or 1) and password for the new account. The privilege levels definitions are as follows:

Privilege level 0

Specifies an ordinary privilege level. Users with ordinary privileges can run CLI commands with privilege level 0 only.

Privilege level 1

Specifies an advanced privilege level. Users with advanced privileges can run CLI commands with privilege level 1 and below.

**Note**

The administrator account that the system creates during Unified Communications Manager installation has a privilege level of 4. The administrator can run all commands in the CLI.

The **set account name** command includes the following new prompts:

- **'Allow this User to login to SAML SSO-enabled system through the Recovery URL ? (Yes / No)'** — Level 4 administrators can enable or disable the access to the recovery URL sign-in option for new platform administrators by typing 'Yes' or 'No' on the CLI. The value can be configured to 'Yes' if a user chooses to sign-in using the Recovery URL.
- **'To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]'** — Level 4 administrator can type the unique identifier value for each platform administrator for this prompt.

**Note**

Only the Level 4 administrator has privileges to run all the CLI commands.

The administrator must ensure to perform the following tasks:

- Type either 'Yes' or 'No' for the 'Allow this User to login to SAML SSO-enabled system through Recovery URL ? (Yes / No)' prompt. If this prompt value is blank, an error message appears.
- Type a value for the 'To authenticate a platform login for SSO, a Unique Identifier (UID) must be provided that identifies this user to LDAP (such as sAMAccountName or UPN). Please enter the appropriate LDAP Unique Identifier (UID) for this user:[UID]' prompt. If the prompt value is duplicate, an error message appears. You can hit the Enter key and then, the user account name is saved by default. After the account is created successfully, the administrator will see the message *Account created successfully. Log in to the CLI and update the password before you log in to OS Administration.*
- In the case of SAML SSO login for Operating System Admin pages, if LDAP user consists of '&' character, make sure you create platform user without '&' and then map to LDAP user consisting of '&' character.
- In the case of SAML SSO login for Operating System Admin pages, if LDAP attribute value for User ID is telephonenumber, make sure you create platform user using consisting of alphanumeric characters or English alphabets only. Do not include platform user name with only numeric values. Then, map to the appropriate LDAP user having the UID value as telephone number.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

set account ssorecoveryurlaccess

This command enables or disables the SSO recovery URL access for platform administrators.

**Note**

By default, the platform administrator Level 4 has access to the recovery URL. If the platform administrator Level 4 attempts to update the recovery URL access for own self, an error appears.

set account ssorecoveryurlaccess {enable | disable}userid

Syntax Description

| Parameters | Description |
|----------------|--|
| enable | Enable the recovery sign-in option for platform administrators. |
| disable | Disable the recovery sign-in option for platform administrators. |
| userid | Specifies a particular Cisco Unified Operating System Administrator account. |

set account ssouidvalue**Command Modes** Administrator (admin:)**Usage Guidelines****Note**

- If you enable or disable the recovery sign-in option, which is already enabled or disabled, an error appears.
- The administrator account that the system creates when Unified Communications Manager installs has a privilege level of 4. The administrator can run all commands in the CLI.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager

set account ssouidvalue

This command updates the unique identifier value for the existing platform administrators.

set account ssouidvalue *userid*

Syntax Description

| Parameters | Description |
|---------------|--|
| <i>userid</i> | Specifies a particular Cisco Unified Operating System Administrator account whose unique identifier value needs to be updated. |

Command Modes

Administrator (admin:)

Usage Guidelines**Note**

- When you run the **set account ssouidvalue *userid*** command, a prompt appears to provide the UID value. If the UID value is blank, then samaccountname is saved as ssouidvalue by default.
- If a duplicate UID value exists, an error appears.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager

set cert bulk consolidate

This command consolidates all the certificates that are available on the unit.

set cert bulk consolidate *unit*

| Syntax Description | Parameters | Description |
|--------------------|-------------|---------------------------|
| | <i>unit</i> | Represents the unit name. |

Command Modes Administrator (admin):

Usage Guidelines You must specify the SFTP server information to use for cert bulk operations.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Related Topics

[set cert bulk sftp](#), on page 62

set cert bulk export

This command exports all the certificates that are available on the unit.

set cert bulk export *unit*

| Syntax Description | Parameters | Description |
|--------------------|---------------|--|
| | export | Exports all the available certificates for this unit in this cluster to the preconfigured SFTP location. |
| | <i>unit</i> | Represents the unit name. |

Command Modes Administrator (admin):

Usage Guidelines You must specify the SFTP server information to use for cert bulk operations.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set cert bulk import**Example**

```
admin:set cert bulk export all
Successfully exported tomcat certificate(s) to sftp server.
Successfully exported tftp certificate(s) to sftp server.
```

Related Topics[set cert bulk sftp](#), on page 62

set cert bulk import

This command imports the certificates that are in the SFTP location into the specified unit trust-store.

set cert bulk import *unit*

| Syntax Description | Parameters Description |
|-------------------------|---|
| | <i>unit</i> Represents the unit name. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | You must specify the SFTP server information to use for cert bulk operations. |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set cert bulk import all
Successfully imported tomcat certificates.
Successfully imported tftp certificates.
```

Related Topics[set cert bulk sftp](#), on page 62

set cert bulk sftp

This command prompts for the SFTP server information to use for bulk operations.

set cert bulk sftp

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Usage Guidelines

You must specify the SFTP server information to use for cert bulk operations.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set cert default-ca-list disable

This command disables all or particular default CA certificates from all servers in the cluster.

When you try to execute this command, a warning message appears displaying that this operation disables all or particular default Cisco CA certificates.

```
set cert default-ca-list disable {all | common-name}
```

**Note**

- Please ensure that you are executing this command from the Unified Communications Manager publisher node.
- The default CA certificate names can be obtained by executing the **show cert default-ca-list** command.

Syntax Description

| Parameters | Description |
|--------------------|--|
| all | Deletes all the default CA certificates from all servers in the cluster. |
| common-name | Deletes the particular default CA certificate from all servers in the cluster. |

Command Modes

Administrator (admin:)

Usage Guidelines

Consider the following information after you disable all the default CA certificates.

- Restart the “Cisco Tomcat”, “Cisco CallManager”, “Cisco Tftp”, and “Cisco Certificate Authority Proxy Function” services.

Consider the following information after you disable the specific default CA certificate.

- Restart the “Cisco CallManager”, “Cisco Tftp”, and “Cisco Certificate Authority Proxy Function” services.
- If you are disabling “VeriSign Class 3 Secure Server CA - G3” certificate, then restarting of only “Cisco Tomcat” service is sufficient.

Requirements

Command privilege level: 1

set cert default-ca-list enable

Applies to: Unified Communications Manager

Example

```
admin:set cert default-ca-list disable all

WARNING: This operation will disable all Cisco CA certificates that have been installed
by default. You can use the "show cert default-ca-list" to view the list of default
Cisco CA certificates.
You must restart the "Cisco Tomcat", "Cisco CallManager", "Cisco Tftp" and
"Cisco Certificate Authority Proxy Function" services after running this command.
This command should be run from the Publisher.
Do you wish to proceed (yes|no)? yes
Successfully disabled the default Cisco CA certificates.
Please wait for a few min to UI to reflect the correct status.

admin:set cert default-ca-list disable common-name
Enter the Common Name of Default CA Certificate : CAP-RTP-001
WARNING: This operation will disable the "CAP-RTP-001" Cisco CA certificate.
You must restart the "Cisco CallManager", "Cisco Certificate Authority Proxy Function" and
"Cisco Tftp" services after running this command. This command should be run from the
Publisher.
Do you wish to proceed (yes|no)? yes
Successfully disabled default "CAP-RTP-001" certificate.

admin:set cert default-ca-list disable common-name
Enter the Common Name of Default CA Certificate : VeriSign Class 3 Secure Server CA - G3
WARNING: This operation will disable the "VeriSign Class 3 Secure Server CA - G3" Cisco CA
certificate. You must restart the "Cisco Tomcat" services after running this command.
This command should be run from the Publisher.
Do you wish to proceed (yes|no)? yes
Successfully disabled default "VeriSign Class 3 Secure Server CA - G3" certificate.

admin:set cert default-ca-list enable common-name
Enter the Common Name of Default CA Certificate : capf
The capf certificate is not in the list of default Cisco CA certificates.
admin:
```

set cert default-ca-list enable

This command enables all or particular default CA certificates except CAPF-trust on all servers in the cluster. CAPF-trust certificate enable only on the Unified Communications Manager publisher node not across the cluster.

When you try to execute this command, a warning message appears displaying that this operation enables all or particular default Cisco CA certificates as a trusted certificate.

```
set cert default-ca-list enable {all | common-name}
```



Note

- Please ensure that you are executing this command from the Unified Communications Manager publisher node.
- The default CA certificate names can be obtained by executing the **show cert default-ca-list** command.

| Syntax Description | Parameters | Description |
|--------------------|--------------------|--|
| | all | Enables all the default CA certificates on all servers in the cluster. |
| | common-name | Enables the particular default CA certificate on all servers in the cluster. |

Command Modes Administrator (admin:)

Usage Guidelines Consider the following information after you enable all the default CA certificates.

- Restart the “Cisco Tomcat”, “Cisco CallManager”, “Cisco Tftp”, and “Cisco Certificate Authority Proxy Function” services.

Consider the following information after you enable the specific default CA certificate.

- Restart the “Cisco CallManager”, “Cisco Tftp”, and “Cisco Certificate Authority Proxy Function” services.
- If you are enabling “VeriSign Class 3 Secure Server CA - G3” certificate, then restarting of only “Cisco Tomcat” service is sufficient.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager

Example

```
admin:set cert default-ca-list enable all
```

```
WARNING: This operation will enable all default Cisco CA certificates
as trusted certificates for all nodes in this cluster.
You can use the "show cert default-ca-list" to view the list of default
Cisco CA certificates. You must restart the "Cisco Tomcat", "Cisco CallManager",
"Cisco Tftp" and "Cisco Certificate Authority Proxy Function" services after
running this command. This command should be run from the Publisher.
```

```
Do you wish to proceed (yes|no)? yes
```

```
Successfully enabled the default Cisco CA certificates.
```

```
Please wait for a few minutes for the UI to reflect the correct status.
```

```
admin:set cert default-ca-list enable common-name
```

```
Enter the Common Name of Default CA Certificate : CAP-RTP-002
```

```
WARNING: This operation will install the "CAP-RTP-002" certificate as a trusted certificate
for all nodes in this cluster. You must restart the "Cisco CallManager",
"Cisco Certificate Authority Proxy Function" and "Cisco Tftp" services after running this
command. This command should be run from the Publisher.
```

```
Do you wish to proceed (yes|no)? yes
```

```
Successfully enabled default "CAP-RTP-002" certificate.
```

```
admin:set cert default-ca-list enable common-name
```

```
Enter the Common Name of Default CA Certificate : VeriSign Class 3 Secure Server CA - G3
WARNING: This operation will install the "VeriSign Class 3 Secure Server CA - G3" certificate
as a trusted certificate for all nodes in this cluster. You must restart the "Cisco Tomcat"
services after running this command. This command should be run from the Publisher.
```

```
Do you wish to proceed (yes|no)? yes
```

set cert delete

```
Successfully enabled default "VeriSign Class 3 Secure Server CA - G3" certificate.
```

```
admin:set cert default-ca-list enable common-name
Enter the Common Name of Default CA Certificate : CAP-RTP-003
The CAP-RTP-003 certificate is not in the list of default Cisco CA certificates.
admin:
```

set cert delete

This command deletes a specific certificate file from the trust unit.

set cert delete *unit* *name*

Syntax Description

Parameters Description

| | |
|-------------|--|
| <i>unit</i> | Specifies the name of the trust category, as "own" or "trust". |
| <i>name</i> | Certificate file name. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set cert delete cucm siptest.pem
```

set cert import

This command imports the specified certificate for the specified certificate type.

set cert import *type* *name* [*caCert*]

Syntax Description

Parameters Description

| | |
|-------------------|--|
| <i>type</i> | Specifies the certificate type as "own" or "trust". |
| <i>name</i> | Represents the unit name. |
| [<i>caCert</i>] | Represents the name of the CA certificate file name. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set cert import trust tomcat
Successfully imported certificate for tomcat.
Please restart services related to tomcat for the new certificate to
become active.
```

set cert regen

This command regenerates the certificate for the specified unit.

set cert regen *name*

| Syntax Description | Parameters | Description |
|--------------------|-------------|---------------------------|
| | <i>name</i> | Represents the unit name. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set cert regen tomcat
Successfully regenerated certificate for tomcat.
```

set cert regen ITLRecovery

This command regenerates the ITLRecovery certificate for the specified unit.

After you type this command, a warning message appears displaying that if you are using a tokenless CTL and if the you are regenerating the CallManager certificate, ensure that the CTL file has the updated CallManager certificate and that certificate is updated to endpoints. To regenerate the certificate, type **yes** or else type **no**.

set cli pagination

set cert regen *ITLRecovery*

Syntax Description**Parameters Description**

ITLRecovery Represents the ITLRecovery certificate.

Command Modes

Administrator (admin:)

Requirements**Caution**

You must restart the services related to ITLRecovery for the regenerated certificates to become active.

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set cert regen ITLRecovery
```

WARNING: If you are using a tokenless CTL and if the CallManager certificate is recently generated, please ensure that the CTL File already has the new CallManager certificate and is updated to the endpoints, before generating the ITL Recovery certificate. Are you sure want to proceed?

Proceed with regeneration (yes|no)? yes

Successfully Regenerated Certificate for ITLRecovery.

You must restart the services related to ITLRecovery for the regenerated certificates to become active.

set cli pagination

For the current CLI session, this command turns automatic pagination On or Off.

set cli pagination {on | off}

Syntax Description**Parameters Description**

on Turns pagination on.

off Turns pagination off.

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

```
admin:set cli pagination off
Automatic pagination is turned off
```

set cli session timeout

This command sets the time, in minutes, after which an active CLI session times out and disconnects.

set cli session timeout *minutes*

Syntax Description

Parameters Description

| | |
|----------------|---|
| <i>minutes</i> | Specifies the time, in minutes, that can elapse before an active CLI session times out and disconnects. |
| | <ul style="list-style-type: none"> • Value range: 5-99999 minutes • Default value: 30 minutes |

Command Modes

Administrator (admin:)

Usage Guidelines

Be aware that the new session timeout value becomes effective immediately for a new CLI session; however, active sessions retain their original timeout value. Also the show cli session timeout command reflects the new value, even if the current session does not use that value.



Note

This setting gets preserved through a software upgrade and does not get reset to the default value.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set commandcount

set commandcount

This command changes the CLI command prompt, so it displays how many CLI commands have executed.

set commandcount {enable | disable}

| Syntax Description | Parameters Description |
|--------------------|---|
| | enable Turns on command count. |
| | disable Turns off command count. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set csr gen

This command generates the csr for the unit name.

set csr gen name

| Syntax Description | Parameters Description |
|--------------------|---|
| | name Specifies the unit on which the certificate is generated. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set csr gen tomcat
Successfully Generated CSR for tomcat.
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set cuc jetty stderrlog

This command enables or disables the error log getting generated while any standard error occurs during communicating with the Jetty server. This error log gets generated and is available at the path `/var/log/active/jetty/`.

set cuc jetty stderrlog {enable | disable}

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | enable | Enables the error log on the Jetty server. Be aware that enable is case sensitive. |
| | disable | Disables the error log on the Jetty server. Be aware that disable is case sensitive. |

Command Modes Administrator (admin:)

Usage Guidelines



Caution

You must restart the Jetty services after enabling or disabling the error log on the Jetty server.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

Enable Error Log on Jetty Server Example

```
admin:set cuc jetty stderrlog enable
```

```
Command is executed successfully
To effect changes restart jetty server
Restart Jetty Server through Unity Connection Serviciability .
Go to Tools -> Service Management -> Restart Connection Jetty Service.
Check the logs that should not be generated after running above command.
Check the requestlog by sending one voice message through webinbox.
Notifications should not come in logs
```

```
set cuc jetty stdoutlog
```

set cuc jetty stdoutlog

This command enables or disables the standard input and output log getting generated while communicating with Jetty server. This standard input and output log gets generated and is available at the path `/var/log/active/jetty/`.

```
set cuc jetty stdoutlog {enable | disable}
```

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | enable | Enables the standard input and output log on the Jetty server. Be aware that enable is case sensitive. |
| | disable | Disables the standard input and output log on the Jetty server. Be aware that disable is case sensitive. |

Command Modes Administrator (admin:)

Usage Guidelines



Caution You must restart the Jetty services after enabling or disabling the standard input and output log on the Jetty server.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

Enable Standard Input and Output Log on Jetty Server Example

```
admin:set cuc jetty stdoutlog enable
Command is executed successfully
To effect changes restart jetty server
Restart Jetty Server through Unity Connection Serviciability .
Go to Tools -> Service Management -> Restart Connection Jetty Service.
Check the logs that should not be generated after running above command.
Check the requestlog by sending one voice message through webinbox.
Notifications should not come in logs
```

set cuc jetty requestlog

This command enables or disables the request log getting generated from the Jetty server while any request is raised for notifications. This request log gets generated and is available at the path `/usr/local/jetty/logs/`.

set cuc jetty requestlog {enable | disable}

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | enable | Enables the request log on the Jetty server. Be aware that “enable” is case sensitive. |
| | disable | Disables the request log on the Jetty server. Be aware that “disable” is case sensitive. |

Command Modes Administrator (admin:)

Usage Guidelines



Caution You must restart the Jetty services after enabling or disabling the request log on the Jetty server.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

Enable Request Log on Jetty Server Example

```
admin:set cuc jetty requestlog enable
```

```
Command is executed successfully
To effect changes restart jetty server
Restart Jetty Server through Unity Connection Serviciability .
Go to Tools -> Service Management -> Restart Connection Jetty Service.
Check the logs that should not be generated after running above command.
Check the requestlog by sending one voice message through webinbox.
Notifications should not come in logs
```

set cuc speechview registration certificate size

This command sets up new certificate bit size for Speech to Text service registration and Voicemail transcription with Nuance server.

set cuc srsrv timeout

set cuc speechview registration certificate size *bit_size*

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | <i>bit_size</i> | Specifies the <i>bit_size</i> of certificate. Its allowed values are 1k, 2k or 4k. |

Command Modes Administrator (admin:)

Usage Guidelines To set the desired certificate bit size, use the **set cuc speechview registration certificate size** (Cisco Unity Connection Only) command. The CLI must be executed on the publisher. It will restart the Connection SpeechView Processor service.

Requirements

Command privilege level: 4

set cuc srsrv timeout

This command sets the value for SRSV session timeout.

set cuc srsrv timeout *timeout_value*

| Syntax Description | Parameters | Description |
|--------------------|----------------------|-----------------------------------|
| | <i>timeout_value</i> | Sets the time for session logout. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

set cuc trace

This command enables or disables the specified traces and trace levels.

set cuc trace {enable | disable} *trace_name level*

| Syntax Description | Parameters | Description |
|--------------------|-------------------|---|
| | enable | Enables Connection traces. |
| | disable | Disables Connection traces. |
| | <i>trace_name</i> | Specifies the name of the trace to enable or disable. Be aware that trace names are case sensitive. |

| Parameters | Description |
|--------------|--|
| <i>level</i> | Specifies the level or levels of trace_name that you want to enable or disable. Each trace comprises up to 31 levels, numbered 0 to 30; each level provides a different type of information for the specified trace. When you enable or disable multiple levels, use a comma to separate levels and a hyphen to indicate a range of levels. Do not include spaces. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

| | |
|-------------------------|--|
| Usage Guidelines | To display a list of the traces and trace levels that are currently enabled, use the show cuc trace levels (Cisco Unity Connection Only) command. |
|-------------------------|--|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection only.

Enable VUI Traces 1, 13, and 17 Through 20 Example

```
admin:set cuc trace enable VUI 1,13,17-20
VUI trace levels are now set to: 1,13,17-20
```

Disable VUI Traces 17 Through 20 While VUI Trace Levels 1 and 13 Remain Set Example

```
admin:set cuc trace disable VUI 17-20
VUI trace levels are now set to: 1,13
```

Related Topics

[show cuc trace levels](#), on page 160

set date

This command changes the time and date on the server.

set date *HH:mm:ss:MM/DD/YY*

| Syntax Description | Parameters | Description |
|--------------------|-----------------|---|
| | <i>HH:mm:ss</i> | Represents the time format (24 hours format). |
| | <i>MM/DD/YY</i> | Represents the date format. |
| | Note | Date format MM/DD/YYYY is also accepted. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

set dscp defaults**Usage Guidelines**

If the server is configured to synchronize with external NTP servers, this command requires the user to remove all of those NTP servers.

Requirements

Applies to: Unified Communications Manager and Cisco Unity Connection.

Set Date and Time to 2:10:33 Pm April 13th 2012 Example

```
admin:set date 14:10:33:04/13/12
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set dscp defaults

This command sets the factory default DSCP settings for all of the port tags.

set dscp defaults

Command Modes

Administrator (admin:)

Usage Guidelines

All non-default DSCP settings get removed after you run this command.

You can use the command `show dscp defaults` to see the factory default DSCP settings.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set dscp

This command enables or disables DSCP marking on outgoing TCP or UDP packets. You can enable or disable DSCP on a single port tag, or on all port tags at once.

set dscp {enable | disable} {allport_tag}

Syntax Description**Parameters Description**

all Disables all DSCP port tags.

| Parameters | Description |
|-----------------|--|
| <i>port_tag</i> | Represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. This value is for the portTag field displayed when you use the command show dscp defaults . The set of port tags is predefined. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set dscp marking

This command sets DSCP markings on port tags by using well-known DSCP classes and numeric values.

set dscp marking *port_tag value*

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | <i>port_tag</i> | Represents a DSCP port tag, which is a string that is mapped to a TCP or UDP port to identify the application that uses the port. This value is for the portTag field displayed when you use the command show dscp defaults . The set of port tags is predefined. |
| | <i>value</i> | A DSCP value. You can enter the name of a well-known DSCP class or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

| | |
|-------------------------|--|
| Usage Guidelines | <p>The valid class names as defined by DSCP are:</p> <ul style="list-style-type: none"> • Class Selector: values CS0, CS1, CS2, CS3, CS5, CS6, CS7 <p>The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence.</p> <ul style="list-style-type: none"> • Expedited Forwarding: value EF <p>EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter.</p> <ul style="list-style-type: none"> • Best Effort: value BE <p>Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router.</p> <ul style="list-style-type: none"> • Assured Forwarding: values AF11, AF12, AF13, AF21, AF22, AF23, AF41, AF42, AF43 <p>There are four types of Assured Forwarding classes, each of which has three drop precedence values.</p> |
|-------------------------|--|

set ipsec policy_group

These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set ipsec policy_group

This command enables ipsec policies with the specified policy group name.

set ipsec policy_group {ALL*group*}

| Syntax Description | Parameters | Description |
|--------------------|--------------|--|
| | ALL | Enables all ipsec policy groups. |
| | <i>group</i> | Specifies the name of a particular ipsec policy group to enable. |

Command Modes Administrator (admin):

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and Cisco Unity Connection.

set ipsec policy_name

This command enables the specified ipsec policy.

set ipsec policy_name {ALL*policy_name*}

| Syntax Description | Parameters | Description |
|--------------------|--------------------|--|
| | ALL | Enables all ipsec policies. |
| | <i>policy_name</i> | Specifies the name of a particular ipsec policy to enable. |

Command Modes Administrator (admin):

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and Cisco Unity Connection.

set key regen authz encryption

Run this command on the Unified Communications Manager publisher node to regenerate the symmetric encryption key that encrypts OAuth access tokens and refresh tokens that are used in Cisco Jabber authentication.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager and the IM and Presence Service.

set key regen authz signing

Run this command on the Unified Communications Manager publisher node to regenerate the asymmetric RSA key pair for signing the OAuth access tokens and refresh tokens that are used in Cisco Jabber authentication.

Command Modes

Administrator (admin:)

Usage Guidelines**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager and the IM and Presence Service.

set logging

This command allows you to enable or disable CLI Admin logs.

set logging {enable | disable}

Syntax Description**Parameters Description**

enable Turns on logging.

set Login Grace Timeout

| Parameters | Description |
|----------------|--------------------|
| disable | Turns off logging. |

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set Login Grace Timeout

This command allows you to configure the LoginGraceTimeout value to the mentioned value.

set Login Grace Timeout *LoginGraceTimeout value*

| Syntax Description | Parameters | Description |
|--------------------|--------------------------------|---|
| | <i>LoginGraceTimeout value</i> | Sets the LoginGraceTimeout value for login grace timeout. |

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network cluster publisher

This command sets the network cluster publisher hostname and IP address.

set network cluster publisher {**hostname** | **ip**} *name*

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | hostname | Specifies the hostname of the network cluster. |
| | ip | Specifies the ip address of the network cluster. |

| Parameters | Description |
|-------------|--|
| <i>name</i> | Hostname or IP address to assign to the network cluster publisher. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network cluster subscriber details

Use this command to add subscriber to the processnode or appserver table when Tomcat Webserver is server down and GUI is inaccessible.

set network cluster subscriber details *servertype hostname ip domainname*

| Syntax Description | Parameter | Description |
|--------------------|-------------------|--|
| | <i>servertype</i> | Choose one of these products for this parameter— Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection. This field is mandatory. |
| | <i>hostname</i> | The hostname of the node that you add to the cluster. The hostname is supported on the same domain. This field is mandatory. |
| | <i>ip</i> | The IPv4 address of the node that you add to the cluster. This field is mandatory for IM and Presence publisher and Cisco Unity Connection. |
| | <i>domainname</i> | The domain name of the IM and Presence Service publisher. This field is mandatory for IM and Presence publisher. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection

set network cluster subscriber dynamic-cluster-configuration

set network cluster subscriber dynamic-cluster-configuration

Use this command to enable the Dynamic Cluster Configuration on the publisher. Use this command to specify the duration in which you can add subscriber nodes to the publisher server table. The addition of subscriber nodes is authenticated immediately and those nodes need not wait for the publisher details during the installation of the subscriber nodes.

set network cluster subscriber dynamic-cluster-configuration {default | no. of hours}

| Syntax Description | Parameter | Description |
|--------------------|---------------------|---|
| | default | Enables the Dynamic Cluster Configuration for 24 hours. |
| | no. of hours | Specifies a value from 1 to 24 hours. |

Command Modes Administrator (admin)

Requirements

Applies to Unified Communications Manager, IM and Presence Service, and Cisco Unity Connection

set network dhcp eth0

This command enables or disables DHCP for Ethernet interface 0. You cannot configure Ethernet interface 1.

set network dhcp eth0 {enable | disable } {node_ipnet_maskgateway_ip }

| Syntax Description | Parameters | Description |
|--------------------|-------------------|---|
| | eth0 | Specifies Ethernet interface 0. |
| | enable | This enables DHCP. |
| | disable | This disables DHCP. |
| | node_ip | Represents the static IP address for the server. |
| | net_mask | Represents the subnet mask for the server. |
| | gateway_ip | Represents the IP address of the default gateway. |

Command Modes Administrator (admin:)

Usage Guidelines**Caution**

If you continue, this command causes the system to restart. Cisco also recommends that you restart all nodes whenever any IP address gets changed.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network dns

This command sets the IP address for the primary or secondary DNS server.

set network dns {primary | secondary} addr

| Syntax Description | Parameters | Description |
|--------------------|------------------|---|
| | primary | |
| | secondary | |
| | addr | Represents the IP address of the primary or secondary DNS server. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

**Note**

If you change the IP address for the DNS servers, you must reboot the server through the **utils system restart** CLI command.

set network dns options

This command sets DNS options.

set network domain

set network dns options [{timeoutseconds}] [{attemptsnumber}] [{rotate}]

Syntax Description**Parameters Description**

timeout Sets the DNS timeout.

attempts Sets the number of times to attempt a DNS request.

rotate Causes the system to rotate among the configured DNS servers and distribute the load.

seconds Specifies the DNS timeout period in seconds.

number Specifies the number of attempts.

Usage Guidelines

Running this command causes an automatic system restart.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network domain

This command sets the domain name for the system.

**Note**

Changing the domain name triggers an automatic regeneration of all Unified Communications Manager certificates, including any third party signed certificates that have been uploaded. After the server reboots automatically, phones running in secure (mixed) mode cannot connect to the server until after the CTL client updates the new CTL file to the phones.

**Note**

Reboot the servers one at a time in order for the phones to register correctly. For more information about changing the domain name, see *Changing the IP Address and Hostname for Cisco Unified Communications Manager*.

set network domain [domain-name]

Syntax Description**Parameters Description**

domain_name Represents the system domain that you want to assign.

| | |
|-------------------------|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The system asks whether you want to continue to execute this command. |

**Caution**

If you continue, this command causes a temporary loss of network connectivity.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network failover

This command enables and disables Network Fault Tolerance on the Media Convergence Server network interface card.

set network failover {ena | dis}

| | |
|---------------------------|--|
| Syntax Description | Parameters Description |
| | ena Enables Network Fault Tolerance. |
| | dis Disables Network Fault Tolerance. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network gateway

This command enables you to configure the IP address of the network gateway.

set network gateway addr

| | |
|---------------------------|---|
| Syntax Description | Parameters Description |
| | addr Represents the IP address of the network gateway that you want to assign. |

set network hostname

| | |
|-------------------------|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The system asks whether you want to continue to execute this command. |
| Caution | If you continue, this command causes the system to restart. |

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network hostname

This command allows an administrator to set the network host name, change the IP address of the node, and restart the system.

Before attempting this command, the administrator should have a valid DRF backup. Additionally, before attempting a Hostname (or Hostname and IP address) change, the administrator should perform the following:

- verify the cluster configuration does not have any configuration problems by executing **show hcs cluster verify detailed**
- update the cluster configuration by executing **set hcs cluster config**
- validate the cluster configuration by executing **show hcs cluster verify detailed**

set network hostname *hostname*

| Syntax Description | Parameters Description |
|---------------------------|---|
| | <i>hostname</i> Represents the new network hostname of the system. |
| | Note The host name must follow the rules for ARPANET host names. It must start with an alphabetic character, end with an alphanumeric character, and consist of alphanumeric characters and hyphens. The host name can have a maximum length of 63 characters. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The system asks whether you want to continue to execute this command. |
| Caution | If you continue, this command causes the system to restart. |

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set network hostname
```

```
WARNING: Changing this setting will invalidate software license  
on this server. The license will have to be re-hosted.  
Continue(y/n):  
Continue (y/n)?y
```

```
ctrl-c: To quit the input.
```

```
*** W A R N I N G ***  
Do not close this window without first canceling the command.
```

```
This command will automatically restart system services.  
The command should not be issued during normal operating  
hours.
```

```
=====  
Note: Please verify that the new hostname is a unique  
name across the cluster and, if DNS services are  
utilized, any DNS configuration is completed  
before proceeding.  
=====
```

```
Security Warning : This operation will regenerate  
all CUCM Certificates including any third party  
signed Certificates that have been uploaded.
```

```
Enter the hostname:: app-lfwelty5  
Would you like to change the network ip address at this time [yes]::
```

```
Warning: Do not close this window until command finishes.
```

```
ctrl-c: To quit the input.
```

```
*** W A R N I N G ***  
=====  
Note: Please verify that the new ip address is unique  
across the cluster.  
=====
```

```
Enter the ip address:: 106.1.34.154  
Enter the ip subnet mask:: 255.0.0.0  
Enter the ip address of the gateway:: 106.1.1.1  
Hostname: app-lfwelty5  
IP Address: 106.1.34.154
```

set network ip eth0

```
IP Subnet Mask: 255.0.0.0
Gateway: 106.1.1.1

Do you want to continue [yes/no]? yes
...
```



Note The administrator can change both the hostname and IP address by responding **yes**. To change just the hostname, respond **no**.

set network ip eth0

This command sets the IP address for Ethernet interface 0. You cannot configure Ethernet interface 1.

Before attempting this command, the administrator should have a valid DRF backup. Additionally, before attempting an IP address change, the administrator should perform the following:

- verify the cluster configuration does not have any configuration problems by executing **show hcs cluster verify detailed**
- update the cluster configuration by executing **set hcs cluster config**
- validate the cluster configuration by executing **show hcs cluster verify detailed**

set network ip eth0 *addr* *mask* *gw*

| Syntax Description | Parameters | Description |
|--------------------|-------------|---|
| | eth0 | Specifies Ethernet interface 0. |
| | addr | Represents the IP address that you want to assign. |
| | mask | Represents the IP mask that you want to assign. |
| | gw | Represents the IP default gw that you want to assign. |

Command Modes Administrator (admin:)

Usage Guidelines The system asks whether you want to continue to execute this command.



Caution If you continue, this command causes the system to restart.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network ipv6 dhcp

This command sets the DHCPv6 client on the server and enables IPv6 support. For changes to take effect, you must restart the server.

set network ipv6 dhcp {enable | disable} [reboot]

| Syntax Description | Parameters | Description |
|--------------------|----------------|---|
| | dhcp | Sets the DHCPv6 client on the server. By default, the server does not restart after you enable the DHCPv6 client. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| | enable | Enables IPv6 support. |
| | disable | Disables IPv6 support. |
| | reboot | (Optional) Causes the server to automatically restart after you enter the command. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection.

set network ipv6 gateway

This command sets the IPv6 gateway for the server. For changes to take effect, you must restart the server.

set network ipv6 gateway *addr* [reboot]

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | gateway | Sets the IPv6 gateway for the server. By default, the server does not restart after you set the IPv6 gateway for the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| | addr | The IPv6 gateway address. |
| | reboot | (Optional) Causes the server to automatically restart after you enter the command. |

Command Modes Administrator (admin:)

set network ipv6 service

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection.

set network ipv6 service

This command enables or disables the IPv6 service on the server. For changes to take effect, you must restart the server.

set network ipv6 service {enable | disable} [reboot]

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | service | Sets the IPv6 service on the server. By default, the server does not restart after you enable or disable the IPv6 service on the server. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |
| | enable | Enables IPv6 service on the server. |
| | disable | Disables IPv6 service on the server. |
| | reboot | (Optional) Causes the server to automatically restart after you enter the command. |

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection.

set network ipv6 static_address

This command assigns the static IPv6 address to the server. For changes to take effect, you must restart the server.

set network ipv6 static_address *addr* *mask* [reboot]

| Syntax Description | Parameters | Description |
|--------------------|-----------------------|--|
| | static_address | Assigns a static IPv6 address to the server. By default, the server does not restart after you assign the static IPv6 address. For your changes to take effect, you must restart the server by either entering the reboot parameter or manually restarting the server. |

| Parameters | Description |
|---------------|--|
| <i>addr</i> | Specifies the static IPv6 address you assign to the server. |
| <i>mask</i> | Specifies the IPv6 network mask (0-128). |
| reboot | (Optional) Causes the server to automatically restart after you enter the command. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection.

set network max_ip_conntrack

This command sets the ip_conntrack_max value.

set network max_ip_conntrack *ip_conntrack_max value*

| Syntax Description | Parameters | Description |
|--------------------|-------------------------------|---|
| | <i>ip_conntrack_max value</i> | Specifies the value for ip_conntrack_max. Note The value of ip_conntrack_max cannot be less than 65536. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set network max_ip_conntrack 65536
```

set network mtu

This command sets the maximum MTU value.

set network name-service hosts cache-enable

set network mtu *mtu_max*

Syntax Description

Parameters Description

mtu_max Specifies the maximum MTU value. The system default MTU value equals 1500.

Caution When packets on UDP port 8500 that have the DF bit set are exchanged between nodes, if there is any policy on the WAN router to clear the DF bit and fragment large packets, this may cause dbreplication issues.

Command Modes

Administrator (admin:)

Usage Guidelines

The system asks whether you want to continue to execute this command.



Caution

If you continue, the system loses network connectivity temporarily.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set network mtu 576      W A R N I N G
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

set network name-service hosts cache-enable

This command enables the nsqd related cache.

set network name-service hosts cache-enable *value*

Syntax Description

Parameters Description

value The boolean value must be either *yes* or *no*.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service hosts max-db-size

This command sets the maximum allowed size for a service.

set network name-service hosts max-db-size *value*

| Syntax Description | Parameters Description |
|----------------------|--|
| | <p><i>value</i> Enter the number of bytes for the database size.</p> |
| Command Modes | Administrator (admin:) |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service hosts negative-time-to-live

This command sets the time-to-live (TTL) for negative entries or unsuccessful queries in the specified cache for service. So, using this command improves the performance if there are various files owned by user IDs (UIDs) and are unavailable in system databases. For example, files that are available in the Linux kernel sources as root. To reduce the cache coherency problems, the number of such files should be kept to the minimum.

set network name-service hosts negative-time-to-live *value*

| Syntax Description | Parameters Description |
|----------------------|--|
| | <p><i>value</i> Enter the number of seconds.</p> |
| Command Modes | Administrator (admin:) |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service hosts persistent

set network name-service hosts persistent

This command retains the content of the cache for service over server restarts. This command is useful when *paranoia* mode is configured.

set network name-service hosts persistent *value*

| Syntax Description | Parameters | Description |
|--------------------|--------------|------------------------------|
| | <i>value</i> | Enter a value for a service. |

| Command Modes | Administrator (admin:) |
|---------------|------------------------|
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service hosts positive-time-to-live

This command sets the time-to-live (TTL) for positive entries or successful queries in the specified cache for service. Configure the value in seconds. Larger values increase cache hit rates and reduce mean response times. However, such values increase problems with cache coherence.

set network name-service hosts positive-time-to-live *value*

| Syntax Description | Parameters | Description |
|--------------------|--------------|------------------------------|
| | <i>value</i> | Enter the number of seconds. |

| Command Modes | Administrator (admin:) |
|---------------|------------------------|
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service hosts suggested-size

This command changes the internal hash table size.

set network name-service hosts suggested-size *value*

Syntax Description**Parameters Description**

value Enter a prime number for optimum efficiency.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service services cache-enable

This command enables the nscd related cache.

set network name-service services cache-enable *value*

Syntax Description**Parameters Description**

value The boolean value must be either *yes* or *no*.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service services max-db-size

This command sets the maximum allowed size for the service.

set network name-service services max-db-size *value*

Syntax Description**Parameters Description**

value Enter the value in number of bytes.

Command Modes

Administrator (admin:)

■ **set network name-service services negative-time-to-live**

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service services negative-time-to-live

This command sets the time-to-live (TTL) for negative entries or unsuccessful queries in the specified cache for service. So, using this command improves the performance if there are various files owned by user IDs (UIDs) and are unavailable in system databases. For example, files that are available in the Linux kernel sources as root. To reduce the cache coherency problems, the number of such files should be kept to the minimum.

set network name-service services negative-time-to-live *value*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>value</i> Enter a prime number for optimum efficiency. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service services persistent

This command retains the content of the cache for service over server restarts. This command is useful when *paranoia* mode is configured.

set network name-service services persistent *value*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>value</i> Enter a value for a service. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service services positive-time-to-live

This command sets the time-to-live (TTL) for positive entries or successful queries in the specified cache for service. If you enter a large value for this command, it increases cache hit rates and reduces mean response times. However, a large value increases issues with cache coherence.

set network name-service services positive-time-to-live *value*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>value</i> Enter the number of seconds. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service services suggested-size

This command sets the internal hash table size.

set network name-service services suggested-size *value*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>value</i> Enter a prime number for optimum efficiency. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network nic eth0

set network nic eth0

This command sets the properties of the Ethernet Interface 0. You cannot configure Ethernet interface 1.

set network nic eth0 {auto | {en | dis}} {speed | {10 | 100}} {duplex half | {half | full}}

| Syntax Description | Parameters | Description |
|--------------------|---------------|---|
| | eth0 | Specifies Ethernet interface 0. |
| | auto | Specifies whether auto negotiation gets enabled or disabled. |
| | speed | Specifies whether the speed of the Ethernet connection: 10 or 100 Mb/s. |
| | duplex | Specifies half-duplex or full-duplex. |

Command Modes Administrator (admin:)

Usage Guidelines The system asks whether you want to continue to execute this command.



Note

You can enable only one active NIC at a time.



Caution

If you continue, this command causes a temporary loss of network connections while the NIC gets reset.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network ntp option

This command adds the *noquery* option to the */etc/config* file.

set network ntp option

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network pmtud state

This command enables and disables Path MTU Discovery.

set network pmtud state {enable | disable}

Syntax Description**Parameters Description**

enable Enables Path MTU Discovery.

disable Disables Path MTU Discovery.

Command Modes

Administrator (admin:)

Usage Guidelines

The system asks whether you want to continue to execute this command.

**Caution**

If you continue, the system loses network connectivity temporarily.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set network pmtud state enable      W A R N I N G
This will cause the system to temporarily lose network connectivity
Do you want to continue ?
Enter "yes" to continue or any other key to abort
yes
executing...
```

set network restore

This command configures the specified Ethernet port to use a specified static IP address.

set network restore

set network restore *eth0* *ip-address* *network-mask* *gateway*

Syntax Description

| Parameters | Description |
|---------------------|--|
| <i>eth0</i> | Specifies Ethernet interface 0. |
| <i>ip-address</i> | Represents the IP address of the primary or secondary DNS server, or the network gateway that you want to assign. If you continue, this command causes a temporary loss of network connectivity. If you change the IP address for the primary DNS server, you must also restart the Cisco Tomcat service. For more information, see the utils service command. We also recommend that you restart all nodes whenever any IP address gets changed. |
| <i>network-mask</i> | Represents the subnet mask for the server. |
| <i>gateway</i> | Specifies the IP address of the default gateway. |
| <i>ip-address</i> | Represents the IP address of the primary or secondary DNS server, or the network gateway that you want to assign. If you continue, this command causes a temporary loss of network connectivity. If you change the IP address for the primary DNS server, you must also restart the Cisco Tomcat service. For more information, see the utils service command. We also recommend that you restart all nodes whenever any IP address gets changed. |

Command Modes

Administrator (admin:)

Usage Guidelines**Caution**

Only use this command option if you cannot restore network connectivity through any other set network commands. This command deletes all previous network settings for the specified network interface, including Network Fault Tolerance. After you run this command, you must restore your previous network configuration manually.

**Caution**

The server temporarily loses network connectivity after you run this command.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set network restore eth0 10.94.150.108 255.255.255.0 10.94.150.1
```

set network status eth0

This command sets the status of Ethernet 0 to up or down. You cannot configure Ethernet interface 1.

set network status eth0 {up | down}

Syntax Description

| Parameters | Description |
|-------------|--|
| eth0 | Specifies Ethernet interface 0. |
| up | Sets the status of Ethernet interface 0 to up. |
| down | Sets the status of Ethernet interface 0 to down. |

Command Modes

Administrator (admin:)

Usage Guidelines

The system asks whether you want to continue to execute this command.



Caution

If you continue, the system loses network connectivity temporarily.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set network name-service

This command displays name service cache attributes.

set network name-service [attribute] [value]

Syntax Description

| Attribute | Value |
|---------------------|---|
| Paranoia | Bool must be either Yes or No. Enabling paranoia mode causes Name Service to restart itself periodically. |
| debug-level | If level is higher than 0, Name Service will create some debug output. Higher the level, more verbose the output. |
| reload-count | Sets the number of times a cached record is reloaded before it is pruned from the cache. Each cache record has a timeout. When that timeout expires Name Service will either reload it (query the NSS service again if the data hasn't changed) or drop it. |

set password complexity minimum-length

| Attribute | Value |
|-------------------------|--|
| restart-interval | Sets the restart interval to time seconds if periodic restart is enabled by enabling paranoia mode. The default value is 3600. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

set password complexity minimum-length

This command modifies the value of minimum password length for the OS administration accounts.



Note

Use this command after you enable the character complexity of passwords.

set password complexity minimum-length *max-repeat*

Syntax Description

Parameters Description

value Enter a value of or greater than 6.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password age

This command modifies the value for password age, in days, for Cisco Collaboration Communication OS (C3OS) accounts.

set password age {maximum | minimum} *days*

Syntax Description

Parameters

Description

maximum Specifies the maximum age.

minimum Specifies the minimum age.

| Parameters | Description |
|-------------|--|
| <i>days</i> | Specifies the maximum password age and must be greater-than or equal-to 90 days. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password change-at-login

Use this command to force new or existing users to change their password when they sign in to the system the next time.

set password change-at-login {disable | enable} *userid*

Syntax Description

| Parameters | Description |
|----------------|---|
| disable | This does not force users to change their password. |
| enable | This forces users to change their password when they sign in to the system the next time. |
| <i>userid</i> | Specifies the affected user account. |

Command Modes Administrator (admin:)

Usage Guidelines By default, this command is enabled for new users, so users have to change their password the first time they sign in to the system.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager only.

set password complexity character

Use this command to enable or disable password complexity rules for the type of characters in a password.

set password complexity character



Note After you enable password complexity, this command also enables password history if it has not already been enabled (for more information, see the **set password history** command). If you had not previously enabled password history, the password history number parameter value gets set to 10. If you previously enabled password history with a value of less than 10, the value gets reset to 10 after you execute this command. If you previously enabled password history with a value of 10 or greater, the value remains unchanged after you execute this command.

set password complexity character {disable | enable} num-char

Syntax Description

Parameters Description

disable This turns off password complexity for character types.

enable This turns on password complexity for character types.

Note When you disable password complexity, you also turn off **password character difference**, **password character max-repeat**, and **password history**.

num-char This specifies the number of characters required from each of the four character sets: lowercase, uppercase, numbers, and special characters.

- Value range: 0-8
- Default value: 1

Command Modes

Administrator (admin:)

Usage Guidelines

When you enable password complexity, you must follow these guidelines when you assign a password:

- It must have at least the current setting, num-chars, of lower-case character.
- It must have at least the current setting, num-chars, of uppercase characters.
- It must have at least the current setting, num-chars, of digit characters.
- It must have at least the current setting, num-chars, of special characters.
- You cannot use adjacent characters on the keyboard; for example, qwerty.
- You cannot reuse any of the previous passwords that match the passwords retained by password history.
- By default, the admin user password can be changed only once in a 24-hour day.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password complexity character difference

This command specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password.

set password complexity character difference *num-char*

Syntax Description

Parameters Description

num-char This specifies the number of characters that the character sequence in a new password must differ from the character sequence in the old password.

- Value range: 0-31

Command Modes

Administrator (admin:)

Usage Guidelines

Enter 0 to indicate no difference.



Note

The maximum password length is 31 characters.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password complexity character max-repeat

This command specifies the number of times you can consecutively repeat a single character in a new password.

set password complexity character max-repeat *max-repeat*

Syntax Description

Parameters Description

max-repeat This specifies the number of times you can consecutively repeat a single character in a new password.

- Value range: 0 – 10

Default value: 0

Command Modes

Administrator (admin:)

set password expiry maximum-age

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password expiry maximum-age

This command enables or disables the password expiry maximum age settings for Cisco Collaboration Communication OS (C3OS) Administrator accounts.

set password expiry maximum-age {enable | disable}

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | enable | Turns on password expiry maximum age settings for Cisco Unified Operating System administrator accounts. The set password expiry enable command sets the value of maximum password age to 3650 days (10 yrs) for Cisco Unified Operating System Administrator accounts. |
| | disable | Turns off password expiry maximum age settings for Cisco Unified Operating System administrator accounts. The set password expiry disable command results in Cisco Unified Operating System Administrator accounts never expiring. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set password expiry maximum-age disable
Operation Successful.
```

set password expiry user maximum-age configure

This command modifies the value of the maximum password age for a particular Cisco Collaboration Communication OS Administration account in days.

set password expiry user maximum-age configure *userid* *maximum password age*

| Syntax Description | Parameters | Description |
|--------------------|-----------------------------|---|
| | <i>userid</i> | Enter Cisco Collaboration Communication OS (C3OS) Administrator account. |
| | <i>maximum password age</i> | Enter the maximum password age in days. This value must be equal to or greater than 10 days but less than 3650 days (10 years). |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password expiry minimum-age

This command enables or disables the password expiry minimum age settings for Cisco Unified Operating System Administrator accounts.

set password expiry minimum-age {enable | disable}

| Syntax Description | Parameters | Description |
|--------------------|---------------|--|
| | <i>enable</i> | Turns on password expiry minimum age settings for Cisco Unified Operating System administrator accounts. The set password expiry enable command sets the value of minimum password age to one day (24 hrs) for Cisco Collaboration Communication OS (C3OS) Administrator accounts. |

set password expiry user maximum-age

| Parameters | Description |
|----------------|---|
| disable | Turns off password expiry minimum age settings for Cisco Collaboration Communication OS (C3OS) administrator accounts. This means that passwords for administrator accounts can be changed at any interval. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set password expiry minimum-age disable
Operation Successful.
```

set password expiry user maximum-age

This command disables the maximum age password expiry for a particular Cisco Unified Operating System Administrator account.

set password expiry user maximum-age {enable | disable}userid

Syntax Description

| Parameters | Description |
|----------------|--|
| enable | Turns on the maximum age password expiry settings for a particular Cisco Collaboration Communication OS (C3OS) administrator account. The set password expiry user enable command sets the value of maximum password age to 3650 days (10 yrs) for the Cisco Unified Operating System Administrator account. |
| disable | Turns on the maximum age password expiry settings for a particular Cisco Collaboration Communication OS (C3OS) administrator account. The set password expiry user enable command sets the value of maximum password age to 3650 days (10 yrs) for the Cisco Unified Operating System Administrator account. |
| userid | Specifies a particular Cisco Collaboration Communication OS (C3OS) Administrator account. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set password expiry user maximum-age enable
Operation Successful.
```

set password expiry user minimum-age

This command enables or disables the maximum age password expiry for a particular Cisco Unified Operating System Administrator account.

set password expiry user minimum-age {enable | disable} *userid*

| Syntax Description | Parameters | Description |
|--------------------|----------------|---|
| | enable | Turns on the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account. |
| | disable | Turns off the minimum age password expiry settings for a particular Cisco Unified Operating System administrator account. |
| | <i>userid</i> | Specifies a particular Cisco Unified Operating System Administrator account. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:set password expiry user minimum-age disable
Operation Successful.
```

set password history

set password history

This command modifies the number of passwords that get maintained in the history for OS admin accounts. New passwords matching remembered passwords get rejected.

set password history *number*

| Syntax Description | Parameters Description |
|-------------------------|--|
| | <i>number</i> Specifies the mandatory number of passwords to maintain in history. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | <ul style="list-style-type: none"> • To disable, enter 0. • Default specifies 10. • Upper limit specifies 20. |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password inactivity

set password inactivity {enable | disable | period} *days*

| Syntax Description | Parameters Description |
|-------------------------|---|
| | <i>enable</i> Enable the password inactivity globally and update individual OS users according to the setting. |
| | <i>disable</i> Disable the password inactivity globally and update individual OS users according to the setting. |
| | <i>period</i> Configure the password inactivity period globally and update individual OS users according to the setting. |
| | <i>days</i> Specify the number of days of inactivity after a password has expired before the account gets disabled. Valid range is 1 - 99. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | <ul style="list-style-type: none"> • To enable password inactivity globally, execute the set password inactivity enable command. This command enables the password inactivity globally and updates individual OS users according to the setting. |

- To disable password inactivity globally, execute the set password inactivity disable command. This command disables the password inactivity globally and updates individual OS users according to the setting.

A user whose account is disabled must contact the system administrator to use the system again.

- To configure the password inactivity period execute the set password inactivity period days command. This command configures the password inactivity globally and updates individual OS users according to the setting.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password system bootloader encryptHash

Use this command to configure the encrypted password in the grub.conf file for the system boot loader.

set password system bootloader encryptHash

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password user admin

This command allows you to change the administrator password.

set password user admin

Command Modes Administrator (admin:)

Usage Guidelines The system prompts you for the old and new passwords.



Note

- You can change the password only for the administrator account that you logged in to.
- The password must contain at least six characters, and the system checks it for strength.

set password user security**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set password user security

This command allows you to change the security password.

set password user security

Command Modes

Administrator (admin):

Usage Guidelines

The systems prompts you for the old and new passwords.



Note The password must contain at least six characters, and the system checks it for strength.

Servers in a cluster use the security password to authenticate communication between servers. You must reset the cluster after you change the security password.

1. Change the security password on the publisher server (first node) and then reboot the server (node).
2. Change the security password on all the subsequent servers and nodes to the same password that you created on the first node and restart subsequent nodes, including application servers, to propagate the password change.



Note Cisco recommends that you restart each server after the password is changed on that server.



Note Failure to reboot the servers (nodes) causes system service problems and problems with the Cisco Collaboration Communication OS (C3OS) Administration windows on the subscriber servers.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Set replication-sync monitor

This command enables or disables replication monitoring by the Cisco Replication Watcher service. The Cisco Replication Watcher service blocks other services from starting until database replication is setup and functioning normally.

set replication-sync monitor {enable | disable}

Syntax Description

Parameters Description

enable Turns on the replication monitoring service.

disable Turns off the replication monitoring service

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager only

set samltrace level

This command sets the SAML trace level.

set samltrace level *trace level*

Syntax Description

Parameters Description

trace level Specifies the trace level. The available options are:

- DEBUG
- INFO
- WARNING
- ERROR
- FATAL

Note The default trace level is INFO.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

set session maxlimit

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set session maxlimit

This command sets the upper limit for concurrent sessions.

set session maxlimit [value]

| Syntax Description | Parameters Description |
|----------------------|---|
| | maxlimit This command sets the upper limit for concurrent sessions. Acceptable values are 1 - 100. If no upper limit is entered, the default value of 10 is assigned to sshd_config param. |
| | value Acceptable values are 1 - 100. |
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 1 |
| | Allowed during upgrade: Yes |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection. |

set smtp

This command sets the SMTP server hostname.

set smtp hostname

| Syntax Description | Parameters Description |
|----------------------|--|
| | hostname Represents the SMTP server name. |
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 0 |
| | Allowed during upgrade: No |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection. |

set strace enable

This command enables the service trace and sets the trace level.

set strace enable [all]tracevalue servicename

Syntax Description

Parameters Description

all Optional parameter to propagate the service trace settings change to all nodes.

tracevalue Represents allowed trace values. Allowed trace values are [Info|Debug|Warn|Error|Fatal]

servicename Represents the service for which the trace is enabled.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

set strace disable

This command disables the service trace.

set strace disable [all] servicename

Syntax Description

Parameters Description

all Optional parameter to propagate the service trace settings change to all nodes.

servicename Represents the service for which the trace is enabled.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

set timezone

This command lets you change the system timezone.

set tls min-version**set timezone zone****Syntax Description****Parameters Description**

zone Specifies the new timezone. Enter the appropriate string or zone index id to uniquely identify the timezone. To view a list of valid timezones, use the CLI command: **show timezone list**.

Command Modes

Administrator (admin:)

Usage Guidelines

Enter characters to uniquely identify the new timezone. Be aware that the timezone name is case-sensitive.

**Note**

Changing the system time zone to US time zone may require system compliance to FCC Call Routing Regulations in US. Unified Communications Manager Administrator must refer the Emergency Call Routing Regulations page and complete necessary configuration.

**Caution**

You must restart the system after you change the timezone.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example Setting Timezone to Pacific Time

admin:set timezone Pac

set tls min-version

This command sets the minimum version of Transport Layer Security (TLS) protocol.

**Note**

- After you set the minimum TLS version, the system reboots.
- Configure the minimum TLS version for each node.

set tls min-version *tls minVersion*

| Syntax Description | Parameters | Description |
|--------------------|---|--|
| | <i>tls minVersion</i> | Type one of the following options to set it as the minimum TLS version: <ul style="list-style-type: none"> • 1.0 • 1.1 • 1.2 |
| Command Modes | Administrator (admin:) | |
| Usage Guidelines | Requirements Command privilege level: 1 Allowed during upgrade: Yes Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager | |
| | Example <pre>admin: set tls min-version 1.1 This command will result in setting minimum TLS version to 1.1 on all the secure interfaces. If you have custom applications that makes secure connection to the system, please ensure they support the TLS version you have chosen to configure. Also, please refer to the Cisco Unified Reporting Administration Guide to ensure the endpoints in your deployment supports this feature. ***** Warning: This will set the minimum TLS to 1.1 and the server will reboot. ***** Do you want to continue (yes/no) ? yes Successfully set minimum TLS version to 1.1 The system will reboot in few minutes.</pre> | |

set trace disable

This command unsets trace activity for the specified task.

set trace disable *tname*

| Syntax Description | Parameters | Description |
|--------------------|---------------------|---|
| | disable | Unsets the task trace settings. |
| | <i>tname</i> | Represents the task for which you want to disable traces. |

set trace enable**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set trace enable

This command sets trace activity for the specified task.

```
set trace enable {Arbitrary | Detailed | Entry_exit | Error | Significant | Special | State_Transition}  
tname
```

Command Modes

| Parameters | Description |
|-------------------------|---|
| Arbitrary | Sets task trace settings to the arbitrary level. |
| Detailed | Sets task trace settings to the detailed level. |
| Entry_exit | Sets task trace settings to the entry_exit level. |
| Error | Sets task trace settings to the error level. |
| Significant | Sets task trace settings to the significant level. |
| Special | Sets task trace settings to the special level. |
| State_transition | Sets task trace settings to the state transition level. |
| <i>tname</i> | Represents the task for which you want to disable traces. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set tlsresumptiontimeout

This command sets the number of seconds after which TLS resumption will not work and sessions are invalidated.

set tlstrace*

Syntax Description

Parameters Description

seconds Enter a value up to 3600 seconds. The TLS sessions are invalid after the configured value.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set tlstrace*

Unified Communications Manager Release 11.0 onwards, you can enable or disable TLS tracing for services. Currently, Tomcat is the only supported service. Use the CLI commands to view the reasons of connection failure of TLS connections to Unified Communications Manager.

Following TLS-based CLI commands are added for TLS tracing:

set tlstrace disable

This CLI command disables the TLS tracing for a service.

set tlstrace disable *service*

Syntax Description

Parameters Description

service Specifies the service that you use to disable TLS tracing.

Command Modes

Administrator (admin:)

Example

```
admin:>set tlstrace disable tomcat
TLS tracing is disabled for: tomcat
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set tlstrace enable

set tlstrace enable

This CLI command enables the TLS tracing for a service.

set tlstrace enable *service*

Syntax Description

Parameters Description

service Specifies the service that you use to enable TLS tracing.

Command Modes

Administrator (admin:)

Example

```
admin:set tlstrace enable tomcat
TLS tracing is enabled for: tomcat
```

Requirements

Command privilege level: 1

Allowed during upgrade: No

set web-security

This command sets the web security certificate information for the operating system.

set web-security *orgunit orgname locality state [country] [alternatehostname]*

Syntax Description

Parameters

Description

orgunit Represents the organizational unit (OU) name.

You can use this command to enter multiple organizational units. To enter more than one organizational unit name, separate the entries with a comma. For entries that already contain a comma, enter a backslash before the comma that is included as part of the entry. To enter multiple values for organizational unit, enclose them in quotation marks, as shown in the example for this command.

Note For OU's that already contains a backslash, do not enter one more backslash as SLM registration and CSR generation fails during the time of installation.

orgname Represents the organizational name.

locality Represents the organization location.

state Represents the organization state.

country (Optional) Represents the organization country.

| Parameters | Description |
|--------------------------|--|
| <i>alternatehostname</i> | (Optional) Specifies an alternate name for the host when you generate a web-server (Tomcat) certificate. You can use alternatehostname to set subject alternate hostname for self signed certificates. Subject alternate hostname for CSR is defined in the Certificate Management page. If you have set the alternate hostname for CSR using this command, the CSR generation process replaces the set alternate hostname. |

**Note**

The set web-security command when adding in the alternate hostname will apply and will be added to all future generated CSR's including, Tomcat, CallManager, CAPF, TVS, and IPsec.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

This example shows the web-security command with multiple organizational unit names using comma separators. The certificate has three OU fields:

- OU=accounting
- OU=personnel, CA
- OU=personnel, MA

```
admin:set web-security "accounting,personnel\,CA,personnel\,MA" Cisco Milpitas
CA
set web-security "Voice\Video" "Cisco" "RTP" NC
```

set webapp session timeout

This command sets the time, in minutes, that can elapse before a web application, such as Unified Communications Manager Administration, times out and logs off the user.

For the new webapp session timeout setting to become effective, you must restart the Cisco Tomcat service. Until you restart the Cisco Tomcat service, the **show webapp session timeout** command reflects the new values, but system continues to use and reflect the old values. This command prompts you to restart the service.

set webapp session maxlimit



Caution

Restarting the Cisco Tomcat service ends all active sessions and can affect system performance. Cisco recommends that you only execute this command during off-peak traffic hours.



Note

This setting gets preserved through a software upgrade and does not get reset to the default value.

set webapp session timeout *minutes*

Syntax Description

Parameters Description

minutes Specifies the time, in minutes, that can elapse before a web application times out and logs off the user.

- Value range: 5-99999 minutes
- Default value: 30 minutes

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set webapp session maxlimit

This command sets the maximum limit for concurrent web application sessions per user. This applies to the following interfaces:

- Cisco Unified CM Administration
- Cisco Unified Serviceability
- Cisco Unified Reporting
- Cisco Unified Communications Self Care Portal
- Cisco Unified CM IM and Presence Administration
- Cisco Unified IM and Presence Serviceability
- Cisco Unified IM and Presence Reporting

For the session maximum limit setting to become effective, the administrator must restart the Cisco Tomcat service.

**Caution**

Restarting the Cisco Tomcat service ends all active sessions and can affect the system performance. Cisco recommends that you only execute this command during off-peak traffic hours.

**Note**

This setting gets preserved through a software upgrade and does not get reset to the default value.

set webapp session maxlimit *number*

Syntax Description**Parameters Description**

number Specifies the number to limit the concurrent web application sessions.

The value ranges from 1 to 10.

Default value is 10.

If the **utils EnhancedSecurityMode** is enabled, then the session limit is restricted to 3. For more details on how to Configure Enhanced Security Mode, see the “FIPS 140-2 Mode Setup” chapter in the *Security Guide for Cisco Unified Communications Manager, Release 11.5(1)SU1* at <https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html>.

Note

- When you exceed the defined sign-in sessions maximum limit, then the interface sign-in page displays the Logon Status message as: The Session limit has already been reached for <username>. Please logout from those sessions or wait 30 minutes for inactive sessions to be automatically closed.
- When Enhanced Security Mode is enabled, then the session limit is restricted to 3. However, Administrator can change the session limit using the **set webapp session maxlimit** command to any value ranging from 1 to 10.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, Unified Communications Manager IM and Presence Service and Cisco Unity Connection.

Example

This example details on how to **set webapp session maxlimit** to 4:

```
admin:set webapp session maxlimit 4
```

```
*****W A R N I N G*****  
The Cisco Tomcat service needs to be restarted for the changes to take effect. This will
```

set webapp session maxlimit

disconnect active web sessions and all web applications on this node will be unavailable until the service restarts. This service restart will take several minutes to complete. Do you want to continue (yes/no) ? yes

```
*****Restarting Tomcat*****
Service Manager is running
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STOPPING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTING]
Cisco Tomcat[STARTED]
The webapp session limit has been successfully set to 4.
```

This example details on how to enable **utils EnhancedSecurityMode**:

```
admin:utils EnhancedSecurityMode enable
```

The system is operating in NON-FIPS and NOT operating in Enhanced Security Mode.

Enhanced Security Mode can be enabled only when the system is operating in FIPS mode
Do you wish to enable FIPS mode as well (yes/no) ? yes

Warning : This operation will modify the password policies

- 1) Password Length should be between 14 to 127 characters.
- 2) Password should have at least 1 lowercase, 1 uppercase, 1 digit and 1 special character.
- 3) Any of the previous 24 passwords cannot be reused.
- 4) Minimum age of the password is 1 day and Maximum age of the password is 60 days.
- 5) Any newly generated password's character sequence will need to differ by at least 4 characters from the old password's character sequence.

Warning : This mode will limit the total number of concurrent web application sessions to 3.

```
*****
This will change the system to Enhanced Security Mode and will reboot
*****
```

Do you want to continue (yes/no) ? yes
The protocol for communication with remote syslog server is already set to tcp. No changes required.

The system is already operating in contact search authentication enable mode; no change required. Exiting.

The concurrent web application session limit has been successfully set to 3.

Setting password restrictions as part of Enhanced Security Mode enable

Calling fips enable

Security Warning : The operation will regenerate certificates for

- 1) CallManager
- 2) Tomcat
- 3) IPsec
- 4) TVS
- 5) CAPF
- 6) SSH
- 7) ITLRecovery

Any third party CA signed certificates that have been uploaded for the above components will need to be re-uploaded.

If the system is operating in mixed mode, then the CTL client needs to be run again to update the CTL file.

If there are other servers in the cluster, please wait and do not change the FIPS settings on any other node until the FIPS operation on this node is complete and the system is back up and running.

This will change the system to FIPS mode and will reboot.

set workingdir

This command sets the working directory for active, inactive, and installation logs.

set workingdir {activelog | inactivelog | tftp} *directory*

Syntax Description

Parameters Description

activelog Sets the working directory for active logs. Choose a valid sub-directory of activelog.

inactivelog Set the working directory for inactive logs. Choose a valid sub-directory of inactivelog.

tftp Sets the working directory for TFTP files.

directory Represents the current working directory.

Command Modes

Administrator (admin:)

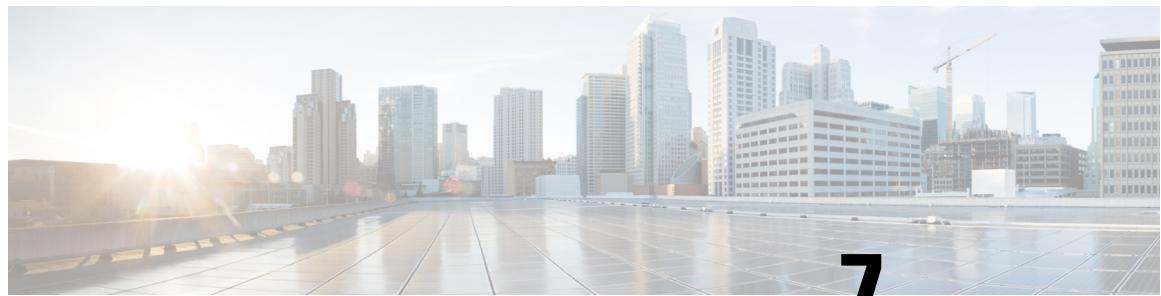
Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

set workingdir



CHAPTER 7

Show Commands

- [show account](#), on page 131
- [show accountlocking](#), on page 131
- [show cert default-ca-list](#), on page 132
- [show cert list](#), on page 133
- [show cert list type](#), on page 134
- [show cert own](#), on page 134
- [show cert trust](#), on page 135
- [show cli pagination](#), on page 135
- [show cli session timeout](#), on page 136
- [show csr list](#), on page 136
- [show csr list type](#), on page 137
- [show csr own](#), on page 137
- [show csr own name](#), on page 138
- [show ctl](#), on page 139
- [show cuc cluster status](#), on page 139
- [show cuc config groups](#), on page 139
- [show cuc config settings](#), on page 140
- [show cuc dbconsistency](#), on page 141
- [show cuc dbcontents](#), on page 142
- [show cuc dbschema](#), on page 143
- [show cuc dbserver disk](#), on page 144
- [show cuc dbserver session](#), on page 144
- [show cuc dbserver sessions all](#), on page 145
- [show cuc dbserver sessions list](#), on page 145
- [show cuc dbserver user list](#), on page 146
- [show cuc dbserver user waiting](#), on page 146
- [show cuc dbtable contents](#), on page 146
- [show cuc dbtable list](#), on page 147
- [show cuc dbtable schema](#), on page 148
- [show cuc dbview contents](#), on page 150
- [show cuc dbview list](#), on page 151
- [show cuc dbview schema](#), on page 152
- [**show cuc jetty ssl status**](#) , on page 153

- [show cuc locales](#), on page 153
- [show cuc speechview registration certificate size](#), on page 154
- [show cuc sysagent task list](#), on page 154
- [show cuc sysagent task results](#), on page 155
- [show cuc sysinfo](#), on page 156
- [show cuc tech dbschemaversion](#), on page 157
- [show cuc tech dbserver all](#), on page 158
- [show cuc tech dbserver integrity](#), on page 158
- [show cuc tech dbserver log diagnostic](#), on page 159
- [show cuc tech dbserver log message](#), on page 159
- [show cuc tech dbserver status](#), on page 160
- [show cuc trace levels](#), on page 160
- [show cuc version](#), on page 161
- [show date](#), on page 162
- [show diskusage](#) , on page 162
- [show dscp all](#), on page 163
- [show dscp defaults](#), on page 163
- [show dscp marking](#), on page 163
- [show dscp status](#), on page 164
- [show environment fans](#), on page 165
- [show environment power-supply](#), on page 165
- [show environment temperatures](#), on page 165
- [show fileserver transferspeed](#), on page 166
- [show haproxy client-auth](#), on page 166
- [show haproxy num-threads](#), on page 167
- [show hardware](#), on page 168
- [show ipsec information](#), on page 168
- [show ipsec policy_group](#), on page 169
- [show ipsec policy_name](#), on page 170
- [show ipsec status](#), on page 170
- [show itl](#), on page 170
- [show logins](#), on page 171
- [show key authz encryption](#), on page 172
- [show key authz signing](#), on page 172
- [show license all](#), on page 173
- [show license status](#), on page 173
- [show license summary](#), on page 173
- [show license tech support](#), on page 174
- [show license trace](#), on page 174
- [show license UDI](#), on page 174
- [show license usage](#), on page 175
- [show Login Grace Timeout](#), on page 175
- [show media streams](#), on page 175
- [show memory](#), on page 177
- [show myself](#), on page 177
- [show network all](#), on page 178

- [show network cluster, on page 178](#)
- [show network dhcp eth0, on page 178](#)
- [show network eth0, on page 179](#)
- [show network failover, on page 179](#)
- [show network ip_conntrack, on page 180](#)
- [show network ipprefs, on page 180](#)
- [show network ipv6, on page 181](#)
- [show network max_ip_conntrack, on page 181](#)
- [show network ntp option, on page 182](#)
- [show network route, on page 182](#)
- [show network status, on page 182](#)
- [show network name-service attributes, on page 183](#)
- [show network name-service cache-stats, on page 184](#)
- [show network name-service {hosts|services} attributes, on page 184](#)
- [show open files all, on page 185](#)
- [show open files process, on page 185](#)
- [show open files regexp, on page 186](#)
- [show open ports all, on page 186](#)
- [show open ports process, on page 186](#)
- [show open ports regexp, on page 187](#)
- [show packages, on page 187](#)
- [show password, on page 188](#)
- [show password complexity character, on page 189](#)
- [show password complexity length, on page 189](#)
- [show password expiry, on page 189](#)
- [show password expiry user, on page 190](#)
- [show password expiry user list, on page 190](#)
- [show perf counterhelp, on page 191](#)
- [show perf list categories, on page 191](#)
- [show perf list classes, on page 192](#)
- [show perf list counters, on page 192](#)
- [show perf list instances, on page 193](#)
- [show perf query class, on page 193](#)
- [show perf query counter, on page 194](#)
- [show perf query instance, on page 194](#)
- [show perf query path, on page 195](#)
- [show process list, on page 195](#)
- [show process load, on page 196](#)
- [show process name, on page 197](#)
- [show process name process-name , on page 197](#)
- [show process open, on page 198](#)
- [show process open-fd, on page 198](#)
- [show process pid, on page 199](#)
- [show process search, on page 199](#)
- [show process user, on page 200](#)
- [show process using-most cpu, on page 200](#)

- [show process using-most memory, on page 201](#)
- [show registry, on page 201](#)
- [show risdb list, on page 202](#)
- [show risdb query, on page 203](#)
- [show samltrace level, on page 203](#)
- [show session maxlimit, on page 204](#)
- [show smtp, on page 204](#)
- [show stats io, on page 204](#)
- [show status, on page 205](#)
- [show tech activesql, on page 206](#)
- [show tech all, on page 206](#)
- [show tech ccm_service, on page 206](#)
- [show tech database, on page 207](#)
- [show tech dberrcode, on page 207](#)
- [show tech dbhighcputasks, on page 208](#)
- [show tech dbintegrity, on page 208](#)
- [show tech dbschema, on page 208](#)
- [show tech dbinuse, on page 209](#)
- [show tech dbstateinfo, on page 209](#)
- [show tech devdefaults, on page 210](#)
- [show tech dumpCSVandXML, on page 210](#)
- [show tech gateway, on page 210](#)
- [show tech locales, on page 211](#)
- [show tech network all, on page 211](#)
- [show tech network hosts, on page 212](#)
- [show tech network interfaces, on page 212](#)
- [show tech network resolv, on page 213](#)
- [show tech network routes, on page 213](#)
- [show tech network sockets, on page 214](#)
- [show tech notify, on page 214](#)
- [show tech params, on page 215](#)
- [show tech prefs, on page 215](#)
- [show tech procedures, on page 216](#)
- [show tech repltimeout, on page 216](#)
- [show tech routepatterns, on page 217](#)
- [show tech routeplan, on page 217](#)
- [show tech runtime, on page 217](#)
- [show tech sqlhistory, on page 218](#)
- [show tech systables, on page 218](#)
- [show tech system, on page 219](#)
- [show tech table, on page 220](#)
- [show tech triggers, on page 220](#)
- [show tech version, on page 220](#)
- [show timezone config, on page 221](#)
- [show timezone list, on page 221](#)
- [show tlstrace, on page 222](#)

- [show tls min-version, on page 222](#)
- [show tlsresumptiontimeout, on page 222](#)
- [show trace, on page 223](#)
- [show ups status, on page 223](#)
- [show version active, on page 224](#)
- [show version inactive, on page 224](#)
- [show vos version , on page 224](#)
- [show web-security, on page 225](#)
- [show webapp session timeout, on page 226](#)
- [show workingdir, on page 226](#)
- [show logins unsuccessful, on page 226](#)

show account

This command lists current administrator accounts, except the primary administrator account.

show account

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

show accountlocking

This command displays the current account locking settings.

show accountlocking

Command Modes Administrator (admin:)

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:show accountlocking
Account Lockout is enabled
Unlock Time : 300 seconds
Retry Count : 3 attempts
```

show cert default-ca-list

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show cert default-ca-list

This command displays all the default CA certificates, which are bundled with Unified Communications Manager and IM and Presence Service.

show cert default-ca-list

Command Modes Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence Service.

Example

admin:show cert default-ca-list

| Common Name | Trust Stores | Purpose |
|---|----------------------------------|---|
| "VeriSign Class 3 Secure Server CA - G3" | tomcat-trust | This certificate is used by UCM to communicate with Cisco if Call-Home feature is enabled. |
| "CAP-RTP-002" | CallManager-trust, CAPF-trust | This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile |
| "Cisco Manufacturing CA" | CallManager-trust, CAPF-trust | This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile |
| "CAP-RTP-001" | CallManager-trust, CAPF-trust | This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile |
| "ACT2 SUDI CA" | CallManager-trust, CAPF-trust | This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM |

| | | |
|-------------------------------|----------------------------------|--|
| "Cisco Manufacturing CA SHA2" | CallManager-trust, CAPF-trust | using the MIC when associated with a secure profile. |
| "Cisco Root CA 2048" | CallManager-trust, CAPF-trust | This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile. |
| "Cisco Root CA M2" | CallManager-trust, CAPF-trust | This certificate was used to sign the MIC installed on Cisco endpoint. Presence of this certificate allows the end point to communicate securely with UCM using the MIC when associated with a secure profile. |

show cert list

This command displays certificate trust lists.

show cert list {own | trust}

| Syntax Description | Parameters | Description |
|--------------------|--------------|---------------------------------|
| | own | Specifies owned certificates. |
| | trust | Specifies trusted certificates. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:cert list own
```

show cert list type

show cert list type

This command displays the available selected type certificate files.

show cert list type {own | trust}

| Syntax Description | Parameters | Description |
|--------------------|--------------|---------------------------------|
| | own | Specifies owned certificates. |
| | trust | Specifies trusted certificates. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

show cert own

This command displays certificate contents.

show cert own *filename*

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | own | Specifies owned certificates. |
| | <i>filename</i> | Represents the name of the certificate file. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

show cert trust

This command displays certificate contents.

show cert trust *filename*

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | trust | Specifies trusted certificates. |
| | <i>filename</i> | Represents the name of the certificate file. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

show cli pagination

This command displays the status of automatic CLI automatic pagination.

show cli pagination

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:show cli pagination
Automatic Pagination : Off.
```

show cli session timeout

show cli session timeout

This command displays the CLI session timeout value, which is the amount of time, in minutes, that can elapse before a CLI session times out and disconnects.

show cli session timeout

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

show csr list

This command displays Certificate Sign Request contents and certificate trust lists.

show csr list {own | trust}

Syntax Description

| Parameters | Description |
|--------------|--|
| own | Shows a list of owned Certificate Sign Requests. |
| trust | Shows a list of trusted Certificate Sign Requests. |

Command Modes

Administrator (admin:)

Usage Guidelines

The certificate name can be obtained by using the **show cert list own** command.

Requirements

Command privilege level: 1

Allowed during upgrade:

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin: show csr list own
tomcat/tomcat.csr
Vipr-QuetzalCoat1/Vipr-QuetzalCoat1.csr
....
```

.....
.....

show csr list type

This command displays the selected own Certificate Sign Request files.

show csr list type own

| Syntax Description | Parameters Description |
|--------------------|---|
| | own Shows a list of owned Certificate Sign Requests. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show csr own

This command displays Certificate Sign Request (CSR) contents and certificate trust lists.

show csr own name

| Syntax Description | Parameters Description |
|--------------------|---------------------------------------|
| | name The name of the CSR file. |

Command Modes Administrator (admin:)

Usage Guidelines The certificate name can be obtained by using the **show cert list own** command.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin:show csr own tomcat/tomcat.csr
```

```
[
```

show csr own name

```
[

-----BEGIN CERTIFICATE SIGN REQUEST-----

MIIDrDCCAxUCBENeUewwDQYJKoZIhvcNAQEEBQAwggEbMTQwMgYDVQQGEytVbmFibGUgdG8gZmlu
ZCBDb3VudHJ5IGluIHBsYXRmb3JtIGRhGFIYXN1MTIwMAYDVQQIEy1VbmFibGUgdG8gZmluZCBT
dGF0ZSBpbIBwbGF0Zm9ybSBkYXRhYmFzZTE1MDMGA1UEBxMsVW5hYmx1IHRvIGZpbmQgTG9jYXRp
b24gaW4gcGxhdGZvcm0gZGF0YWJhc2UxMDAuBgNVBAoTJ1VuYWJsZSB0byBmaW5kIE9yZyBpbIBw
bGF0Zm9ybSBkYXRhYmFzZTE1UEAxMoVW5hYmx1IHRvIGZpbmQgVW5pdCBpbIBwbGF0Zm9y
bSBkYXRhYmFzZTETMBEGA1UEAxMKYmxkc1jY20zNjAeFw0wNTEwMjUxNTQwMjhaFw0xMDEwMjQx
NTQwMjhaMIIBgE0MDIGA1UEBhMrVW5hYmx1IHRvIGZpbmQgQ291bnRyeSEpbIBwbGF0Zm9ybSBk
YXRhYmFzZTEyMDAGA1UECBMpVW5hYmx1IHRvIGZpbmQgU3RhdGUgA4gcGxhdGZvcm0gZGF0YWJh
c2UxNTAzBqNVBAcTLFVuYWJsZSB0byBmaW5kIEExvY2F0aW9uIGluIHBsYXRmb3JtIGRhGFIYXN1
MTAwLgYDVQQKEydVbmFibGUgdG8gZmluZCBPcmcgA4gcGxhdGZvcm0gZGF0YWJhc2UxMTAvBgNV
BAsTKFVuYWJsZSB0byBmaW5kIFVuaxQgaW4gcGxhdGZvcm0gZGF0YWJhc2UxEzARBgNVBAMTCmJs
ZHITY2NtMzYwqZ8wDQYJKoZIhvcNAQEEBQADgY0AMIGJAoGBAMoZ4eLmk1Q3uEFwmb4iU5nrMbhm
J7bexSnC3PuDGncxT3Au4zpGgMaQRL+mk+dAt8gDZffKz8uUkUoibcUhvqk4h3FoTEM+6ggFWVMk
gSNUU+1i9MST4mlaq5hCP87G1jtPbnCXEsFXaKH+gxBq5eBvmmzm01D/otXrsfsnmSt1AgMBAAEw
DQYJKoZIhvcNAQEEBQADgYEAKwhDyOoUDiZv1AOJVTNF3VuUqv4nSJ1GafB6WF1dnh+3yqBWwfGn

```

show csr own name

This command displays Certificate Sign Request (CSR) own certificate files.

show csr own *name* *name of certificate sign request*

| Syntax Description | Parameters | Description |
|--------------------|---|---|
| | <i>name</i> | The name of the CSR file. |
| | <i>name of certificate sign request</i> | The name of the certificate sign request. |

Command Modes Administrator (admin:)

Usage Guidelines The certificate name can be obtained by using the **show cert list own** command.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show ctl

This command displays the contents of the Certificate Trust List (CTL) file on the server. It notifies you if the CTL is invalid.

show ctl

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show cuc cluster status

This command shows the status of the servers in the cluster.

show cuc cluster status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

show cuc config groups

This command displays a list of the valid configuration group names.

show cuc config groups [page]

Syntax Description

Parameters Description

page Causes the output to display one page at a time. Be aware that **page** is case sensitive.

Command Modes

Administrator (admin:)

Usage Guidelines

To see a list of the settings for a specified group, run the command **show cuc config settings**.

show cuc config settings

Requirements

Command privilege level: 0
Allowed during upgrade: Yes
Applies to: Cisco Unity Connection

Example

admin: show cuc config groups

```
CiscoLicensing
ConfigurationAssistant
Conversations
Directory
Groupware
LogMgr
Messaging
:
:
Telephony
```

show cuc config settings

This command displays the settings and values for a specified group of Connection configuration settings.

show cuc config settings *group_name* *page*

Syntax Description

Parameters Description

group_name Specifies the name of the configuration group whose settings you want to display. To see a list of valid group names, run the command **show cuc config groups**. Be aware that group names are case sensitive.

page Causes the output to display one page at a time. Be aware that **page** is case sensitive.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0
Allowed during upgrade: Yes
Applies to: Cisco Unity Connection

Configuration Settings for the Group SA

admin: show cuc config settings SA

| SA Setting | Value |
|------------|-------|
|------------|-------|

```
-----
SessionTimeout      20
Use24HrClockFormat 0
```

show cuc dbconsistency

This command checks the tables and indexes of a specified database for inconsistencies.

show cuc dbconsistency [database_name]

| Syntax Description | Parameters | Description |
|-------------------------|---|---|
| | <i>database_name</i> | Specifies the name of the database that you want to check. Be aware that database names are case sensitive. Connection databases include: <ul style="list-style-type: none"> • unitydirdb-Contains the directory and configuration data. • unitydynedb-Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5-Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb-Contains audit log data. |
| Command Modes | Administrator (admin:) | |
| Usage Guidelines | After the command completes, the system saves detailed information in a log file and displays a summary of the results, including the location of the log file. Use the file commands to display the contents of the file. | |
| |  Caution Checking database consistency makes a significant impact on system performance. Run this command only when little or no system activity is occurring. After the operation begins, you can not cancel it. Do not restart the server during the operation; the operation must complete successfully before Connection will function properly. | |

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example of a Consistency Check of the unityrptdb Database

```
admin: show cuc dbconsistency unityrptdb
```

show cuc dbcontents

Checking consistency of unityrptdb tables. Please wait.

Consistency check of unityrptdb tables successful.

Validation of unityrptdb indexes successful.

Output is in file: cuc/cli/consistency_unityrptdb_070404-123636.txt

show cuc dbcontents

This command exports the data from a specified database to a CSV file.

show cuc dbcontents [database_name]

| Syntax Description | Parameters | Description |
|-------------------------|---|---|
| | <i>database_name</i> | Specifies the name of the database whose data you want to export to a CSV file. Be aware that database names are case sensitive. Connection databases include: <ul style="list-style-type: none"> • unitydirdb-Contains the directory and configuration data. • unitydyndb-Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5-Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb-Contains audit log data. |
| Command Modes | Administrator (admin:) | |
| Usage Guidelines | After the command completes, the location of the CSV file displays. Use the file commands to display the contents of the file. | |
| Caution |  Saving the contents of a database to a CSV file affects system performance. Run this command only when little or no system activity is occurring. | |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example of Exporting the Data From the **unitydirdb** Database to a CSV File and Displays the Location of the File

```
admin: show cuc dbcontents unitydirdb
```

This operation may take a few minutes to complete. Please wait.

Output is in file: cuc/cli/contents_unitydirdb_070404-124027.csv

show cuc dbschema

This command exports the SQL statements that are necessary to replicate the schema for a specified database to a file.

show cuc dbschema [*database_name*]

| Syntax Description | Parameters | Description |
|--------------------|----------------------|--|
| | <i>database_name</i> | Specifies the name of the database whose schema you want to export. Be aware that database names are case sensitive. Connection databases include: <ul style="list-style-type: none"> • unitydirdb-Contains the directory and configuration data. • unityndb-Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5-Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb-Contains audit log data. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

| | |
|------------------|---|
| Usage Guidelines | After the command completes, the location of the file displays. Use the file commands to display the file. |
|------------------|---|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example of Exporting the Schema of the **unitydirdb** Database to a File and Displays the Location of the File

```
admin: show cuc dbschema unitydirdb
```

show cuc dbserver disk

Output is in file: cuc/cli/schema_unitydirdb_061013-115815.sql

show cuc dbserver disk

This command displays summary information about informix storage space for all Connection databases on the current server.

show cuc dbserver disk [page] [file]

| Syntax Description | Parameters | Description |
|--------------------|---------------|---|
| | [page] | Causes the output to display one page at a time. Be aware that page is case sensitive. |
| | [file] | Saves the output to a file. If you include this option, the summary includes the location of the file. Be aware that file is case sensitive. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

show cuc dbserver session

This command displays summary information about a specified informix database user session.

show cuc dbserver session *session_id* [page] [file]

| Syntax Description | Parameters | Description |
|--------------------|-------------------|--|
| | <i>session_id</i> | Specifies the database user session for which you want to display summary information. To get a list of current sessions, use either the show cuc dbserver sessions list command or the show cuc dbserver user list command. |
| | [page] | Causes the output to display one page at a time. Be aware that page is case sensitive. |
| | [file] | Saves the output to a file. If you include this option, the summary includes the location of the file. Be aware that file is case sensitive. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

show cuc dbserver sessions all

This command displays summary information about all the current Informix database user sessions.

show cuc dbserver sessions all [page] [file]

| Syntax Description | Parameters Description |
|--------------------|--|
| | <p>[page] Causes the output to display one page at a time. Be aware that page is case sensitive.</p> |
| | <p>[file] Saves the output to a file. If you include this option, the summary includes the location of the file. Be aware that file is case sensitive.</p> |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

show cuc dbserver sessions list

This command displays a list of the current Informix database user sessions.

show cuc dbserver sessions list [page]

| Syntax Description | Parameters Description |
|--------------------|--|
| | <p>[page] Causes the output to display one page at a time. Be aware that page is case sensitive.</p> |

Command Modes Administrator (admin:)

Usage Guidelines The names of internal database users generally correspond with the names of Connection components. Run this command before you run the **show cuc dbserver session** command to obtain the required session id. Results are sorted by session id.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

show cuc dbserver user list

show cuc dbserver user list

This command displays a list of the active Connection internal database users.

show cuc dbserver user list [page]

| Syntax Description | Parameters Description |
|------------------------------------|---|
| | [page] Causes the output to display one page at a time. Be aware that page is case sensitive. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The names of internal database users generally correspond with the names of Connection components. Results get sorted first by database and then by user. |
| Requirements | |
| Command privilege level: 1 | |
| Allowed during upgrade: Yes | |
| Applies to: Cisco Unity Connection | |

show cuc dbserver user waiting

This command displays a list of the Connection internal users that are waiting for a resource.

show cuc dbserver user waiting [page]

| Syntax Description | Parameters Description |
|------------------------------------|---|
| | [page] Causes the output to display one page at a time. Be aware that page is case sensitive. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The names of the internal database users generally correspond with the names of Connection components. |
| Requirements | |
| Command privilege level: 1 | |
| Allowed during upgrade: Yes | |
| Applies to: Cisco Unity Connection | |

show cuc dbtable contents

This command exports the contents of a specified Connection table to a CSV file.

show cuc dbtable contents{database_nametable_name}

Syntax Description

Parameters Description

database_name Specifies the database that contains the table whose contents you want to export to a CSV file. Be aware that database names are case sensitive. Connection databases include:

- **unitydirdb**—Contains the directory and configuration data.
- **unitydyndb**—Contains dynamic data that Connection uses internally.
- **unitymbxdb1** to **unitymbxdb5**—Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always **unitymbxdb1**.
- **unityrptdb**—Contains audit log data.

table_name Specifies the table whose contents you want to export to a CSV file.

Note For a list of the tables in a specified database, use the **show cuc dbtable list** command. Be aware that table names are case sensitive.

Command Modes

Administrator (admin:)

Usage Guidelines

After the command completes, the location of the CSV file displays. Use the **file** commands to display the contents of the file.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: show cuc dbtable contents unitydirdb tbl_cos
```

```
Output is in file: cuc/cli/contents_tbl_cos_1013-113910.csv
```

show cuc dbtable list

This command displays a list of the tables in a specified database.

show cuc dbtable list *database_name* [page]

show cuc dbtable schema

| Syntax Description | Parameters | Description |
|----------------------|---------------|---|
| <i>database_name</i> | | <p>Specifies the database for which you want a list of tables. Be aware that database names are case sensitive. Connection databases include:</p> <ul style="list-style-type: none"> • unitydirdb—Contains the directory and configuration data. • unitydyndb—Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5—Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb—Contains audit log data. |
| | [page] | Causes the output to display one page at a time. Be aware that page is case sensitive. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: show cuc dbtable list unitydirdb

tbl_accountlogonpolicy
tbl_agency
tbl_agencyextensionrange
tbl_alias
tbl_alternatename
tbl_broadcastmessage
tbl_broadcastmessagerecipient
...
tbl_waveformat
```

show cuc dbtable schema

This command displays a description for a specified table and a list of the columns in the table.

show cuc dbtable schema {*database_nametable_name*} **[page]**

| Syntax Description | Parameters | Description |
|--------------------|----------------------|--|
| | <i>database_name</i> | <p>Specifies the database that contains the table show schema you want to display. Be aware that database names are case sensitive.</p> <p>Connection databases include:</p> <ul style="list-style-type: none"> • unitydirdb—Contains the directory and configuration data. • unitydyndb—Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5—Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb—Contains audit log data. |
| | <i>table_name</i> | <p>Specifies the table whose schema you want to display.</p> <p>Note For a list of the tables in a specified database, use the show cuc dbtable list command. Be aware that table names are case sensitive.</p> |
| | [page] | Causes the output to display one page at a time. Be aware that page is case sensitive. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

show cuc dbview contents

Example of Displaying the Schema for the Table `tbl_user` in the `unitydirdb` Database

```
admin: show cuc dbtable schema unitydirdb tbl_cos
```

A collection of service privileges for subscribers that control access to features and use of the system into classes. Class of Service objects determine which features a subscriber is licensed to use, the maximum length of their greetings and messages, what numbers they are allowed to dial, and what options are available to the subscriber among other things.

```
Columns:
displayname
movetodeletefolder
accessunifiedclient
...
accesslivereply
```

show cuc dbview contents

This command saves the results from a specified SQL view in a CSV file.

show cuc dbview contents {database_nameview_name}

| Syntax Description | Parameters | Description |
|-------------------------|--|--|
| | <i>database_name</i> | Specifies the database that contains the view whose results you want to save to a file. Be aware that database names are case sensitive. Connection databases include: <ul style="list-style-type: none"> • unitydirdb—Contains the directory and configuration data. • unitydyndb—Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5—Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb—Contains audit log data. |
| | <i>view_name</i> | Specifies the view whose results you want to save to a file. |
| | Note | For a list of the views in a specified database, use the show cuc dbview list command. Be aware that view names are case sensitive. |
| Command Modes | Administrator (admin:) | |
| Usage Guidelines | After the command completes, the location of the CSV file displays. Use the file commands to display the contents of the file. | |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

The following example saves the results from the view `vw_cos`, in the database `unitydirdb`, to a CSV file.

```
admin: show cuc dbview contents unitydirdb vw_cos_061013-113910.csv
```

show cuc dbview list

This command displays a list of the views in a specified database.

show cuc dbview list *database_name* [*page*]

| Syntax Description | Parameters | Description |
|--------------------|----------------------|--|
| | <i>database_name</i> | Specifies the database for which you want a list of views. Be aware that database names are case sensitive. Connection databases include: <ul style="list-style-type: none"> • unitydirdb—Contains the directory and configuration data. • unitydynedb—Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5—Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb—Contains audit log data. |
| | [<i>page</i>] | Causes the output to display one page at a time. Be aware that page is case sensitive. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Example

The following example displays a list of the views in the `unitydirdb` database.

```
admin: show cuc dbview list unitydirdb
```

show cuc dbview schema

```

vw_agency
vw_agencyextensionrange
vw_alias
vw_alternatename
vw_broadcastmessage
vw_broadcastmessagerecipient
vw_callaction
...
vw_waveformat

```

show cuc dbview schema

This command displays the schema for a specified view.

show cuc dbview schema {database_nameview_name} [page]

| Syntax Description | Parameters | Description |
|--------------------|----------------------|--|
| | <i>database_name</i> | Specifies the database that contains the view for which you want to display the schema. Be aware that database names are case sensitive. Connection databases include: <ul style="list-style-type: none"> • unitydirdb—Contains the directory and configuration data. • unitydyndb—Contains dynamic data that Connection uses internally. • unitymbxdb1 to unitymbxdb5—Contains the data about the current voice messages in the corresponding mailbox store, including pointers to the audio files that are stored in the file system. If only one mailbox store is configured, the name of the mailbox store database is always unitymbxdb1. • unityrptdb—Contains audit log data. |
| | <i>view_name</i> | Specifies the view for which you want to display the schema. <p>Note For a list of the views in a specified database, use the show cuc dbview list command. Be aware that view names are case sensitive.</p> |
| | [page] | Causes the output to display one page at a time. Be aware that page is case sensitive. |

Command Modes Administrator (admin):

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

The following example displays the schema for the view **vw_user** in the database **unitydirdb**.

```
admin: show cuc dbview schema unitydirdb vw_cos
```

```
A simple view for tbl_Cos.
```

```
Columns:  
objectid  
accessfaxmail  
accesstts  
callholdavailable  
callscreenavailable  
canrecordname  
...  
requiresecuremessages
```

show cuc jetty ssl status

This command allows you to check the status of SSL (Enabled/Disabled) on the Jetty server for notifications.

show cuc jetty ssl status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: show cuc jetty ssl status
```

```
Command completed successfully.  
SSL notification is DISABLED
```

show cuc locales

This command displays a list of the locales currently installed.

show cuc locales

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

```
show cuc speechview registration certificate size
```

Example

```
admin: show cuc locales

Installed Locale Package    Locale
-----
uc-locale-en_GB-6.0.0.0-0    en-GB
uc-locale-fr_CA-6.0.0.0-0    fr-CA
```

show cuc speechview registration certificate size

This command displays the current certificate bit size used for Speech to Text service registration and Voicemail transcription with Nuance server.

show cuc speechview registration certificate size

Command Modes

Administrator (admin):

Usage Guidelines

To view the current certificate bit size, use the **show cuc speechview registration certificate size** (Cisco Unity Connection Only) command.

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only.

show cuc sysagent task list

This command displays a list of the Sysagent tasks.

show cuc sysagent task list [page]

Syntax Description

Parameters Description

[page] Causes the output to display one page at a time. Be aware that **page** is case sensitive.

Command Modes

Administrator (admin):

Usage Guidelines

To run a sysagent task, use the **run cuc sysagent task** command. If the value of the Is Singleton column is Y for a specified task, the task can only be run on the primary server in a multi-server cluster. If this server is standalone, then all tasks run on this server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: show cuc sysagent task list
```

| Task Name | Is Singleton |
|-------------------------------------|--------------|
| ----- | ----- |
| Data.BroadcastMessagePurge | N |
| Umss.CleanDeletedMessagesTask | Y |
| Umss.CleanDirectoryStreamFilesTask | Y |
| Umss.CleanOrphanAttachmentFilesTask | Y |
| ... | |
| Data.UpdateDatabaseStats | N |

show cuc sysagent task results

This command displays the times at which the specified task started and completed, with the most recent time listed first.

show cuc sysagent task results *task_name* [*page*]

Syntax Description

Parameters Description

task_name Specifies the task for which you want to display information when the task starts and completes.

Note For a list of task names, run the **show cuc sysagent task list** command. Be aware that task names are case sensitive.

[*page*] Causes the output to display one page at a time. Be aware that **page** is case sensitive.

Command Modes

Administrator (admin:)

Usage Guidelines

To run a Sysagent task, use the **run cuc sysagent task** command.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

show cuc sysinfo

Applies to: Cisco Unity Connection

Example

The following example displays the times at which the Sysagent task Umss.CleanDeletedMessagesTask started and completed.

```
admin: show cuc sysagent task results Umss.CleanDeletedMessagesTask
```

| Time Started | Time Completed |
|-------------------------|-------------------------|
| 2006-10-25 17:31:45.689 | 2006-10-25 17:31:45.785 |
| 2006-10-25 17:16:45.702 | 2006-10-25 17:16:45.742 |
| 2006-10-25 17:01:45.690 | 2006-10-25 17:01:45.730 |

show cuc sysinfo

This command displays a summary of hardware and software system information for the current Connection server, including the version installed on the active and inactive partitions; whether a cluster is configured; QOS settings; hardware specifications; the amount of used and free disk space on the active, inactive, and common partitions; licensing information; and so on.

show cuc sysinfo

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection

Example

```
admin: show cuc sysinfo

Gather Data/Time : Wed Oct 21 09:45:29 PDT 2009

Connection Install Information:

Host Name : connection1

Version:

Active Version : 8.0.0.98000-210
```

```

Inactive Version : 8.0.0.98000-201

High Availability (this server is) : Pri_Single_Server

Publisher : connection1.cisco.com - 10.10.10.10

Subscriber(s) : None

QOS Settings :

Call Signaling DSCP : CS3

Media Signaling DSCP : EF

Hardware :

HW Platform : 7825I3

Processors : 1

Type : Family: Core 2

CPU Speed : 2130

Memory : 2048

Object Id : 1.3.6.1.4.1.9.1.746

OS Version : UCOS 4.0.0.0-31

...

```

show cuc tech dbschemaversion

This command displays the schema version information for each database.

show cuc tech dbschemaversion [page]

Syntax Description

Parameters Description

[page] Causes the output to display one page at a time. Be aware that **page** is case sensitive.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

```
show cuc tech dbserver all
```

Example

```
admin: show cuc tech dbschemaversion

unitydirdb
=====
Schema Version Product Version Date
-----
1.2.363 2.1 2007-02-13 19:10:50.0
```

show cuc tech dbserver all

This command runs all the show cuc tech commands in sequence and saves the results in a text file.

show cuc tech dbserver all

Command Modes Administrator (admin:)

Usage Guidelines After the command completes, detailed information gets saved in a text file and the location of the text file displays. Use the file commands to display the contents of the file.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Example

```
admin: show cuc tech dbserver all

Output is in file: cuc/cli/dbserverall_061013-111801.txt
```

show cuc tech dbserver integrity

This command checks the integrity of the Informix database server storage space structure.

show cuc tech dbserver integrity

Command Modes Administrator (admin:)

Usage Guidelines After the command completes, detailed information gets saved in a text file, and a summary of the results displays, including the location of the file. Use the file commands to display the contents of the file.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: show cuc tech dbserver integrity
Database system catalog tables were successfully validated.
Database disk extents were successfully validated.
Database reserved pages were successfully validated.
Output is in file: cuc/cli/integrity_061013-95853.txt
```

show cuc tech dbserver log diagnostic

This command checks for the existence of Informix assertion-failure and shared-memory-dump logs.

show cuc tech dbserver log diagnostic

Command Modes

Administrator (admin:)

Usage Guidelines

If the logs exist, their location displays. Use the file commands to display the contents of the files.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only.

Example

```
admin:show cuc tech dbserver log diagnostic
The following Informix logs are available for the UC database server:
core/af.3599c
core/af.36858
```

show cuc tech dbserver log message

This command displays the end of the Informix message log.

show cuc tech dbserver log message [lines] [{page}]

Syntax Description
Parameters Description

lines Specifies the number of lines that display at the end of the Informix message log. If the *lines* parameter is not included, the last 20 lines of the log are displayed.

```
show cuc tech dbserver status
```

Parameters Description

| | |
|-------------|---|
| page | (Optional) Causes the output to display one page at a time. Be aware that page is case sensitive. |
|-------------|---|

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only.

Example

```
admin:show cuc tech dbserver log message
Message Log File: online.ciscounity.log
18:09:01 Fuzzy Checkpoint Completed: duration was 0 seconds, 6 buffers
not flushed.
18:09:01 Checkpoint loguniq 57, logpos 0x208418, timestamp: 0x33b807
18:09:01 Maximum server connections 159
18:14:01 Fuzzy Checkpoint Completed: duration was 0 seconds, 6 buffers
not flushed.
18:14:01 Checkpoint loguniq 57, logpos 0x20a57c, timestamp: 0x33b9fc
```

show cuc tech dbserver status

This command saves a detailed status report of the database server instance to a file.

show cuc tech dbserver status

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only.

Example

```
admin:show cuc tech dbserver status
Output is in file: cuc/cli/status_061013-95031.txt
```

show cuc trace levels

This command displays a list of all the diagnostic traces and trace levels that are currently enabled.

show cuc trace levels [page]

| Syntax Description | Parameters Description |
|--|--|
| | page (Optional) Causes the output to display one page at a time. Be aware that page is case sensitive. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | To enable or disable specified traces and trace levels, use the set cuc trace (Cisco Unity Connection only) command. |
| Requirements | |
| Command privilege level: 0 | |
| Allowed during upgrade: Yes | |
| Applies to: Cisco Unity Connection only. | |

Example

```
admin:show cuc trace levels
Trace Name Levels
-----
Arbiter -
AudioStore 0
AxlAccess -
BulkAdministrationTool 0
CCL 10,11
CDE 3,14
CDL 11,13,15,17
::
VirtualQueue -
```

show cuc version

This command displays the Cisco Unity Connection version that is currently installed on the active and inactive partitions.

show cuc version

| Command Modes | Administrator (admin:) |
|--|---|
| Usage Guidelines | This command always displays the version in the active partition. If the active partition contains an upgrade, the command also shows the version in the inactive partition. The current Engineering Special also displays. |
| Requirements | |
| Command privilege level: 0 | |
| Allowed during upgrade: Yes | |
| Applies to: Cisco Unity Connection only. | |

show date

Example

```
admin:show cuc version
Active version: 7.0.1.10000-323
Inactive version: 7.0.0.39700-277
```

show date

This command displays the date and time on the server.

show date

Command Modes Administrator (admin:)

Example

```
admin: show date
Sat Jul 17 01:28:57 IST 2010
```

show diskusage

This command displays disk usage information about specific directories.

show diskusage activelog {activelog | common | inactivelog | install | tftp | tmp} filename {directory | sort}

| Syntax Description | Parameters | Description |
|--------------------|---------------------------------|---|
| | filename <i>filename</i> | Saves the output to a specified file. These files are stored in the platform/cli directory. To view saved files, use the file view activelog command. |
| | directory | Displays the directory sizes only. |
| | sort | Sorts the output on the basis of file size. File sizes display in 1024-byte blocks. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show dscp all

This command displays the current DSCP traffic markings on all the ports. It displays the DSCP markings in decimal and hexadecimal. If the value corresponds to a class then it displays the correct class. If the value does not correspond to a class, then it displays N/A.

show dscp all

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager and Cisco Unity Connection

show dscp defaults

This command displays the default factory DSCP settings. These values take effect if the **set dscp defaults** command is executed.

show dscp defaults

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager and Cisco Unity Connection

show dscp marking

This command displays the current DSCP traffic markings for a particular DSCP value.

show dscp marking *value*

Syntax Description

Parameters Description

| | |
|--------------|---|
| <i>value</i> | DSCP value. You can enter the name of a well-known DSCP class, or a numeric value in decimal or hexadecimal format. Precede hexadecimal values with 0x or 0X. |
|--------------|---|

show dscp status

| | |
|---|--|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | <p>The valid class names as defined by DSCP are:</p> <ul style="list-style-type: none"> • Class Selector: values CS0, CS1, CS2, CS3, CS5, CS6 CS7 The class selector (CS) values correspond to IP Precedence values and are fully compatible with IP Precedence. • Expedited Forwarding: value EF EF PHB is ideally suited for applications such as VoIP that require low bandwidth, guaranteed bandwidth, low delay, and low jitter. • Best Effort: value BE Also called default PHB, this value essentially specifies that a packet be marked with 0x00, which gets the traditional best-effort service from the network router. • Assured Forwarding: values AF11, AF12, AF13, AF21, AF22, AF23, AF41, AF42, AF43 There are four types of Assured Forwarding classes, each of which has three drop precedence values. These precedence values define the order in which a packet is dropped (if needed) due to network congestion. For example, packets in AF13 class are dropped before packets in the AF12 class. |
| Requirements | |
| Command privilege level: 1 | |
| Allowed during upgrade: No | |
| Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection | |

show dscp status

This command displays the current DSCP traffic markings.

show dscp status {enabled | disabled}

| Syntax Description | | Parameters | Description |
|---------------------------|--|--|--------------------|
| enabled | | Filters the output to show only DSCP traffic markings that are enabled. If you do not specify a status, this filter is the default option. | |
| disabled | | Filters the output to show only DSCP traffic markings that are disabled. | |

| | |
|----------------------------|------------------------|
| Command Modes | Administrator (admin:) |
| Requirements | |
| Command privilege level: 0 | |
| Allowed during upgrade: No | |

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show environment fans

This command shows the status of the fan sensors.

show environment fans

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show environment power-supply

This command shows the status of the power supply for MCS-7845, MCS-7835, MCS-7825H3/H4, and MCS-7816H3 servers—those with redundant power supply or embedded health hardware.

show tlstrace

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show environment temperatures

This command retrieves the status of the temperature sensors.

show environment temperatures

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

show fileserver transferspeed

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show fileserver transferspeed

This command shows the reading and writing speed between the IM and Presence Service node and the external file server. It involves copying a large file onto the mounted directory and then copying it back onto the node. As a result, this command may have a performance impact on the node from which it is run.

show fileserver transferspeed

Command Modes

Administrator (admin:)

Requirements

Applies to: IM and Presence Service on Unified Communications Manager.

Example

```
admin:show fileserver transferspeed

WARNING: This command involves copying a large file to and from the mounted directory. It
can impact the performance of the system.

Do you want to continue? (y/n):y

Creating a file to perform the test, please wait...

Copying the file onto the mounted file system. Please note the writing speed recorded below.
262144+0 records in
262144+0 records out
1073741824 bytes (1.1 GB) copied, 28.9302 s, 37.1 MB/s

Copying the file from the mounted file system. Please note the reading speed recorded below.
262144+0 records in
262144+0 records out
1073741824 bytes (1.1 GB) copied, 67.7504 s, 15.8 MB/s

Clean-up finished
admin:
```

show haproxy client-auth

This command displays the client authentication configured on the specified port.

show haproxy client-auth *portnum*

| Parameter | Description |
|----------------|---|
| <i>portnum</i> | <p>Enter the port number to view the client authentication configured on the specified port.</p> <p>Note The supported port numbers are 6971, 6972 and 9443.</p> |

Command Modes Administrator (admin:)

Usage Guidelines Administrator can execute the **help show haproxy client-auth <portnum>** command to view the help content.

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager

Example

```
admin:show haproxy client-auth 9443
Client authentication on the port 9443 is currently set to optional
admin:show haproxy client-auth 9456
Enter valid values for the port.
Suggested values are 6971, 6972 and 9443
Executed command unsuccessfully

admin:help show haproxy client-auth 9443
show haproxy client-auth help:
This command will display client-auth for the specified port.
Example:
admin:show haproxy client-auth 6971
Client authentication on the port 6971 is currently set to required.
```

show haproxy num-threads

This command displays the number of HAProxy threads.

show haproxy num-threads

Command Modes Administrator (admin:)

Usage Guidelines Administrator can execute the **help show haproxy num-threads** command to view the help content.

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager

show hardware

Example

```
admin:show haproxy num-threads
HAProxy process running 2 threads
admin:help show haproxy num-threads

show haproxy num-threads:
This command updates the number of threads started by HaProxy service.
Example:
admin:show haproxy num-threads
```

show hardware

This command displays hardware-related information about the platform.

show hardware

Command Modes Administrator (admin:)

Usage Guidelines The following information is displayed:

- Platform
- Serial number
- BIOS build level
- BIOS manufacturer
- Active processors
- RAID controller status
- Disk partition details

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show ipsec information

This command displays detailed information about the specified ipsec policy.

show ipsec information {*policy_group_name*}

| Syntax Description | Parameters Description |
|-------------------------|---|
| | <i>policy_group</i> |
| | <i>policy_name</i> |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | Requirements |
| | Command privilege level: 1 |
| | Allowed during upgrade: yes |
| | Applies to: IM and Presence service on Unified Communications Manager |

Example

```
admin:show ipsec information test test1
PolicyGroup          : test
PolicyName           : test1
Type                 : transport
Source Address       : 10.94.171.3
Source Type          : ip
Destination Address : 10.94.1.2
Destination Type    : ip
Protocol             : tcp
Source Port          : Any
Destination Port     : Any
Remote Port          : Any
Authentication Method: psk
Destination Certificate: null
PSK                 : cisco
Phase 1 Life Time   : 3600
Encryption Algorithm : des
Hash Algorithm       : sha1
Phase 1 DH Value    : null
Phase 2 Life Time   : 3600
ESP                 : null_enc
AH                  : hmac_sha1
Phase 2 DH Value    : null
Peer Type            : null
Status               : disabled
Source Certificate  : null
```

show ipsec policy_group

This command displays all the ipsec policy group on the node.

show ipsec policy_group

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
| Requirements | |

Command privilege level: 1

show ipsec policy_name

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show ipsec policy_name

This command displays the list of ipsec policy names that exist in the specified policy group.

show ipsec policy_name policy_group

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>policy_group</i> Specifies the policy group name. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show ipsec status

show ipsec status

Command Modes Administrator (admin:)

Usage Guidelines Requirements

Command privilege level:

Allowed during upgrade:

Applies to: IM and Presence service on Unified Communications Manager

show itl

This command displays the ITL file contents or prints an error message if the ITL file is invalid.

show itl

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show logins

This command lists recent logins to the server

show login [number]

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>number</i> Specifies the number of the most recent logins to display. The default is 20. |

| Command Modes | Administrator (admin:) |
|---------------|------------------------|
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show logins successful

This command shows the previous successful logins.

show logins successful [{last n}]

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>last n</i> (Optional) Represents the last number of logins. By default, the value of this variable is 20. |

| Command Modes | Administrator (admin:) |
|---------------|------------------------|
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show logins unsuccessful

Use this command to list recent unsuccessful login attempts to the following web applications:

- On Unified Communications Manager

show key authz encryption

- Disaster Recovery System
- Cisco Unified OS Administration
- On IM and Presence Service
 - IM and Presence Disaster Recovery System
 - Unified IM and Presence OS Administration

show logins unsuccessful [number]

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>number</i> Specifies the number of most recent logins to display. The default is 20. |

Command Modes Administrator (admin)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to Unified Communications Manager and IM and Presence Service

show key authz encryption

Run this command on any Unified Communications Manager node to view the OAuth signing key checksum that Unified Communications Manager uses to authenticate Cisco Jabber clients.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager and the IM and Presence Service.

show key authz signing

Run this command on any Unified Communications Manager node to view the OAuth signing key checksum that Unified Communications Manager uses to authenticate Cisco Jabber clients.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager and the IM and Presence Service.

show license all

This command displays license status, license usage, UDI, and the agent version.

show license all

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show license status

This command displays the smart licensing status.

show license status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show license summary

This command displays the smart licensing status and the license usage details.

show license summary

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show license tech support

show license tech support

This command displays smart licensing status, product information, and product version.

show license tech support

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show license trace

This command traces the content of smart agent-related logs to the console.

show license trace

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show license UDI

This command displays all members in the Unique Device Identification(UDI) structure that are not NULL. Following are the list of UDI instances displayed for Unified Communications Manager:

- PID—Product Identifier
- SN—Serial Number
- UUID—Universal Unique Identifier

show license UDI

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show license usage

This command displays the entitlements that are currently in use.

show license usage

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

show Login Grace Timeout

This command shows the login Grace Timeout.

show Login Grace Timeout

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show media streams

This command captures information on current media stream connections.

show media streams [options]

show media streams

| Syntax Description | Parameters | Description |
|--------------------|---|-------------|
| | <p><i>options</i> Enter one of the following options:</p> <ul style="list-style-type: none"> • file fname: Limit (valid characters alphanumeric [a-Z, A-Z, 0-9, (-) ad , (_)]. Default: mediainfo • count #: Range 1-1000; Default: 2 • sleep #: Range 1-300 seconds; Default 5 • device {ALL ANN CFB CRA MOH MTP} Default: device ALL • info: Displays extra information • buffers: Displays buffer usage information. • trace: Activates extra trace from media driver to system log. <p>Note Ignore any kernel messages that display on the console screen when show media streams trace is entered.</p> | |

| | |
|--|------------------------|
| Command Modes | Administrator (admin:) |
| <p>Requirements</p> <p>Command privilege level: 1</p> <p>Allowed during upgrade: Yes</p> <p>Applies to: Unified Communications Manager and Cisco Unity Connection</p> | |

Example

```
admin: show media streams info buffers

Resulting file /platform/log/mediainfo.txt contains:

Time: 2008.03.04 11:01:42
I/F Ver=5, #Apps: Free= 7, Alloc= 4, #Conf: Free= 12, #Streams: Free= 40
Buffer Size = 652, Allocated Buffers= 1, Free Buffers = 5147
Buffer Size = 8192, Allocated Buffers= 0, Free Buffers = 450
App ID= 332, Cfg=CFB, Dead App Timer=86400, Active=Yes, Streams: Available= 92 Active=
4
Conf ID = 16777225, Type = Two No Sum, Streams: Tx = 2, Rx = 2, Active = Yes
Rx Stream: PktCnt= 5979, PID=16777653, PktSz=20ms, Payld=uLaw, IP=10.89.80.178:24652,
MCast=N, Mute=N, UsrMd=N, Actv=Y, QdPkts=2, PktOR=0, DtmfPL=0 DiscTimeSlice= 0 DiscPkts= 0
10:59:42
Buffer Size = 652, Used Buffers = 1
Buffer Size = 8192, Used Buffers = 0
Rx Stream: PktCnt= 6179, PID=16777651, PktSz=20ms, PayId=uLaw, IP=10.89.80.178:24650,
MCast=N, Mute=N, UsrMd=N, Actv=Y, QdPkts=0, PktOR=0, DtmfPL=0 DiscTimeSlice= 0 DiscPkts= 0
10:59:38
Buffer Size = 652, Used Buffers = 0
Buffer Size = 8192, Used Buffers = 0
Tx Stream: PktCnt= 5988, PID=16777653, PktSz=20ms, Payld=uLaw,
IP=10.13.5.189:29450 (24652), MCast=N, Mute=N, UsrMd=N, Actv=Y, DtmfPL=0, DtmfQ=0 10:59:42
Buffer Size = 652, Used Buffers = 0
Buffer Size = 8192, Used Buffers = 0
```

```

Tx Stream: PktCnt= 6193, PID=16777651, PktSz=20ms, Payld=uLaw,
IP=10.13.5.182:28516(24650), MCast=N, Mute=N, UsrMd=N, Actv=Y, DtmfPL=0, DtmfQ=0 10:59:42
Buffer Size = 652, Used Buffers = 0
Buffer Size = 8192, Used Buffers = 0
App ID= 331, Cfg=ANN, Dead App Timer=86400, Active=Yes, Streams: Available= 96 Active=
0
App ID= 330, Cfg=MOH, Dead App Timer=86400, Active=Yes, Streams: Available= 658 Active=
0
App ID= 329, Cfg=MTP, Dead App Timer=86400, Active=Yes, Streams: Available= 96 Active=
0

```

show memory

This command displays information about the onboard memory.

show memory {count | modules | size}

Syntax Description

| Parameters | Description |
|----------------|---|
| count | Displays the number of memory modules on the system. |
| modules | Displays detailed information about all the memory modules. |
| size | Displays the total amount of physical memory. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show myself

This command displays information about the current account.

show myself

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show network all

show network all

This command shows network information for listening and nonlistening sockets.

show network all [detail] [page] [search *srchtext*]

| Syntax Description | Parameters | Description |
|--------------------|-------------------------------|---|
| | detail | Shows additional information. |
| | page | Displays information one page at a time. |
| | search <i>srchtext</i> | Searches for <i>srchtext</i> in the output. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network cluster

This command lists nodes in the network cluster and also shows the remaining timer value when you enable Dynamic Cluster Configuration.

show network cluster

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network dhcp eth0

This command shows DHCP status information.

show network dhcp eth0

| | |
|---|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The eth0 parameter displays Ethernet port 0 settings, including DHCP configurations and options. |
| Requirements | |
| Command privilege level: 0 | |
| Allowed during upgrade: Yes | |
| Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

show network eth0

This command shows network information for ethernet 0.

show network eth0 [detail] [search *srctxt*]

| Syntax Description | Parameters | Description |
|---|---|---|
| | detail | Shows additional information. |
| | search | Searches for <i>srctxt</i> in the output. |
| <i>srctxt</i> | | |
| Command Modes | Administrator (admin:) | |
| Usage Guidelines | The eth0 parameter displays Ethernet port 0 settings | |
| Requirements | | |
| Command privilege level: 0 | | |
| Allowed during upgrade: Yes | | |
| Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | | |

show network failover

This command shows Network Fault Tolerance information.

show network failover [detail] [page]

| Syntax Description | Parameters | Description |
|---------------------------|-------------------|---------------------------------------|
| | detail | Shows additional information. |
| | page | Shows information one page at a time. |

show network ip_conntrack

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network ip_conntrack

This command shows ip_conntrack usage information.

show network ip_conntrack

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network ipprefs

This command shows the list of ports that have been requested to be opened or translated in the firewall.

show network ipprefs {all | enabled | public}

Syntax Description

Parameters Description

all Shows all incoming ports that may be used on the product.

enabled Shows all incoming ports that are currently opened.

public Shows all incoming ports that are currently opened for a remote client.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin:show network ipprefs public
Application IPProtocol PortValue HashLimit (max:rate) H-Status ConnLimit C-Status Type
XlatedPort Status Description
-----
----- -----
sshd      tcp      22      1500:25/second  enabled   -  disabled public
-      enabled sftp and ssh
tomcat    tcp      443     4000:50/second  disabled  300  enabled public
8443     enabled  secure web
tomcat    tcp      80      4000:50/second  disabled  300  enabled public
8080
```

show network ipv6

This command shows IPv6 network routes and network settings.

show network ipv6 {route | settings}

Syntax Description

| Parameters | Description |
|-----------------|----------------------------------|
| route | Shows all IPv6 routes. |
| settings | Shows all IPv6 network settings. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, Cisco Unity Connection

show network max_ip_conntrack

This command shows max_ip_conntrack information.

show network max_ip_conntrack

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network ntp option

show network ntp option

This command displays the security option that is configured in the /etc/config file.

show network ntp option

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network route

This command shows network routing information.

show network route [detail] [search *srchtext*]

| Syntax Description | Parameters | Description |
|--------------------|-------------------------------|---|
| | detail | Shows additional information. |
| | search <i>srchtext</i> | Searches for the <i>srchtext</i> in the output. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show network status

This command shows active internet connections.

show network status [detail] [listen] [process] [all] [nodns][search *stext*]

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | detail | Shows additional information. |
| | listen | Shows only listening sockets. |
| | process | Shows the process ID and name of the program to which each socket belongs. |
| | all | Shows both listening and nonlistening sockets. |
| | nodns | Shows numerical addresses without any DNS information. |
| | search | Searches for the <i>stext</i> in the output. <i>stext</i> |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

This example displays active internet connections.

```
admin: show network status
```

show network name-service attributes

This command displays name service cache general attributes.

show network name - service attributes

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example:

```
admin:show network name-service hosts attributes
enable-cache          yes
positive-time-to-live 3600
negative-time-to-live 20
```

Successful

show network name-service cache-stats

show network name-service cache-stats

This command displays name service cache statistics.

show network name-services[host][services] cache-stats

| Syntax Description | Parameters | Description |
|--------------------|-----------------|-------------------------|
| | hosts | host services cache. |
| | services | services service cache. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example:

```
admin:show network name-service hosts cache-stats
yes cache is enabled
    no cache is persistent
    yes cache is shared
    211 suggested size
    216064 total data pool size
    272 used data pool size
    3600 seconds time to live for positive entries
    20 seconds time to live for negative entries
    0 cache hits on positive entries
    0 cache hits on negative entries
    2 cache misses on positive entries
    0 cache misses on negative entries
    0% cache hit rate
    2 current number of cached values
    2 maximum number of cached values
    0 maximum chain length searched
    0 number of delays on rdlock
    0 number of delays on wrlock
    0 memory allocations failed
    yes check /etc/hosts for changes
```

Successful

show network name-service {hosts|services} attributes

This command displays name service cache attributes.

show networkname - service{hosts|services} attributes

| Syntax Description | Parameters | Description |
|--------------------|-----------------|-------------------------|
| | hosts | hosts services cache. |
| | services | services service cache. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Example:

```
admin:show network name-service hosts attributes
enable-cache          yes
positive-time-to-live 3600
negative-time-to-live 20
suggested-size         211
persistent             no
max-db-size            33554432
```

Successful

show open files all

This command shows all open files on the system.

show open files all

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show open files process

The command shows open files that belong to a specified process.

show open files process *processID*

| Syntax Description | Parameters | Description |
|--------------------|------------------|----------------------|
| | <i>processID</i> | Specifies a process. |

show open files regexp

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show open files regexp

This command shows open files that match the specified regular expression.

show open files regexp *reg_exp*

Syntax Description

Parameters Description

reg_exp Specifies a regular expression.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show open ports all

This command shows all open ports on the system.

show open ports all

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show open ports process

This command displays open ports the belong to a specified process.

show open ports process *processID*

| Syntax Description | Parameters Description |
|--------------------|---------------------------------------|
| | <i>processID</i> Specifies a process. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show open ports regexp

This command shows open ports that match the specified regular expression.

show open ports regexp *reg_exp*

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>reg_exp</i> Specifies a regular expression. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show packages

This command displays the name and version for installed packages.

show packages {active | inactive} *name* [*page*]

| Syntax Description | Parameters Description |
|--------------------|--|
| | active Specifies active packages. |
| | inactive Specifies inactive packages. |
| | name Specifies the package name. To display all active or inactive packages, use the wildcard character, * . |
| | page Shows the output one page at a time |

show password

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password

This command shows information about the configured password.

show password {age | history | inactivity}

| Syntax Description | Parameters | Description |
|--------------------|-------------------|---|
| | age | Shows information about the configured password age parameters |
| | history | Shows the number of passwords that the history maintains for OS administration accounts. |
| | inactivity | Shows the status of the password inactivity for OS accounts. Password inactivity is the number of days of inactivity after a password has expired before the account is disabled. |

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password change-at-login

This command shows whether a user is forced to change passwords after the user signs in to the system the next time.

show password change-at-login *userid*

| Syntax Description | Parameters | Description |
|--------------------|----------------------|---|
| | <i>userid</i> | Specifies the user account that you want to show. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password complexity character

This command displays the status of the password complexity rules—whether they are disabled or enabled. If the password complexity rules are enabled, this command displays the shows their current configuration.

show password complexity character

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password complexity length

This command displays the minimum length of passwords that need to be used for Cisco OS administrator accounts. The default minimum length of a password is six characters.

show password complexity length

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password expiry

This command shows the configured password expiration parameters.

show password expiry {maximum-age | minimum-age}

show password expiry user

| Syntax Description | Parameters | Description |
|--------------------|--------------------|---|
| | maximum-age | Shows the maximum number of days for set password expiry. |
| | minimum-age | Shows the minimum number of days for set password expiry. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password expiry user

This command shows the configured password expiration parameters for the specified user.

show password expiry user {maximum-age | minimum-age} *userid*

| Syntax Description | Parameters | Description |
|--------------------|--------------------|---|
| | maximum-age | Shows the maximum number of days for set password expiry. |
| | minimum-age | Shows the minimum number of days for set password expiry. |
| | <i>userid</i> | Specifies the user account that you want to show. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show password expiry user list

This command shows the password maximum age and password minimum age for each CLI user in the system.

show password expiry user

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf counterhelp

This command displays information about the specified perfmon counter.

show perf counterhelp *class-name* *counter-name*

Syntax Description**Parameters** **Description**

class-name Represents the class name that contains the counter.

counter-name Represents the counter that you want to view.

Command Modes

Administrator (admin:)

Usage Guidelines

If the class name or counter name contains white spaces, enclose the name in double quotation marks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf list categories

This command lists the categories in the perfmon system.

show perf list categories

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf list classes

show perf list classes

This command lists perfmon classes (objects).

show perf list classes [{cat *category*}] [{detail}]

| Syntax Description | Parameters | Description |
|--------------------|---------------|---|
| | cat | Displays perfmon classes for the specified category. <i>category</i> |
| | detail | Displays detailed information. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf list counters

This command lists perfmon counters for the specified perfmon class.

show perf list counters *class-name* [{detail}]

| Syntax Description | Parameters | Description |
|--------------------|-------------------|--|
| | <i>class-name</i> | Represents the class name that contains the counter. |
| | detail | Displays detailed information. |

Command Modes Administrator (admin:)

Usage Guidelines If the class name contains white spaces, enclose the name in double quotation marks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf list instances

This command lists the perfmon instances for the specified perfmon class.

show perf list instances *class-name* [*{detail}*]

Syntax Description

Parameters Description

class-name Represents the class name that contains the counter.

detail Displays detailed information.

Command Modes

Administrator (admin):

Usage Guidelines

If the class name contains white spaces, enclose the name in double quotation marks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf query class

This command queries a perfmon class and displays all the instances and counter values of each instance.

show perf query class *class-name* [*{,class-name...}*]

Syntax Description

Parameters Description

class-name Represents the class name that contains the counter.

Command Modes

Administrator (admin):

Usage Guidelines

If the class name contains white spaces, enclose the name in double quotation marks.

You can specify a maximum of five classes for each command.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf query counter

show perf query counter

This command queries the specified counter or counters and displays the counter value of all instances.

show perf query counter *class-name* *counter-name* [{,counter-name...}]

Syntax Description

Parameters Description

class-name Represents the class name that contains the counter.

counter-name Represents the counter that you want to view.

Command Modes

Administrator (admin:)

Usage Guidelines

If the class name or counter name contains white spaces, enclose the name in double quotation marks.

You can specify a maximum of five counters for each command.



Note

The output that this command returns depends on the number of endpoints that is configured in the Route Groups in Unified Communications Manager.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf query instance

This command queries the specified instance and displays all its counter values.

show perf query instance *class-name* *instance-name* [{,instance-name...}]

Syntax Description

Parameters Description

class-name Represents the class name that contains the counter.

instance-name Specifies the perfmon instance to view.

Command Modes

Administrator (admin:)

Usage Guidelines

If the class name contains white spaces, enclose the name in double quotation marks.

You can specify a maximum of five instances for each command.

This command does not apply to singleton perfmon classes.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show perf query path

This command queries a specified perfmon path.

show perf query path *path-spec* [{*path-spec...*}]

Syntax Description

Parameters Description

path-spec Specifies a perfmon path.

Command Modes

Administrator (admin:)

Usage Guidelines

For an instance-based perfmon class, you must specify *path-spec* as follows:

class-name(*instance-name*)*counter-name*

For a noninstance-based perfmon class (a singleton), you must specify *path-spec* as follows:

*class-name**counter-name*

You can specify a maximum of five paths for each command.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin: show perf query path "Cisco Phones (phone-0)\CallsAttempted","Cisco Unified Communications Manager\T1ChannelsActive"
```

show process list

This command displays a list of all the processes and critical information about each process and visually indicates the child-parent relationships between the processes.

show process list [{file *filename*}] [{detail}]

show process load

| Syntax Description | Parameters | Description |
|--------------------|-----------------|---|
| | file | Outputs the results to the file that is specified by the filename variable. |
| | <i>filename</i> | Specifies the filename. |
| | detail | Displays detailed output. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process load

This command displays the current load on the system.

```
show process load [{cont}] [{clear}] [{noidle}] [{num number}] [{thread}] [{cpu | memory | time}] [{page}]
```

| Syntax Description | Parameters | Description |
|--------------------|--------------------------|--|
| | cont | Repeats the command continuously. |
| | clear | Clears the screen before displaying output. |
| | noidle | Ignores the idle or zombie processes. |
| | num <i>number</i> | Displays the number of processes that are specified by number. The default number of processes equals 10. Set <i>number</i> to all to display all processes. |
| | thread | Displays threads. |
| | cpu | Sorts output by CPU usage. This is the default sorting. |
| | memory | Sorts output by memory usage. |
| | time | Sorts output by time usage. |
| | page | Displays the output in pages. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process name

This command displays the details of processes that share the same name and indicates their parent-child relationship.

show process name *process* [{file *filename*}]

| Syntax Description | Parameters | Description |
|--------------------|--------------------------------|--|
| | <i>process</i> | Specifies the name of a process. |
| | file <i>filename</i> | Outputs the results to the file that is specified by <i>filename</i> . |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process name process-name

The command shows the details of processes that share the same name. This command displays parent-child relationship.

show process name *process name* [{file **vm **detail** **cont**}]**

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | <i>process</i> | Specifies the name of a process. |
| | <i>name</i> | |
| | file | (Optional) Shows the file name where the output is to be received. |
| | vm | (Optional) Shows the virtual memory of the process. |
| | detail | (Optional) Shows the details, such as page fault, virtual memory, and start time of the process. |
| | cont | (Optional) Repeats the command continuously. |

Command Modes Administrator (admin:)

show process open**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process open

This command lists the open file descriptors for a comma separated list of process IDs.

show process open file**Syntax Description****Parameters Description****file** (Optional) Shows the file name where the output is to be received.**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process open-fd

This command lists the open file descriptors for a comma-separated list of process IDs.

show process open-fd *process-id* [{,*process-id2*}]**Syntax Description****Parameters Description****process-id** Specifies the process-id.**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process pid

This command shows a specific process number or command name.

show process pid *pid* [{file *filename*}]

Syntax Description

| Parameters | Description |
|--------------------------------|--|
| <i>pid</i> | Specifies the process ID number of a process. |
| file <i>filename</i> | Outputs the results to the file that is specified by <i>filename</i> . |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process search

This command searches for the pattern that the regular expression *regexp* specifies in the output of the operating system-specific process listing.

show process search *regexp* [{file *filename*}]

Syntax Description

| Parameters | Description |
|--------------------------------|--|
| <i>regexp</i> | Represents a regular expression. |
| file <i>filename</i> | Outputs the results to the file that is specified by <i>filename</i> . |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process user

show process user

This command retrieves details of processes that share the user name and displays parent-child relationship.

show process user *username* [{file** *detail detail detail cont*}]**

| Syntax Description | Parameters | Description |
|--------------------|-----------------------------|--|
| | <i>username</i> | Specifies the username. |
| | file <i>filename</i> | Outputs the results to the file that is specified by <i>filename</i> . |
| | <i>vm</i> | (Optional) Shows the virtual memory of the process. |
| | <i>detail</i> | (Optional) Shows the details, such as page fault, virtual memory, and start time of the process. |
| | <i>cont</i> | (Optional) Repeats the command continuously. |

Command Modes Administrator (admin):

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process using-most cpu

This command displays a list of the most CPU-intensive processes.

show process using-most cpu [{*number*} [{file** *filename* | [{**cont**}]}]]**

| Syntax Description | Parameters | Description |
|--------------------|-----------------------------|--|
| | <i>number</i> | Specifies the number of processes to display. The default specifies 5. |
| | file <i>filename</i> | Outputs the results to the file that is specified by <i>filename</i> . |
| | cont | Repeats the command continuously. |

Command Modes Administrator (admin):

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show process using-most memory

This command displays a list of the most memory-intensive processes.

show process using-most memory [{ number }] [{ file filename } | [{ cont }]]

Syntax Description

| Parameters | Description |
|--------------------------------|--|
| <i>number</i> | Specifies the number of processes to display. The default specifies 5. |
| file <i>filename</i> | Outputs the results to the file that is specified by <i>filename</i> . |
| cont | Repeats the command continuously. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show registry

This command displays the contents of the registry.

show registry system component [{name}] [{page}]

Syntax Description

| Parameters | Description |
|------------------|---|
| <i>system</i> | Represents the registry system name. |
| <i>component</i> | Represents the registry component name. |
| <i>name</i> | Represents the name of the parameter to show. |
| page | Displays one page at a time. |

Command Modes

Administrator (admin:)

Usage Guidelines

If the name is “page,” and you want to display the output one page at a time, use the command **show registry system component name page page**

show risdb list

To show all components in a system, enter the wildcard character * in the command: **show registry system ***

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

This example shows the contents of the cm system, dbl/sdi component.

```
admin:show registry cm dbl/sdi
system = cm
  component = dbl/sdi
  tracelevel=127
  enable=1
  outputdebugstringflag=0
  numminutes=1440
  tracefile=/var/log/active/cm/trace/dbl/sdi/dbl.log
  numfiles=250
  numlines=10000
```

show risdb list

This command displays the tables that are supported in the Realtime Information Service (RIS) database.

show risdb list [{file filename}]

Syntax Description

| Parameters | Description |
|--------------------------------|------------------------------------|
| file <i>filename</i> | Outputs the information to a file. |

Command Modes

Administrator (admin:)

Usage Guidelines

The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the filename does not contain the “.” character.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

This command displays a list of all RIS database tables.

```
admin: show risdb list
```

show risdb query

This command displays the contents of the specified RIS tables.

```
show risdb query table1 table2 table3 ...[{file filename}]
```

Syntax Description

| Parameters Description | |
|--------------------------------|------------------------------------|
| <i>table1</i> | Specifies the name of a table. |
| file <i>filename</i> | Outputs the information to a file. |

Command Modes

Administrator (admin:)

Usage Guidelines

The file option saves the information to `platform/cli/filename.txt`. Ensure that the filename does not contain the “.” character.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show samltrace level

This command displays the trace level that is currently configured.

```
show samltrace level
```

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection.

show session maxlimit

show session maxlimit

This command shows the upper limit for concurrent SSH sessions.

show session maxlimit

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show smtp

This command displays the name of the SMTP host.

show snmp

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show stats io

This command displays the IO statistics.

show stats io [{kilo}] [{detail}] [{page}] [{file filename}]

| Syntax Description | Parameters | Description |
|--------------------|---------------|--|
| | kilo | Displays statistics in kilobytes. |
| | detail | Displays detailed statistics on every available device on the system and overrides the kilo option. |
| | page | Displays one page at a time. |

Parameters Description

| | |
|-------------|--|
| file | Outputs the information to a file specified by <i>filename</i> |
| | |

Command Modes

Administrator (admin):

Usage Guidelines

The **file** option saves the information to `platform/cli/filename.txt`. Ensure that the filename does not contain the “.” character.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show status

This command displays basic platform status.

show status**Command Modes**

Administrator (admin):

Usage Guidelines

This command displays the following basic platform status:

- hostname
- date
- timezone
- locale
- product version
- platform version
- CPU usage
- memory and disk usage

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech activesql

show tech activesql

This command displays the active queries to the database taken at one minute intervals as far back as the logs allow.

show tech activesql

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech all

This command displays the combined output of all **show tech** commands.

show tech all [{page}] [{file filename}]

Syntax Description

| Parameters | Description |
|--------------------------------|------------------------------------|
| page | Displays one page at a time. |
| file <i>filename</i> | Outputs the information to a file. |

Command Modes

Administrator (admin:)

Usage Guidelines

The file option saves the information to `platform/cli/filename.txt`. Ensure that the file name does not contain the “.” character

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech ccm_service

This command displays information about all services that can run on the system.

show tech ccm_service**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech database

This command shows information about the database.

show tech database {dump | sessions}**Syntax Description****Parameters Description****dump** Creates a CSV file of the entire database.**sessions** Redirects the session and SQL information of the present session IDs to a file.**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dberrcode

This command displays information (from the database log files) about the error code that is specified.

show tech dberrcode *errorcode***Syntax Description****Parameters Description*****errorcode*** Specifies the error code as a positive integer.**Command Modes**

Administrator (admin:)

Usage Guidelines

If the error code is a negative number, enter it without the minus sign (-).

```
show tech dbhighcpustasks
```

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dbhighcpustasks

This command displays the currently running high cost tasks and high CPU-intensive tasks.

```
show tech dbhighcpustasks
```

Command Modes Administrator (admin):

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dbintegrity

This command displays the database integrity.

```
show tech dbintegrity
```

Command Modes Administrator (admin):

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dbschema

This command displays the database schema in a CSV file.

```
show tech dbschema [{car | cm}]
```

Syntax Description

| Parameters | Description |
|------------|------------------------------|
| car | Represents the car database. |
| cm | Represents the cm database. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dbinuse

This command displays the database in use.

show tech dbinuse [{car | cm}]

Syntax Description
Parameters Description

| | |
|------------|------------------------------|
| car | Represents the car database. |
| cm | Represents the cm database. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dbstateinfo

This command displays the state of the database.

show tech dbstateinfo [{car | cm}]

Syntax Description
Parameters Description

| | |
|------------|------------------------------|
| car | Represents the car database. |
| cm | Represents the cm database. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

show tech devdefaults

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech devdefaults

This command displays the device defaults table.

show tech devdefaults**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech dumpCSVandXML

This command provides detailed information for customer support in the case of a standard upgrade condition.

show tech dumpCSVandXML**Command Modes** Administrator (admin:)**Usage Guidelines** You can get this file in the following ways:

1. Use the `file view activelog cm/trace/db1/xmlcsv.tar` command to view the contents of the file.
2. Use the `file get activelog cm/trace/db1/xmlcsv.tar` command to download the file.
3. Use RTMT: **Trace and Log Central > Collect Files > Cisco Database Cli Output > Install and upgrade log**.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech gateway

This command displays the gateway table from the database.

show tech gateway**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech locales

This command displays the locale information for devices, device pools, and end users.

show tech locales**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech network all

This command displays all network tech information.

show tech network all [{page}] [{search text}] [{file filename}]

| Syntax Description | Parameters | Description |
|--------------------|-----------------------------|--|
| | page | Displays one page at a time. |
| | search <i>text</i> | Searches the output for the string that <i>text</i> specifies. Be aware that the search is case insensitive. |
| | file <i>filename</i> | Outputs the information to a file. |

Command Modes Administrator (admin:)**Usage Guidelines** The **file** option saves the information to *platform/cli/filename.txt*. Ensure that the file name does not contain the “.” character

show tech network hosts

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech network hosts

This command displays information about hosts configuration.

show tech network hosts [{page}] [{search text}] [{file filename}]

| Syntax Description | Parameters | Description |
|--------------------|-----------------------------|--|
| | page | Displays one page at a time. |
| | search <i>text</i> | Searches the output for the string that <i>text</i> specifies. Be aware that the search is case insensitive. |
| | file <i>filename</i> | Outputs the information to a file. |

Command Modes Administrator (admin:)**Usage Guidelines** The **file** option saves the information to *platform/cli/filename.txt*. Ensure that the file name does not contain the “.” character**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech network interfaces

This command displays information about the network interfaces.

show tech network interfaces [{page}] [{search text}] [{file filename}]

| Syntax Description | Parameters | Description |
|--------------------|-----------------------------|--|
| | page | Displays one page at a time. |
| | search <i>text</i> | Searches the output for the string that <i>text</i> specifies. Be aware that the search is case insensitive. |
| | file <i>filename</i> | Outputs the information to a file. |

| | |
|---|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The file option saves the information to <code>platform/cli/filename.txt</code> . Ensure that the file name does not contain the “.” character |
| Requirements | |
| Command privilege level: 0 | |
| Allowed during upgrade: Yes | |
| Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

show tech network resolv

This command displays information about hostname resolution.

show tech network resolv [{page}] [{search text}] [{file filename}]

| Syntax Description | | Parameters Description |
|---------------------------|-----------------------------|--|
| | page | Displays one page at a time. |
| | search <i>text</i> | Searches the output for the string that <i>text</i> specifies. Be aware that the search is case insensitive. |
| | file <i>filename</i> | Outputs the information to a file. |

| | |
|---|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The file option saves the information to <code>platform/cli/filename.txt</code> . Ensure that the file name does not contain the “.” character |
| Requirements | |
| Command privilege level: 1 | |
| Allowed during upgrade: Yes | |
| Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

show tech network routes

This command displays information about network routes.

show tech network routes [{page}] [{search text}] [{file filename}]

show tech network sockets

| Syntax Description | Parameters | Description |
|--------------------|--------------------------------|--|
| | page | Displays one page at a time. |
| | search <i>text</i> | Searches the output for the string that <i>text</i> specifies. Be aware that the search is case insensitive. |
| | file <i>filename</i> | Outputs the information to a file. |

Command Modes Administrator (admin:)

Usage Guidelines The **file** option saves the information to *platform/cli/filename.txt*. Ensure that the file name does not contain the “.” character**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech network sockets

This command displays the list of open sockets.

show tech network sockets{numeric}

| Syntax Description | Parameters | Description |
|--------------------|----------------|---|
| | numeric | Displays the numerical addresses of the ports instead of determining symbolic hosts. This parameter is equivalent to running the Linux shell numeric [-n] command. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech notify

This command displays the database change notify monitor.

show tech notify [search pattern_to_match]

| Syntax Description | Parameters | Description |
|--------------------|---|--|
| | <i>search pattern_to_match</i> | Represents the string that needs to be searched in the command output. |
| Command Modes | Administrator (admin:) | |
| | Requirements | |
| | Command privilege level: 0 | |
| | Allowed during upgrade: Yes | |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

show tech params

This command displays the database parameters.

show tech params {all | enterprise | service}

| Syntax Description | Parameters | Description |
|--------------------|---|--|
| | all | Displays all the database parameters. |
| | enterprise | Displays the database enterprise parameters. |
| | service | Displays the database service parameters. |
| Command Modes | Administrator (admin:) | |
| | Requirements | |
| | Command privilege level: 0 | |
| | Allowed during upgrade: Yes | |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

show tech prefs

This command displays database settings.

show tech prefs

| | |
|---------------|----------------------------|
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 0 |

show tech procedures

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech procedures

This command displays the CAR or CM procedures that are in use for the database.

show tech procedures {car | cm}

| Syntax Description | Parameters Description |
|--------------------|--|
| | car Specifies the CAR procedures. |
| | cm Specifies the CM procedures. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech repltimeout

This command displays the replication timeout.

show tech repltimeout

Command Modes Administrator (admin:)

Usage Guidelines When you increase the replication timeout, ensure that as many servers as possible in a large system are included in the first round of replication setup. If you have the maximum number of servers and devices, set the replication timeout to the maximum value. Be aware that this delays the initial set up of replication to give all servers time to get ready for setup.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech routepatterns

This command displays the route patterns that are configured for the system.

show tech routepatterns

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech routeplan

This command displays the route plans that are configured for the system.

show tech routeplan

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech runtime

This command displays CPU usage information at the time the command is run.

show tech runtime {all | cpu | disk | env | memory} page file *filename*

Syntax Description

| Parameters | Description |
|-------------|--|
| all | Displays all runtime information. |
| cpu | Displays CPU usage information at the time the command is run. |
| disk | Displays system disk usage information. |
| env | Displays environment variables. |

```
show tech sqlhistory
```

| Parameters | Description |
|-----------------|---|
| memory | Displays memory usage information. |
| page | Displays one page at a time. |
| file | Outputs the information to a specified file. |
| <i>filename</i> | Note This option saves the information to platform/cli/<filename>.txt. Ensure that the file name does not contain the "." character. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

show tech sqlhistory

This command prints the history of SQL statements executed.

show tech sqlhistory

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech systables

This command displays the name of all tables in the sysmaster database.

show tech systables

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech system

This command displays all the system information.

show tech system {all | bus | hardware | host | kernel modules | software | tools} {page | file | filename}

| Syntax Description | Parameters | Description |
|--------------------|------------------------|---|
| | all | Displays all the system information. |
| | bus | Displays information about the data buses on the server. |
| | hardware | Displays information about the server hardware. |
| | host | Displays information about the server. |
| | kernel modules | Lists the installed kernel modules. |
| | software | Displays information about the installed software versions. |
| | tools | Displays information about the software tools on the server. |
| | page | Displays one page at a time. |
| | file filename | Outputs the information to a file. This option saves the information to <code>platform/cli/<filename>.txt</code> . Ensure that the file name does not contain the <code>"."</code> character. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech table

show tech table

This command displays the contents of the specified database table.

show tech table *table_name* [*page*]

Syntax Description

Parameters Description

| | |
|-------------------|--|
| <i>table_name</i> | Represents the name of the table to display. |
| <i>page</i> | Displays the output one page at a time. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech triggers

This command displays table names and the triggers that are associated with those tables.

show tech triggers

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tech version

This command displays the version of the installed components.

show tech version [*page*]

Syntax Description

Parameters Description

| | |
|-------------|------------------------------|
| <i>page</i> | Displays one page at a time. |
|-------------|------------------------------|

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show timezone config

This command displays the current timezone settings.

show timezone config

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show timezone list

This command displays the available timezones.

show timezone list [{page}]

| Syntax Description | Parameters | Description |
|--------------------|------------|---|
| | page | Displays the output one page at a time. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

| | |
|-------------------------|--|
| Usage Guidelines | Although the list of available time zones includes Factory , Unified Communications Manager does not support the Factory timezone. |
|-------------------------|--|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show tlstrace

show tlstrace

This command shows the status of TLS trace for a service.

show tlstrace [{service}]

| Syntax Description | Parameters Description |
|----------------------|---|
| | <i>service</i> Represents the TLS tracing status of a service. It is a mandatory parameter. |
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 0 |
| | Allowed during upgrade: Yes |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection |

show tls min-version

This command shows the minimum configured version of Transport Layer Security (TLS) protocol.

show tls min-version

| | |
|----------------------|--|
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 1 |
| | Allowed during upgrade: Yes |
| | Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager |

Example

```
admin:show tls min-version
Configured TLS minimum version: 1.0
```

show tlsv1resumptiontimeout

This command shows the TLS session resumption timeout.

show tlsv1resumptiontimeout

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show trace

This command displays trace information for a particular task.

show trace [{task_name}]

Syntax Description

Parameters Description

task_name Represents the name of the task for which you want to display the trace information.

Command Modes

Administrator (admin:)

Usage Guidelines

If you do not enter a parameter, the command returns a list of available tasks.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

admin: show trace cdps

show ups status

This command shows the current status of the USB-connected APC smart-UPS device and starts the monitoring service if this service is not already started.

show ups status

Command Modes

Administrator (admin:)

Usage Guidelines

This command provides full status only for 7835-H2 and 7825-H2 servers.

show version active**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show version active

This command displays the software version on the active partition.

show version active**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show version inactive

This command displays the software version on the inactive partition

show version inactive**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show vos version

With Unity Connection 12.0(1) and later, Unity Connection supports a specific ISO that is separated from the Cisco Unified CM ISO. However, Unity Connection will provide all the latest VOS changes. To see the VOS version integrated with Unity Connection **show vos version** CLI is introduced.

This command displays the VOS version stored in the active and inactive partitions. If there is no VOS version in the inactive partition, it displays **"VOS version not available"**.

For more information, see "Support for Cisco Unity Connection ISO" section of the *Release Notes for Cisco Unity Connection 12.0(1)* available at <http://www.cisco.com/c/en/us/support/unified-communications/unity-connection/products-release-notes-list.html>

show vos version

Command Modes Administrator (admin:)

Usage Guidelines This command always displays the VOS version in the active partition. If the active partition contains an upgrade, the command also shows the VOS version in the inactive partition.



Note If you are upgrading from Cisco Unity Connection 11.5(1) or earlier version to 12.0(1) or later, the inactive partition does not contain the information of VOS version.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin:show vos version
Active version: 12.0.1.10000-1
Inactive version: VOS version not available
```

show web-security

This command displays the contents of the current web-security certificate.

show web-security

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show webapp session timeout

show webapp session timeout

This command displays the webapp session timeout value, which is the amount of time, in minutes, that can elapse before a web application times out and logs off the user.

show webapp session timeout

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show workingdir

This command retrieves the current working directory for activelog, inactivelog, install, and TFTP.

show workingdir

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

show logins unsuccessful

Use this command to list recent unsuccessful login attempts to the following web applications:

- On Unified Communications Manager
 - Disaster Recovery System
 - Cisco Unified OS Administration
- On IM and Presence Service
 - IM and Presence Disaster Recovery System
 - Unified IM and Presence OS Administration

show logins unsuccessful [number]

Syntax Description**Parameters Description**

number Specifies the number of most recent logins to display. The default is 20.

Command Modes

Administrator (admin)

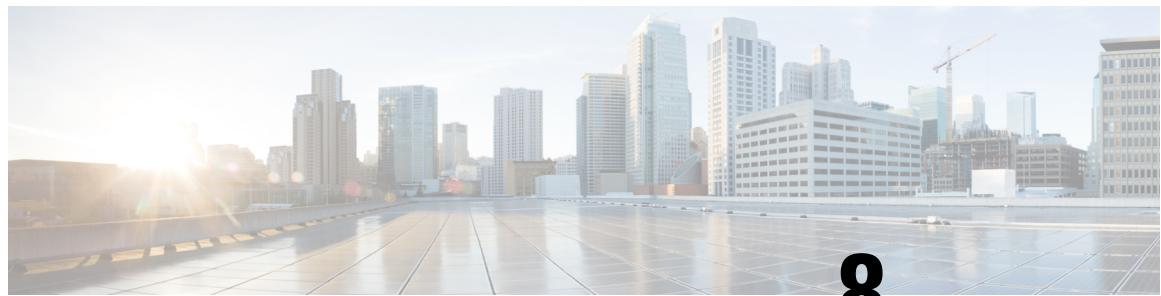
Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to Unified Communications Manager and IM and Presence Service

show logins unsuccessful



CHAPTER 8

Unset Commands

- [unset ipsec policy_group](#), on page 229
- [unset ipsec policy_name](#), on page 229
- [unset network cluster subscriber details](#), on page 230
- [unset network cluster subscriber dynamic-cluster-configuration](#), on page 230
- [unset network dns options](#), on page 231
- [unset network domain](#), on page 231
- [unset network ntp options](#), on page 232
- [unset network ipv6 gateway](#), on page 232
- [unset network ipv6 static_address](#), on page 233

unset ipsec policy_group

This command disables the ipsec policy on the specified group.

unset ipsec policy_group *policy_group*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>policy_group</i> Specifies the group name. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

unset ipsec policy_name

This command disables the ipsec policy with the specified name.

unset network cluster subscriber details

unset ipsec policy_name *policy_name*

Syntax Description

Parameters Description

policy_name Specifies the policy name to disable.

Command Modes

Administrator (admin:)

Usage Guidelines

Enter **ALL** for *policy_name* to disable all policy names.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

unset network cluster subscriber details

This command shows the message that you need to delete a subscriber node from the GUI instead of the command prompt.

unset network cluster subscriber details

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to Unified Communications Manager, IM and Presence Service on Communications Manager, and Cisco Unity Connection

Message to delete the subscriber from GUI

```
admin: unset network cluster subscriber details
Please use the Cisco Unified Communications Manager on the first node.
Navigate to System > Server and click "Find".
    Unable to del: NULL
Executed command unsuccessfully.
```

unsetnetworkclustersubscriberdynamic-cluster-configuration

This command disables Dynamic Cluster Configuration on the publisher. The value of **Dynamic Cluster Configuration** option is set to zero on publisher.

unset network cluster subscriber dynamic-cluster-configuration

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

unset network dns options

This command unsets DNS options.

unset network dns options [{timeout}] [{attempts}] [{rotate}]

Syntax Description

Parameters Description

timeout Sets the wait time before the system considers a DNS query as failed to the default.

attempts Sets the number of DNS attempts to make before the system fails to the default.

rotate Sets the method for selecting a nameserver to the default. This affects how loads are distributed across nameservers.

Usage Guidelines

Running this command causes an automatic system restart.

Command Modes

Administrator (admin:)

Usage Guidelines

You are asked to confirm that you want to execute this command.



Caution

If you continue, the system loses network connectivity temporarily.

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

unset network domain

This command unsets the domain name and restarts the server.

unset network domain

Command Modes

Administrator (admin:)

unset network ntp options

Usage Guidelines You are asked to confirm that you want to execute this command.

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin: unset network domain
cmdSetIp.domain.name.change.warning
Continue (y/n)?
trying to restart system...
Warning: Restart could take up to 5 minutes...
Shutting down Service Manager. Please wait...
```

unset network ntp options

This command unsets the domain name and restarts the server.

unset network ntp options

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

unset network ipv6 gateway

This command unsets the IPv6 gateway on the server.

unset network ipv6 gateway [{reboot}]

Syntax Description

Parameters **Description**

reboot Reboots the server after applying the change.

Note By default, the reboot on the server does not happen.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

unset network ipv6 static_address

This command unsets the IPV6 static address.

unset network ipv6 static_address [{reboot}]

Syntax Description

Parameters Description

reboot Reboots the server after applying the change.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

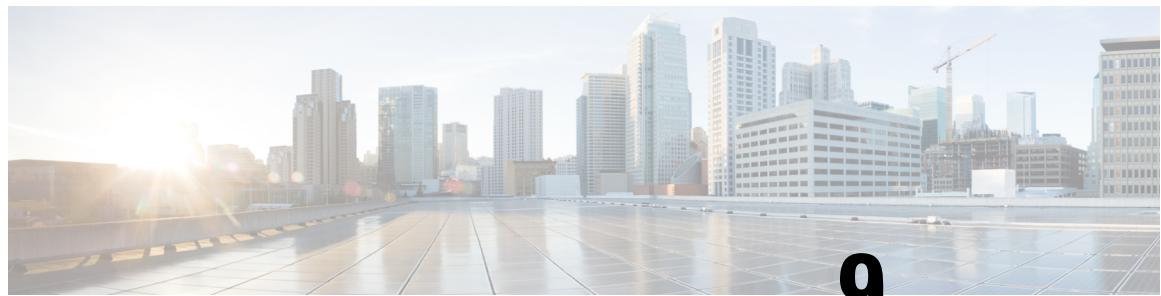
Allowed during upgrade: No

Applies to: Unified Communications Manager, Cisco Unity Connection

Example

```
admin: admin:unset network ipv6 static_address
W A R N I N G
The Server must be rebooted for these changes to take effect.
Please make sure that you reboot this server.
IPv6 static address was removed.
```

```
unset network ipv6 static_address
```



CHAPTER 9

Utils Commands

- [utils auditd, on page 240](#)
- [utils BE6000Mode enable, on page 240](#)
- [utils BE6000Mode disable, on page 241](#)
- [utils BE6000Mode status, on page 241](#)
- [utils branding enable, on page 241](#)
- [utils branding disable, on page 241](#)
- [utils branding status, on page 242](#)
- [utils contactsearchauthentication disable, on page 242](#)
- [utils contactsearchauthentication enable, on page 242](#)
- [utils contactsearchauthentication status, on page 243](#)
- [utils core analyze, on page 243](#)
- [utils core list, on page 244](#)
- [utils capf cert import, on page 244](#)
- [utils capf set keep_alive, on page 244](#)
- [utils capf stale-lsc, on page 245](#)
- [utils create report, on page 245](#)
- [utils create report database, on page 246](#)
- [utils ctl, on page 246](#)
- [utils cuc activate CUSRSP, on page 248](#)
- [utils cuc auto ITL download, on page 248](#)
- [utils cuc cluster activate, on page 249](#)
- [utils cuc cluster deactivate, on page 249](#)
- [utils cuc cluster makeprimary, on page 249](#)
- [utils cuc cluster overwritedb, on page 250](#)
- [utils cuc cluster renegotiate, on page 250](#)
- [utils cuc create report, on page 251](#)
- [utils cuc dbreplication 01_tear_down, on page 251](#)
- [utils cuc dbreplication 02_define_servers, on page 252](#)
- [utils cuc dbreplication 03_define_db_template, on page 253](#)
- [utils cuc dbreplication 04_sync_database, on page 253](#)
- [utils cuc dbreplication reset_all, on page 254](#)
- [utils cuc encryption, on page 255](#)
- [utils cuc hwconfig update, on page 256](#)

- [utils cuc jetty ssl disable](#), on page 257
- [utils cuc jetty ssl enable](#), on page 257
- [utils cuc networking clear_replication](#), on page 258
- [utils cuc networking dscp](#), on page 258
- [utils cuc odbc non-secure enable](#), on page 259
- [utils cuc odbc non-secure disable](#), on page 259
- [utils cuc odbc non-secure status](#), on page 260
- [utils cuc reset password](#), on page 260
- [utils cuc set PinExpiry_PromptTime “Authentication Rule Name”](#), on page 260
- [utils container-engine start](#), on page 261
- [utils container-engine stop](#), on page 261
- [utils container-engine restart](#), on page 261
- [utils container-engine status](#), on page 262
- [utils dbreplication dropadmindb](#), on page 262
- [utils dbreplication forcedatasyncsub](#), on page 263
- [utils dbreplication quickaudit](#), on page 264
- [utils dbreplication rebuild](#), on page 264
- [utils dbreplication repair](#), on page 265
- [utils dbreplication repairreplicate](#), on page 265
- [utils dbreplication repairtable](#), on page 266
- [utils dbreplication reset](#), on page 267
- [utils dbreplication runtimestate](#), on page 267
- [utils dbreplication setprocess](#), on page 268
- [utils dbreplication setreptimeout](#), on page 269
- [utils dbreplication status](#), on page 269
- [utils dbreplication stop](#), on page 270
- [utils imbd_replication replication status](#), on page 271
- [utils diagnose](#), on page 271
- [utils disaster_recovery backup network](#), on page 272
- [utils disaster_recovery cancel_backup](#), on page 272
- [utils disaster_recovery device add network](#), on page 273
- [utils disaster_recovery device delete](#), on page 274
- [utils disaster_recovery device list](#), on page 274
- [utils disaster_recovery estimate_tar_size](#), on page 274
- [utils disaster_recovery history](#), on page 275
- [utils disaster_recovery jschLogs operation](#), on page 275
- [utils disaster_recovery prepare restore pub_from_sub](#), on page 276
- [utils disaster_recovery restore network](#), on page 276
- [utils disaster_recovery schedule add](#), on page 277
- [utils disaster_recovery schedule](#), on page 278
- [utils disaster_recovery schedule delete](#), on page 278
- [utils disaster_recovery schedule disable](#), on page 279
- [utils disaster_recovery schedule list](#), on page 279
- [utils disaster_recovery show_backupfiles](#), on page 279
- [utils disaster_recovery show_registration](#), on page 280
- [utils disaster_recovery status](#), on page 280

- [utils EnhancedSecurityMode disable](#), on page 281
- [utils EnhancedSecurityMode enable](#), on page 281
- [utils EnhancedSecurityMode status](#), on page 281
- [utils filebeat config](#), on page 282
- [utils filebeat disable](#), on page 282
- [utils filebeat enable](#), on page 283
- [utils filebeat status](#), on page 283
- [utils filebeat tls](#), on page 283
- [utils fior](#), on page 284
- [utils fior disable](#), on page 284
- [utils fior enable](#), on page 285
- [utils fior list](#), on page 285
- [utils fior start](#), on page 286
- [utils fior status](#), on page 286
- [utils fior stop](#), on page 286
- [utils fior top](#), on page 287
- [utils fips](#), on page 287
- [utils fips_common_criteria](#), on page 288
- [utils firewall ipv4 debug](#), on page 289
- [utils firewall ipv4](#), on page 290
- [utils firewall ipv4 list](#), on page 290
- [utils firewall ipv4 status](#), on page 291
- [utils firewall ipv6 debug](#), on page 291
- [utils firewall ipv6](#), on page 292
- [utils firewall ipv6 list](#), on page 292
- [utils firewall ipv6 status](#), on page 293
- [utils ha failover](#), on page 293
- [utils ha fallback](#), on page 294
- [utils haproxy set {required|optional|disable} client-auth](#), on page 294
- [utils haproxy set num-threads](#), on page 296
- [utils ha recover](#), on page 298
- [utils ha status](#), on page 298
- [utils ils showpeerinfo](#), on page 299
- [utils import config](#), on page 300
- [utils iostat](#), on page 301
- [utils iothrottle](#), on page 301
- [utils itl reset](#), on page 302
- [utils ipsec restart](#), on page 303
- [utils ldap config](#), on page 303
- [utils managementAgent alarms minpushLevel](#), on page 304
- [utils managementAgent alarms pushfrequency](#), on page 305
- [utils managementAgent alarms pushnow](#), on page 305
- [utils network arp delete](#), on page 305
- [utils network arp set](#), on page 306
- [utils network arp list](#), on page 307
- [utils network capture](#), on page 307

- [utils network capture-rotate, on page 308](#)
- [utils network connectivity, on page 309](#)
- [utils network host, on page 311](#)
- [utils network ipv6 host, on page 311](#)
- [utils network ipv6 traceroute, on page 312](#)
- [utils network ipv6 ping, on page 312](#)
- [utils network ping, on page 312](#)
- [utils network traceroute, on page 313](#)
- [utils network name-service {hosts|services} cache invalidate, on page 313](#)
- [utils ntp auth symmetric-key, on page 314](#)
- [utils ntp auth auto-key, on page 316](#)
- [utils ntp server add, on page 319](#)
- [utils ntp server delete, on page 320](#)
- [utils ntp config, on page 321](#)
- [utils ntp restart, on page 322](#)
- [utils ntp server list, on page 322](#)
- [utils ntp start, on page 322](#)
- [utils ntp status, on page 323](#)
- [utils os kerneldump , on page 323](#)
- [utils os kerneldump ssh, on page 324](#)
- [utils os kerneldump status, on page 325](#)
- [utils os secure , on page 325](#)
- [utils os secure dynamic-policies compile, on page 326](#)
- [utils os secure dynamic-policies list, on page 326](#)
- [utils os secure dynamic-policies load, on page 326](#)
- [utils os secure dynamic-policies remove, on page 327](#)
- [utils os secure dynamic-policies show, on page 327](#)
- [utils os secure dynamic-policies start-recording, on page 328](#)
- [utils os secure dynamic-policies stop-recording, on page 329](#)
- [utils PlatformWebAccess disable, on page 329](#)
- [utils PlatformWebAccess enable, on page 330](#)
- [utils PlatformWebAccess status, on page 330](#)
- [utils processCoreDumps disable, on page 330](#)
- [utils processCoreDumps enable, on page 331](#)
- [utils processCoreDumps status, on page 331](#)
- [utils remote_account create, on page 331](#)
- [utils remote_account disable, on page 332](#)
- [utils remote_account enable, on page 332](#)
- [utils remote_account status, on page 332](#)
- [utils remotesyslog set protocol tcp, on page 333](#)
- [utils remotesyslog set protocol udp, on page 333](#)
- [utils remotesyslog set protocol tls, on page 333](#)
- [utils remotesyslog show protocol, on page 334](#)
- [utils reset_application_ui_administrator_name, on page 334](#)
- [utils reset_application_ui_administrator_password, on page 335](#)
- [utils restore_application_ui_administrator_account, on page 335](#)

- [utils rosters list limited, on page 336](#)
- [utils rosters list full, on page 336](#)
- [utils rosters list watchers, on page 336](#)
- [utils rosters list contacts, on page 337](#)
- [utils rosters delete, on page 337](#)
- [utils scheduled-task disable, on page 337](#)
- [utils scheduled-task enable , on page 338](#)
- [utils scheduled-task list, on page 338](#)
- [utils set urlpattern disable, on page 339](#)
- [utils set urlpattern enable, on page 339](#)
- [utils service, on page 339](#)
- [utils service list, on page 340](#)
- [utils service auto-restart, on page 341](#)
- [utils service start, on page 341](#)
- [utils service stop, on page 342](#)
- [utils snmp config 1/2c community-string, on page 342](#)
- [utils snmp config 1/2c inform, on page 343](#)
- [utils snmp config 1/2c trap, on page 343](#)
- [utils snmp config 3 inform, on page 344](#)
- [utils snmp config mib2, on page 345](#)
- [utils snmp config 3 trap, on page 345](#)
- [utils snmp config 3 user, on page 346](#)
- [utils snmp get, on page 346](#)
- [utils snmp get 1, on page 347](#)
- [utils snmp get 2c, on page 348](#)
- [utils snmp get 3, on page 348](#)
- [utils snmp hardware-agents, on page 349](#)
- [utils snmp test, on page 350](#)
- [utils snmp walk, on page 350](#)
- [utils snmp walk 1, on page 352](#)
- [utils snmp walk 2c, on page 352](#)
- [utils snmp walk 3, on page 353](#)
- [utils soap realtimeservice test, on page 354](#)
- [utils sso, on page 354](#)
- [utils sso recovery-url, on page 355](#)
- [utils system restart, on page 355](#)
- [utils system shutdown, on page 356](#)
- [utils system switch-version, on page 356](#)
- [utils system boot, on page 356](#)
- [utils system upgrade, on page 357](#)
- [utils system upgrade cluster, on page 360](#)
- [utils system enableAdministration, on page 363](#)
- [utils update dst, on page 364](#)
- [utils users validate, on page 364](#)
- [utils vmtools refresh, on page 365](#)
- [utils vmtools status, on page 365](#)

- [utils vmtools switch open, on page 366](#)
- [utils vmtools switch native, on page 366](#)
- [utils system boot status, on page 366](#)
- [utils system upgrade dataexport initiate, on page 367](#)
- [utils system upgrade dataexport status, on page 368](#)
- [utils system upgrade dataexport cancel, on page 368](#)

utils auditd

This command starts, stops, and provides the status of the system auditing service.

utils auditd {enable | disable | status}

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | enable | Enables the collection of audit logs. When enabled, the system monitors and records user actions as well as Linux events such as the creation and removal of users, as well as the editing and deleting of files . |
| | disable | Disables the collection of audit logs. |
| | status | Displays the status of audit log collection. Cisco recommends that you retrieve the audit log by using the Real-Time Monitoring Tool, but you can also retrieve it by using the CLI. |

Command Modes Administrator (admin:)

Usage Guidelines After the service has been enabled, it monitors and logs activity on the system. Be aware that the system auditing service logs a lot of information. Care must be taken not to overfill the disk.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils BE6000Mode enable

Run this command to enable BE6000 mode on Unified Communications Manager.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils BE6000Mode disable

Run this command to disable BE6000 mode on Unified Communications Manager.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unfied Communications Manager

utils BE6000Mode status

Run this command to see the Status of BE6000 mode on CUCM.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unfied Communications Manager

utils branding enable

Run this command to enable branding on this node.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Cisco Unfied Communications Manager, IM and Presence Service, or Cisco Unity Connection.

utils branding disable

Run this command to disable branding on this node.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

utils branding status

Applies to: Cisco Unfiied Communications Manager, IM and Presence Service, or Cisco Unity Connection.

utils branding status

Run this command to see the status of whether branding is enabled or disabled on this node.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Cisco Unfiied Communications Manager, IM and Presence Service, or Cisco Unity Connection.

utils contactsearchauthentication disable

This command disables the secure contact search authentication mode. After this mode is disabled, you need to reset the phone for the changes to take effect.

utils contactsearchauthentication disable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils contactsearchauthentication enable

This command enables the secure contact search authentication mode. After this mode is enabled, reset the phone for the changes to take effect.

utils contactsearchauthentication enable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils contactsearchauthentication status

This command shows whether the system is operating in contact search authentication enable mode or contact search authentication disable mode.

utils contactsearchauthentication status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils core analyze

This command generates a backtrace for a core file, a thread list, and the current value of all CPU registers.

utils core {active | inactive} analyze [core_filename]

| Syntax Description | Parameters | Description |
|--------------------|----------------------|---|
| | active | Specifies an active version |
| | inactive | Specifies an inactive version |
| | <i>core_filename</i> | Specifies the name of the core file from which to generate the stack trace. |

Command Modes Administrator (admin:)

Usage Guidelines This command creates a file of the same name as the core file, with a .txt extension, in the same directory as the core file. After you execute this command on a core file created by cimserver, an unexpected message displays. This message is a known limitation of the command.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils core list

utils core list

This command displays all active or inactive core files.

utils core {active | inactive} list

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils capf cert import

utils capf cert import

Use this command to upload signed phone certificates to your system.

Usage Guidelines You can choose to import your signed certificates through either FTP or TFTP.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils capf set keep_alive

Run this command to set the keep_alive timer for all connections between the Certificate Authority Proxy Function (CAPF) service and endpoints. The system default is 15 minutes.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils capf stale-lsc

utils capf stale-lsc {delete | list}

This command helps you manage your system's stale LSC certificates.

Syntax Description

| Parameters | Description |
|---------------|--|
| delete | Deletes all stale LSC certificates from your system. |
| list | Lists all stale LSC certificates on the system. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils create report

This command creates reports about the server in the platform/log directory.

utils create report {hardware | platform | security}

Syntax Description

| Parameters | Description |
|-----------------|---|
| hardware | Creates a system report that contains disk array, remote console, diagnostic, and environmental data. |
| platform | Collects the platform configuration files into a TAR file. |
| security | Collects the diagnostic reports and creates a TAR file that you can download for troubleshooting purposes. You can retrieve this file with the file get command. |

Command Modes

Administrator (admin:)

Usage Guidelines

You are prompted to continue after you enter the command.

After you create a report, use the command **file get activelog platform/log/filename** command, to get the report. where *filename* specifies the report filename that displays after the command completes.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils create report database

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils create report database

This command collects all log files that are needed for database troubleshooting.

utils create report {hardware | platform | security}

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils ctl

utils ctl {set-cluster mixed-mode | set-cluster non-secure-mode | update CTLfile}

This command changes the cluster security mode or updates the CTL file in each of the nodes.

| Syntax Description | Parameters | Description |
|--------------------|------------------------------------|---|
| | set-cluster mixed-mode | <p>Updates the CTL file and sets the cluster to mixed mode (db secure mode is set to 1). If the cluster is already in mixed mode, this command shows that Unified Communications Manager is in mixed mode and Autoregistration is active. You need to confirm your action.</p> <p>Note To enable mixed-mode, ensure that the Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.</p> |
| | set-cluster non-secure-mode | <p>Updates the CTL file and set the cluster to non-secure mode. If the cluster is already in mixed mode, this command shows that Unified Communications Manager is in non-secure mode.</p> |
| | update CTLfile | <p>Updates the CTL file in each of the nodes of the cluster.</p> <p>Note To update the CTLfile in mixed-mode, ensure that the Unified Communications Manager is registered with the Cisco Smart Software Manager or Cisco Smart Software Manager satellite and the Registration Token received from the Smart account or Virtual account has Allow export-controlled functionality enabled while registering with this cluster.</p> |

| | |
|-------------------------|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | The CLI must be executed on the publisher. On all other nodes, this CLI command is disabled. |
| Note | After you regenerate the CTL file, you must restart CallManager and TFTP services across the cluster. |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager.

utils ctl reset localkey

This command is used to regenerate the CTL file and sign it with the secondary SAST role (CallManager). Use this command when the ITLRecovery certificate that was used to sign the original CTL file has changed and the endpoints are locked out.

utils ctl reset {localkey}

| | |
|---------------------------|---|
| Syntax Description | localkey Generates a new CTL file, updates the CTL file on the publisher. The command signs the CTLfile with CallManager key. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | |
| Note | <ul style="list-style-type: none"> • You must run this command on the Unified Communications Manager publisher node. • After the endpoints receive the new CTL file, which is signed by CallManager Key and contains the new ITLRecovery certificate, execute the CTL update command (utils ctl update CTLFile) again to sign it with the ITLRecovery certificate. The CTL file is regenerated but signed by the new ITLRecovery certificate, which is now trusted by the endpoint. |
| Requirements | |
| Command privilege level: | 4 |
| Allowed during upgrade: | No |
| Applies to: | Unified Communications Manager |

utils cuc activate CUSRVS

utils cuc activate CUSRVS

This command converts the standalone Cisco Unity Connection server to Cisco Unity Connection SRSV server.

utils cuc activate CUSRVS

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc auto ITL download

This command allows Unity Connection to disable the functionality of automatically downloading CallManager certificate for Cisco Unity Connection.

utils cuc auto ITL download { enable | disable | status }

Syntax Description

| Parameters | Description |
|------------|---|
| enable | Enables the functionality of automatically downloading the CallManager certificates on port-group reset. By default, the functionality is enabled. |
| disable | Disables the functionality of automatically downloading the CallManager certificates. When disabled, you need to upload the certificates manually. |
| status | Displays the status of the functionality. |



Note

In case of a cluster, the CLI commands are executed only on publisher server.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Cisco Unity Connection

Example

```
admin:utils cuc auto ITL download enable  
After successful execution, Unity Connection will download trust list from the TFTP server automatically.
```

For this, you must do the following:

1. Configure TFTP server for Next Generation enabled port groups through Cisco Unity Connection Administration
2. Restart the Connection Conversation Manager on all nodes in the cluster

Auto downloading of ITL enabled successfully

utils cuc cluster activate

This command activates this server in a Cisco Unity Connection cluster.

utils cuc cluster activate

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc cluster deactivate

This command deactivates this server in a Cisco Unity Connection cluster.

utils cuc cluster deactivate

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc cluster makeprimary

This command forces the specified server to take the primary server status in a Cisco Unity Connection cluster.

utils cuc cluster overwritedb

utils cuc cluster makeprimary

| Syntax Description | Parameters Description |
|----------------------|---|
| | server Specifies the name of the server to take the primary server status in a Cisco Unity Connection cluster. |
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 1 |
| | Allowed during upgrade: Yes |
| | Applies to: Cisco Unity Connection |

utils cuc cluster overwritedb

This command overwrites the data on the server with the data on the other server in a Cisco Unity Connection cluster.

utils cuc cluster overwritedb

| | |
|-------------------------|--|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | This command overwrites the database on the server on which you run this command with the database from the other server in the Connection cluster. Replication restarts after the database is overwritten. This method is used when you restore one server from a backup and must copy the restored data to the other server. |
| | Requirements |
| | Command privilege level: 1 |
| | Allowed during upgrade: Yes |
| | Applies to: Cisco Unity Connection |

utils cuc cluster renegotiate

This command creates a cluster relationship with the publisher server in a Connection cluster after the server was replaced or the Connection was reinstalled on the publisher server. This command overwrites all data on the publisher server with data from the subscriber server and initializes replication between the servers.

utils cuc cluster renegotiate

| | |
|-------------------------|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | Run this command on the subscriber server in a Connection cluster to set up a trust with a publisher server that has been replaced or on which Connection has been reinstalled. |

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

utils cuc create report

This command collects data that is helpful to technical support staff for troubleshooting the system. Data collected includes version information, cluster status, service information, database information, trace files, log files, disk information, memory information, and restart information.

utils cuc create report

Command Modes

Administrator (admin:)

Usage Guidelines

After the command completes, detailed information gets saved in a .zip file, and the location of the zip file displays. Use the **file get** command to move the file to a computer on which you can uncompress the file and view the contents.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only

Example

```
admin: utils cuc create report
Getting unity connection version. Please wait...Done
Getting cluster status. Please wait...Done
Getting service information. Please wait...Done
Getting installed locales. Please wait...Done
Getting database schema version. Please wait...Done
Getting database integrity. Please wait...Done
Getting database diagnostic log. Please wait...Done
Getting database message log. Please wait...Done
Getting trace files. Please wait...Done
Getting log files. Please wait...Done
Getting platform status. Please wait...Done
Compressing 75 files. Please wait...Done
Output is in file: cuc/cli/systeminfo_080318-140843.zip
To free disk space, delete the file after copying it to another computer
```

utils cuc dbreplication 01_tear_down

This command breaks the replication and connectivity between two Unity Connection servers in a cluster. Running this command on both the servers ensures ideal cleanup before establishing a good replication between the servers.

utils cuc dbreplication 02_define_servers

utils cuc dbreplication 01_tear_down

Command Modes

Administrator (admin:)

Usage Guidelines

In case of long Unity Connection database CDR queue buildup, this command cleans the buildup for providing clean ground to establish server connectivity and replication between the two servers in the cluster.



Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication 02_define_servers

This command establishes the network connectivity between the two Unity Connection servers in a cluster.

utils cuc dbreplication 02_define_servers

Command Modes

Administrator (admin:)

Usage Guidelines

You can use this command to track and report the CDR traffic from one server to another in a Unity Connection cluster. During SBR process, this command helps in defining the roles of the two server in a cluster.



Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.



Note You should run this command on the server that has obsolete data in a Unity Connection cluster.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication 03_define_db_template

This command creates the replication record of the set of tables in Unity Connection databases for replication synchronization. This command also negotiates the table templates of Unity Connection database on which the replication scheme needs to be established.

utils cuc dbreplication 03_define_db_template

Command Modes

Administrator (admin:)

Usage Guidelines

This command lists all the tables and defines templates on basis of which the data is negotiated and synchronized between the two servers in a Unity Connection cluster.



Note It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication 04_sync_database

This command synchronizes the database from the remote server to the server on which the command is executed.

utils cuc dbreplication 04_sync_database

```
utils cuc dbreplication reset_all
```

Command Modes

Administrator (admin:)

Usage Guidelines

You should run this command on the server that has obsolete data in a Unity Connection cluster to copy the recent data from the remote server on the current server.



Note

It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc dbreplication reset_all

This command performs all the tasks, such as tear down and defining servers required to reset database replication between the two servers in a Unity Connection cluster.

```
utils cuc dbreplication reset_all
```

Command Modes

Administrator (admin:)

Usage Guidelines

This command executes the following commands sequentially to successfully reset database replication between the two servers in a Unity Connection cluster:

- utils cuc dbreplication01_tear_down
- utils cuc dbreplication 02_define_servers
- utils cuc dbreplication 03_define_db_template
- utils cuc dbreplication 04_sync_database

**Note**

It is recommended to :

- Take the system backup before running the command.
- Collect the screen log information along with command line logs if the command fails and escalate it to Cisco TAC.
- Ensure that only Cisco TAC runs the command.
- Run the command on the server with obsolete data as the synchronization process deletes the data that clashes with the information on the other server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc encryption

This command enables, disables and provides the status of the encryption on Cisco Unity Connection.

utils cuc encryption { enable | disable | status }

Syntax Description

| Parameters | Description |
|------------|--|
| enable | Enables the encryption on Unity Connection. When enabled, Unity connection allows you to use the security features. |
| disable | Disables the encryption on Unity Connection. When disabled, you can not use the security features in Unity Connection. |
| status | Displays the encryption status of the Unity Connection. |

Usage Guidelines

When you enable the encryption on Unity Connection, make sure the following:

- The Cisco Unity Connection is registered with Cisco Smart Software Manager (CSSM) or Cisco Smart Software Manager satellite.
- Export Control Functionality is enabled for the product.

For more information on how to register and enable the Export Control Functionality for Cisco Unity Connection, see "Configuring Cisco Smart Software Licensing in Unity Connection" section of "Managing Licenses" chapter of *Install, Upgrade and Maintenance Guide for Cisco Unity Connection Release 12.x* available at

https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/install_upgrade/guide/b_12xcuciumg.html.

**Note**

In case of cluster, the CLI is executed only on publisher server.

utils cuc hwconfig update

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Cisco Unity Connection

Example

```
admin:utils cuc encryption enable
After successful execution, restart the following services on all nodes in the cluster

1.Connection Conversation Manager
2.Connection IMAP Server

Do you want to proceed (yes/no)? yes
Encryption enabled successfully
```

utils cuc hwconfig update

This CLI command updates the configuration dependencies of Connection Notifier service when the virtual hardware configuration that is vCPU or vRAM are modified as per supported OVA configurations.

For supported OVA configurations, see [Virtualization for Cisco Unity Connection \(CUC\)](#).

utils cuc hwconfig update

Command Modes Administrator (admin:)

Usage Guidelines

1. You should execute this CLI on Unity Connection node after performing the hardware configuration changes on virtual machines. Configuration applies to below OVA changes.
 - 4vCPU 6GB vRAM configuration is increased to 7vCPU 10GB vRAM.
 - 7vCPU 8GB vRAM configuration is increased to 7vCPU 10GB vRAM.
2. In case of cluster, this CLI should be executed on both nodes.
3. Restart Connection Notifier service on primary node of cluster after successful configuration changes.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Cisco Unity Connection.

utils cuc jetty ssl disable

This command allows you to set the status of SSL (Disabled) on the Jetty Server for notifications.

utils cuc jetty ssl disable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: utils cuc jetty ssl disable
```

```
After successful execution of this command restart of Jetty server is required, which will
result in loss of current event subscriptions. Are you sure?
Enter (yes/no)? yes
```

```
Command completed successfully.
Please restart Connection Jetty Service.
In case of cluster, run this command on the other node also.
```

utils cuc jetty ssl enable

This command allows you to enable the SSL on the Jetty Server for notifications.

utils cuc jetty ssl enable

Usage Guidelines When you enable the SSL on the Jetty server, make sure the following:

- You are using the Restricted version of Cisco Unity Connection.
- The encryption is enabled on the Cisco Unity Connection.



Note

In Evaluation Mode, you are not allowed to run the CLI command.

For more information, see "Cisco Unity Connection- Restricted and Unrestricted Version" chapter of Security Guide for Cisco Unity Connection Release 12.x available at
https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/security/b_12xcucsecx.html.

Command Modes Administrator (admin:)

```
utils cuc networking clear_replication
```

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection

Example

```
admin: utils cuc jetty ssl enable
```

```
After successful execution of this command restart of Jetty server is required, which will
result in loss of current event subscriptions. Are you sure?
Enter (yes/no)? yes
```

Command completed successfully.

Please restart Connection Jetty Service.

In case of cluster, run this command on the other node also.

utils cuc networking clear_replication

This command stops all Digital Networking replication activities on the server.

utils cuc networking clear_replication

Command Modes

Administrator (admin:)

Usage Guidelines

This command stops the Connection Digital Networking Replication Agent and Connection SMTP service, deletes the drop, queue, and pickup replication folders, clears the status of in-progress directory pushes to or pulls from this server, and restarts the Connection Digital Networking Replication Agent and Connection SMTP service. Depending on the size of the replication folders, this operation may take several minutes.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Cisco Unity Connection

utils cuc networking dscp

This command causes Connection either to start or to stop including a DSCP value of 18 in packets sent between the Connection servers in a cluster, so a router configured to prioritize packets based on their DSCP value can prioritize Connection data and voice messages.

utils cuc networking dscp {on | off}

Syntax Description

Parameters Description

| | |
|-----------|--|
| on | Causes Connection to start including a DSCP value of 18 packets sent over the network. |
|-----------|--|

| Parameters | Description |
|------------|--|
| off | Causes to stop including a DSCP value of 18 in packets sent over the network. 18 is the default value. |

Command Modes Administrator (admin:)

Usage Guidelines This command makes the DSCP value available in the packets being passed between the Connection servers in a cluster. For the information to be used, you must configure the router. The command lets you control whether a DSCP value is included in outgoing packets, but you can not change the value.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only

utils cuc odbc non-secure enable

Use this CLI command to enable the non-secure port 20532 on the node. By default port 20532 is enabled.

utils cuc odbc non-secure enable

Command Modes Administrator (admin:)

Usage Guidelines In case of cluster, this CLI should be executed on both the nodes.

Requirements

Command privilege level: 4

Applies to: Cisco Unity Connection.

utils cuc odbc non-secure disable

Use this CLI command to disable the non-secure port 20532 on the node.

utils cuc odbc non-secure disable

Command Modes Administrator (admin:)

Usage Guidelines In case of cluster, this CLI should be executed on both nodes.

Requirements

Command privilege level: 4

Applies to: Cisco Unity Connection.

utils cuc odbc non-secure status

utils cuc odbc non-secure status

Use this CLI command to see the status of non-secure odbc port whether it is enabled or disabled on the node.

utils cuc odbc non-secure status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Cisco Unity Connection.

utils cuc reset password

This command resets the password for a specified user account. If Connection locked the account because of too many failed sign-in attempts, this command also unlocks the account.

utils cuc reset password

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Cisco Unity Connection only

Example

```
admin: utils cuc reset password jdoe
Enter password:
Re-enter password:
jdoe
07/29/2008 12:41:14.704 : Update SUCCESSED
```

utilscucsetPinExpiry_PromptTime“AuthenticationRuleName”

This Command enables the Cisco Unity Connection telephone user interface (touchtone conversation) PIN feature and allows you to update the time interval during when the conditional expiry warning prompt will be played.

Requirements

If the value is set to:

- 0: disabled

- 1: enabled
 - Enter the time interval

For more information on utilscuc set PinExpiry_PromptTime "Authentication Rule Name" CLI command, see the Cisco Unity Connection telephone user interface (touchtone conversation) PIN section in Release Notes for Cisco Unity Connection 10.0(1).

utils container-engine start

This command starts the docker engine.

utils container-engine start

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager and Cisco Unity Connection.

utils container-engine stop

This command stops the container engine.

utils container-engine stop

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager and Cisco Unity Connection.



Note

All the containers will be undeployed.

utils container-engine restart

This command restarts the container engine.

utils container-engine status

utils container-engine restart

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager and Cisco Unity Connection.

utils container-engine status

This command shows the containers and its states on the server when container-engine is running. Additionally displays PIDs and usage of CPU, MEM, I/O for running containers.

utils container-engine status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager and Cisco Unity Connection.

utils dbreplication dropadmindb

This command drops the Informix syscdr database on any server in the cluster.

utils dbreplication dropadmindb

Command Modes Administrator (admin:)

Usage Guidelines You should run this command only if database replication reset or cluster reset fails and replication cannot be restarted.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication forcedatasyncsub

This command forces a subscriber server to have its data restored from data on the publisher server.

utils dbreplication forcedatasyncsub *nodename* [offloadpub] [timeoutvalue]

Syntax Description

Parameters Description

nodename Specifies a particular subscriber server to have its data restored from data on the publisher server. Enter **all** to restore data on all subscriber servers.

offloadpub Minimizes the usage of the publisher server during the forcedatasyncsub process.

Note Adding this option increases the time taken for forcedatasyncsub to finish

timeoutvalue Specifies the recovery timeout value for each node in minutes (should be greater than the default timeout).

Default: 40 minutes.

Command Modes

Administrator (admin):

Usage Guidelines

Use this command only after you have run the **utils dbreplication repair** command several times, but the **utils dbreplication status** command still shows non-dynamic tables that are not in sync



Note

Do not run this command if only dynamic tables are out of sync; dynamic tables can be out of sync during normal system operation.

You can only run this command from the publisher server. Enter **all** to force sync on all subscriber servers in the cluster. If only one subscriber server is out of sync, use the ***nodename*** parameter.



Note

This command erases all existing data on the subscriber server and replaces it with the database from the publisher server. This erasure makes it impossible to determine the root cause for the subscriber server tables going out of sync.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication quickaudit

utils dbreplication quickaudit

This command runs a quick database check on selected content on dynamic tables.

utils dbreplication quickaudit {*nodename* | **all}**

Syntax Description

Parameters Description

nodename Specifies the node on which the quick audit should be run.

all Causes the audit to be run on all nodes

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication rebuild

This command is used to set up database replication across the cluster and runs the following commands on the specified nodes:

- **utils dbreplication stop**
- **utils dbreplication dropadmindb** or **dropadmindbforce**
- **utils dbreplication reset**

utils dbreplication rebuild {*[nodename]* | **all}**

Syntax Description

Parameters Description

nodename Specifies the node or nodes on which database replication will be rebuilt.

all Specifies that database replication will be rebuilt on all nodes in the cluster.

Command Modes

Administrator (admin:)

Usage Guidelines



Caution

This command can affect performance of other nodes in your cluster. We recommend that you run this command during a system maintenance window.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication repair

This command repairs database replication.

utils dbreplication repair {nodename | all}

Syntax Description

Parameters Description

nodename Specifies a particular subscriber server for data repair.

all Causes data repair to take place on all subscriber servers.

Command Modes

Administrator (admin:)

Usage Guidelines

If the command **utils dbreplication status** shows that servers are connected but one or more tables have data that is out of sync, the **utils dbreplication repair** repairs the data on the subscriber servers so that the data is in sync with the data on the publisher server.

Specify **all** to repair all nodes in the cluster, or if only one subscriber server is out of sync, specify the *nodename* parameter.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication repairreplicate

This command repairs mismatched data between cluster nodes and changes the node data to match the publisher data.

utils dbreplication repairreplicate replicatename [{nodename | all}]

Syntax Description

Parameters Description

replicatename Specifies the replicate to repair.

nodename Specifies the node on which to repair replication.

utils dbreplication repairable

| Parameters | Description |
|------------|--|
| all | Specifies to fix replication on all nodes. |

Command Modes**Usage Guidelines**

Note This command can be executed on the publisher.



Note This command does not repair replication setup

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication repairable

This command repairs mismatched data between cluster nodes and changes the node to match the publisher data.

utils dbreplication repairable *tablename* [{*nodename* | **all}]**

Syntax Description

| Parameters | Description |
|------------------|--|
| <i>tablename</i> | Specifies the table to repair |
| <i>nodename</i> | Specifies the node on which to repair replication. |
| all | Specifies to fix replication on all nodes. |

Command Modes**Usage Guidelines**

Note This command does not repair replication setup.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication reset

This command resets and restarts database replication. You can use this command to rebuild replication when the system has not set up replication properly.

utils dbreplication reset {nodename | all}

| Syntax Description | Parameters | Description |
|--------------------|-----------------|---|
| | <i>nodename</i> | Specifies a particular subscriber server to on which to have replication rebuilt. |
| | all | Specifies that all subscriber servers in the cluster have replication rebuilt. |

Command Modes Administrator (admin:)

Usage Guidelines This command is the best option to use when servers show an RTMT state of 4. If only one subscriber server shows an RTMT state of 4, you may reset that server by specifying the *hostname* parameter. To reset the entire cluster, use the **all** parameter.



Tip

Before you run this command, first run the command **utils dbreplication stop** on all subscriber servers that are reset and then on the publisher server.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication runtimestate

This command monitors progress of the database replication process and provides replication state in the cluster.

utils dbreplication setprocess

utils dbreplication runtimestate *nodename*

Syntax Description

Parameters Description

nodename Specifies the node to monitor.

Command Modes

Administrator (admin:)

Usage Guidelines

If you provide a node name, the system provides the replication state from the context of the selected node.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication setprocess

This command improves replication performance of clusters that have nodes separated by WANs with delay (Clustering over WAN configuration).

utils dbreplication setprocess [*process*]

Syntax Description

Parameters Description

process The new database replication . Ensure that the value is between 1 and 40.

Default value: 1

Command Modes

Administrator (admin:)

Usage Guidelines



Caution

Setting the PROCESS option to near maximum consumes more system resources.

Changes made to this setting after an upgrade but before the switch-over to the new version will need to be manually re-applied.

Requirements

Command privilege level: 1

Allowed during upgrade: No

utils dbreplication setrepltimeout

This command sets the timeout for database replication on large clusters.

utils dbreplication setrepltimeout *timeout*

Syntax Description

Parameters Description

timeout The new database replication timeout, in seconds. Ensure that the value is between 300 and 3600.
Default value: 300 (5 minutes)

Command Modes

Administrator (admin:)

Usage Guidelines

After the first subscriber server requests replication with the publisher server, the system sets this timer. After the timer expires, the first subscriber server, plus all other subscriber servers that requested replication within that time period, begin data replication with the publisher server in a batch. If you have several subscriber servers, batch replication is more efficient than individual server replication. For large clusters, you can use the command to increase the default timeout value, so that more subscriber servers are included in the batch.



Tip

Cisco recommends that you restore this value back to the default of 300 (5 minutes) after you finish upgrading the entire cluster, and the subscriber servers have successfully set up replication.



Note

After you upgrade the publisher server and restart it on the upgraded partition, you should set this timer value before you switch the first subscriber server to the new release. After the first subscriber server requests replication, the publisher server sets the replication timer based on the new value.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils dbreplication status

This command shows the status of database replication and indicates whether the servers in the cluster are connected and the data is in sync.

utils dbreplication status {all | node | replicate}

utils dbreplication stop

| Syntax Description | Parameters Description |
|-------------------------|--|
| | all Specifies to show the status of all servers. |
| | node Specifies the node for which to show status. |
| | replicate Specifies the replicate for which to show status. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines |  <p>Note You should run this command only on the first node (publisher server) of a cluster.</p> |
| | Requirements |
| | Command privilege level: 0 |
| | Allowed during upgrade: No |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection |

utils dbreplication stop

This command stops the automatic setup of database replication. Run this command on subscriber and publisher servers before executing the CLI command **utils dbreplication reset**. You can run this command on the subscriber servers simultaneously, before you run it on the publisher server.

utils dbreplication stop {nodename | all}

| Syntax Description | Parameters Description |
|----------------------|---|
| | nodename Specifies the name of the node on which to stop the automatic setup of database replication. |
| | all Stops database replication on all nodes. |
| Command Modes | Administrator (admin:) |
| | Requirements |
| | Command privilege level: 1 |
| | Allowed during upgrade: No |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection |

utils imdb_replication replication status

This command validates that In Memory Database (IMDB) replication between the node pairs in each subcluster of the deployment has run correctly.

The command performs writes and reads on IMDB tables in each relevant Datastore using a utility from the calling IM and Presence Service node.

```
utils imdb_replication status
```

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

| | |
|-------------------------|--|
| Usage Guidelines | For the utility to run successfully, ports 6603, 6604, and 6605 must be opened on any firewalls that are configured between the nodes on the IM and Presence Service clusters. |
|-------------------------|--|

This is not required for the normal operation of the IMDB.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: IM and Presence Service

utils diagnose

This command enables you to diagnose and attempt to automatically fix system problems.

```
utils diagnose { fix | list | test | version } [module_name]
```

```
utils diagnose { module } [module_name] [container_name]
```

| Syntax Description | Parameters | Description |
|--------------------|--------------------|---|
| | fix | Runs all diagnostic commands and attempts to fix problems. |
| | hcs | Lists all the diagnostic commands available for HCS services. |
| | list | Lists all available diagnostic commands. |
| | module | Runs a single diagnostic command or group of commands and attempts to fix problems. |
| | test | Runs all diagnostic commands but does not attempt to fix problems. |
| | version | Displays the diagnostic framework version. |
| | <i>module_name</i> | Specifies the name of a diagnostics module. |

utils disaster_recovery backup network

| Parameters | Description |
|-----------------------|--|
| <i>container_name</i> | Specifies the name of container. This is applicable only for the module parameter. |
| Note | Specify the container name, it runs the diagnostic module inside the container, if containers are running. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 0 for **version** and 1 for all other parameters

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery backup network

Displays information about the backup files that are stored on a remote server.

utils disaster_recovery backup network [featurelist][path][servername][username]

| Syntax Description | Parameters | Description |
|--------------------|----------------------|--|
| | <i>[featurelist]</i> | Specifies a list of features to back up, separated by commas. |
| | <i>[path]</i> | Represents the location of the backup files on the remote server. |
| | <i>[servername]</i> | Represents the IP address or hostname of the server where you stored the backup files. |
| | <i>[username]</i> | Represents the username that is needed to log in to the remote server. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

| | |
|-------------------------|--|
| Usage Guidelines | The system prompts you to enter the password for the account on the remote server. |
|-------------------------|--|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery cancel_backup

This command cancels the ongoing backup.

utils disaster_recovery cancel_backup [confirm]

| | |
|---|--|
| Command Modes | Administrator (admin): |
| Usage Guidelines | After you enter the command, you must confirm that you want to cancel the backup. Enter Y to cancel the backup or any other key to continue the backup. |
| Requirements | |
| Command privilege level: 1 | |
| Allowed during upgrade: Yes | |
| Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection | |

Example

```
admin: utils disaster_recovery cancel_backup yes
 Cancelling backup...
 Backup cancelled successfully.
```

utils disaster_recovery device add network

This command adds the backup network device.

utils disaster_recovery device add network *devicename path server_name/ip_address username [Number_of_backups]*

| Syntax Description | Parameters | Description |
|--------------------|-------------------------------|--|
| | <i>devicename</i> | Specifies the name of the backup device to be added (mandatory). |
| | <i>path</i> | Specifies the path to retrieve the backup device (mandatory). |
| | <i>server_name/ip_address</i> | Specifies the hostname or IP address of the server where the backup file is stored (mandatory). |
| | <i>username</i> | Specifies the userid required to connect to the remote machine (mandatory). |
| | <i>[Number_of_backups]</i> | Specifies the number of backups to store on the Network Directory (default 2). This parameter is optional. |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin): |
| Requirements | |

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery device delete

Example

```
admin: utils disaster_recovery device add network networkDevice /root 10.77.31.116 root 3
```

utils disaster_recovery device delete

This command deletes the specified device.

utils disaster_recovery device delete
*device_name**

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery device list

Displays the device name, device type, and device path for all the backup devices.

utils disaster_recovery device list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery estimate_tar_size

This command provides the estimated size of last successful backup from SFTP or local device.

utils disaster_recovery estimate_tar_size **utils disaster_recovery device list**

Syntax Description
Parameters Description

featurelist Specifies a list of features to back up, separated by commas.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery history

This command displays the history of previous backups and restores.

utils disaster_recovery history *[operation]*

Syntax Description
Parameters Description

operation Specifies backup or restore.

Command Modes

Administrator (admin:)

Requirements

Command privilege level:

Allowed during upgrade:

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery history backup
Tar Filename: Backup Device: Completed On: Result: Backup Type: Features Backed Up:
2009-10-30-14-53-32.tar TAPE Fri Oct 30 14:55:31 CDT 2009 ERROR MANUAL
2009-12-10-10-30-17.tar TAPE Thu Dec 10 10:35:22 CST 2009 SUCCESS MANUAL CDR_CAR,CCM
```

utils disaster_recovery jschLogs operation

This command enables and disables the detailed JSch logging.

utils disaster_recovery prepare restore pub_from_sub

utils disaster_recovery jschLogs operation [operation]

Syntax Description

Parameters Description

operation Specifies the name of operation—enable or disable.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery prepare restore pub_from_sub

This command handles the tasks to prepare for restore of a publisher node from a subscriber node.



Note

This command is applicable only when a publisher node is rebuilt and restored from the subscriber node database. A specific procedure is used for restore instead of restoring the data from the remote backup source. After a publisher node is rebuilt, you must use this command prior to the insertion of process node information.

utils disaster_recovery prepare restore pub_from_sub

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery restore network

This command restores a remote server. You must restore the Unified Communications Manager publisher node before you restore subscriber nodes in the same cluster. If you are restoring IM and Presence Service nodes, you must restore the database publisher node before you restore subscriber nodes in the same cluster.

utils disaster_recovery restore network restore_server tarfilename devicename

| Syntax Description | Parameters | Description |
|--------------------|-----------------------|---|
| | <i>restore_server</i> | Specifies the hostname of the remote server that you want to restore. |
| | <i>tarfilename</i> | Specifies the name of the file to restore. |
| | <i>devicename</i> | Specifies the name of the device on which to restore files. |

| Command Modes | Administrator (admin:) |
|---------------|------------------------|
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule add

This command adds the configured schedules.

utils disaster_recovery schedule add *schedulename devicename featurelist datetime frequency*

| Syntax Description | Parameters | Description |
|--------------------|---------------------|--|
| | <i>schedulename</i> | Represents the name of the scheduler (mandatory). |
| | <i>devicename</i> | Represents the name of the device for which scheduling is done (mandatory). |
| | <i>featurelist</i> | Represents the comma-separated feature list to back up (mandatory). |
| | <i>datetime</i> | Represents the date when the scheduler is set (mandatory). Format specified (yyyy/mm/dd-hh:mm) 24-hr clock. |
| | <i>frequency</i> | Represents the frequency at which the schedule is set to take a backup. Examples: once, daily, weekly and monthly. |

| Command Modes | Administrator (admin:) |
|---------------|------------------------|
|---------------|------------------------|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule

utils disaster_recovery schedule

This command enables or disables the specified schedule.

utils disaster_recovery schedule {enable | disable} [schedulename]

Syntax Description

| Parameters | Description |
|---------------------|---------------------------------------|
| enable | Enables the specified schedule. |
| disable | Disables the specified schedule. |
| <i>schedulename</i> | Represents the name of the scheduler. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level:1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery schedule enable schedule1
Schedule enabled successfully.
```

utils disaster_recovery schedule delete

This command deletes the configured schedules.

utils disaster_recovery schedule delete *schedulename*

Syntax Description

| Parameters | Description |
|---------------------|--|
| <i>schedulename</i> | Represents the name of the schedule that is to be deleted. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule disable

This command disables the configured schedules.

utils disaster_recovery schedule disable *schedulename*

Syntax Description

Parameters Description

schedulename Represents the name of the schedule that is to be disabled.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery schedule list

Displays the schedules that are configured.

utils disaster_recovery schedule list

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
admin: utils disaster_recovery schedule list
schedule name device name Schedule Status
-----
schedule1      device 1      enabled
schedule2      device 2      disabled
```

utils disaster_recovery show_backupfiles

This command retrieves the information of backup files, which are available at storage location.

utils disaster_recovery show_registration

utils disaster_recovery show_backupfiles *devicename*

Syntax Description

Parameters Description

devicename Represents the name of the device to show backup files at the storage location.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery show_registration

This command displays the registered features and components on the specified server.

utils disaster_recovery show_registration *hostname*

Syntax Description

Parameters Description

hostname Specifies the server for which you want to display registration information.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils disaster_recovery status

This command displays the status of the current backup or restore job.

utils disaster_recovery status *operation*

Syntax Description

Parameters Description

operation Specifies the name of the ongoing operation: backup or restore.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils EnhancedSecurityMode disable

The command disables the EnhancedSecurityMode mode on the system. The system reboots after this mode is disabled.

utils EnhancedSecurityMode disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils EnhancedSecurityMode enable

The command enables the EnhancedSecurityMode mode on the system. The system reboots after this mode is enabled.

utils EnhancedSecurityMode enable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils EnhancedSecurityMode status

The command displays whether the system is operating in EnhancedSecurityMode or non-EnhancedSecurityMode mode.

utils EnhancedSecurityMode status

utils filebeat config**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat config

The command configures the Logstash server details for downloading the information.

utils filebeat configIP addressport numberlog type

| Syntax Description | Parameters | Description |
|--------------------|--------------------|--|
| | IP address | Enter the IP address of the Logstash server. |
| | port number | Enter the port number of Logstash server. |
| | log type | Enter the log type that you have to uploaded to the Logstash server. |

You can also secure the FileBeat service by enabling TLS. The following prompt is displayed after setting the parameters.

```
Do you wish to secure the filebeat service by enabling TLS?
```

```
Enter (yes/no) ?
```

Enter **Yes** to enable TLS.

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat disable

The command disables the filebeat configuration on the system.

utils filebeat disable**Command Modes** Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat enable

The command enables the filebeat configuration on the system.

utils filebeat disable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat status

The command shows whether the filebeat is running or not and its configuration values.

utils filebeat status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils filebeat tls

This command configures Transport Layer Security (TLS) 1.2 as the protocol for communication between the FileBeat client and the logstash server. This enables a secure connection between the FileBeat client and the logstash server, which is a requirement for compliance to Common Criteria guidelines.

In Common Criteria Mode, strict host name verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

utils filebeat tls {enable | disable | status}**Command Modes****Parameters Description****enable** Enables a secure connection between the FileBeat client and the logstash server.**disable** Disables the TLS for FileBeat client.**status** Displays the status for TLS.**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 4

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

A security certificate has to be uploaded from logstash server to the tomcat trust store on Unified Communications Manager and IM and Presence service.

utils fior

This command allows you to monitor the I/O on the server. The File I/O Reporting service provides a kernel-base daemon for collecting file I/O per process.

utils fior**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior disable

This command disables I/O statistics monitoring and deletes all the monitoring data collected on the system. Use this command to disable monitoring and free up disk space that is used by the monitoring data.

utils fior disable**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior enable

This command enables I/O statistics monitoring.



Note Use this command before monitoring begins.

utils fior enable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior list

This command displays a list of the I/O events for all processes.

utils fior list

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior start

This command starts the I/O statistics utility monitoring and data collection. After the monitoring starts, the I/O statistics data is collected in the platform logs. This data can range up to 25 MB per day. Data is rotated after 7 days of data collection. This data is deleted after you disable the I/O statistics utility monitoring.



Note Enable the I/O statistics utility monitoring begins before the monitoring begins.

utils fior start

Command Modes Administrator (admin):

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior status

This command provides the status of the I/O statistics monitoring utility.

utils fior status

Command Modes Administrator (admin):

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior stop

This command stops the I/O statistics monitoring and data collection. However, this command does not delete the collected data.



Note If I/O statistics are no longer needed, disable the cleanup of the monitoring data from the platform logs.

utils fior stop**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils fior top

This command displays a list of I/O statistics for I/O bound processes at the time that you run this command.

utils fior top**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils tips

**Caution**

FIPS mode is only supported on releases that have been through FIPS compliance. Be warned that FIPS mode should be disabled before you upgrade to a non-FIPS compliance version of Unified Communications Manager.

For information about which releases are FIPS compliant and to view their certifications, see the *FIPS 140* document at <https://www.cisco.com/c/en/us/solutions/industries/government/global-government-certifications/fips-140.html>.

This command enables, disables, or displays the status of FIPS 140-2 mode. FIPS 140-2 mode is disabled by default; only an administrator can enable FIPS.

utils tips {enable | disable | status}**Syntax Description****Parameters Description****enable** Activates FIPS 140-2 mode.**disable** Deactivates FIPS 140-2 mode.

utils fips_common_criteria

Parameters Description**status** Displays the status of FIPS 140-2 mode.**Command Modes** Administrator (admin:)**Usage Guidelines** Before enabling FIPS mode, we recommend that you perform a system backup. If FIPS checks fail at start-up, the system halts and requires a recovery CD to be restored.

Consider the following information before you enable FIPS 140-2 mode:

- When you switch from non-FIPS to FIPS mode, the MD5 and DES protocols will not be functional.
- After FIPS mode is enabled on a server, please wait until the server reboots and the phones re-register successfully before enabling FIPS on the next server.
- In FIPS mode, the IM and Presence service uses Red Hat Openswan (FIPS validated) in place of Racoon (non-FIPS validated). If the security policies in Racoon contain functions that are not FIPS approved, the CLI command asks you to redefine the security policies with FIPS approved functions and abort.

**Note** Certificates and SSH key are regenerated automatically, in accordance with FIPS requirements.

Consider the following information before you disable FIPS 140-2 mode: In multiple server clusters, each server must be disabled separately; FIPS mode is not disabled cluster-wide but on a per server basis.

Consider the following information after you enable FIPS 140-2 mode: If you have a single server cluster and chose to apply "Prepare Cluster for Rollback to pre 8.0" enterprise parameter before enabling FIPS mode, disable this parameter after making sure that all the phones registered successfully with the server.

Consider the following information before you enable or disable FIPS 140-2 mode for IM and Presence Service: After you enable or disable FIPS 140-2 mode for IM and Presence Service, the Tomcat certificate is regenerated and the node reboots. The Intercluster Sync Agent syncs the new Tomcat certificate across the cluster; this can take up to 30 minutes. Until the new Tomcat certificate is synced across the cluster, an IM and Presence Service subscriber node cannot access information from the IM and Presence Service database publisher node. For example, a user who is logged into the Cisco Unified Serviceability GUI on a subscriber node will not be able to view services on the IM and Presence Service database publisher node. Users will see the following error message until the sync is complete: Connection to server cannot be established (certificate exception)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils fips_common_criteria

This command configures the Common Criteria mode in the system.

utils fips_common_criteria {enable | disable | status}

Syntax Description**Parameters Description**

enable Enables the Common Criteria mode in the system

disable Disables the Common Criteria mode in the system

When Common Criteria mode is disabled, a prompt is displayed to set the minimum TLS version.

status Displays the status of Common Criteria mode in the system

Command Modes

Administrator (admin:)

Usage Guidelines

Secure connections using TLS version 1.0 are not permitted after enabling the Common Criteria mode. FIPS mode will be enabled while enabling Common Criteria mode. Enabling or disabling Common Criteria mode does not require certificates to be regenerated. However, enabling or disabling FIPS does require rebooting of the system along with regeneration of certificates.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service

**Note**

This CLI command is not applicable to Cisco Unity Connection.

utils firewall ipv4 debug

This command turns IPv4 firewall debugging on or off. If you do not enter a time parameter, this command turns on debugging for 5 minutes.

utils firewall ipv4 debug {off[time]}

Syntax Description**Parameters Description**

off Turns off the IPv4 firewall debugging. If you do not enter the time parameter, this command disables the firewall for 5 minutes.

time (Optional) Sets the duration for which the firewall debugging is to be enabled in the following formats:

- Minutes: 0–1440m
- Hours: 0–23h
- Hours and minutes: 0–23h 0–60m

utils firewall ipv4

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv4

This command enables and disables IPv4 firewall.

utils firewall ipv4 {enable | disable[time]}

| Syntax Description | Parameters | Description |
|--------------------|----------------|--|
| | enable | Turns on the IPv4 firewall. |
| | disable | Turns off the IPv4 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes. |
| | time | (Optional) Sets the duration for which the firewall is to be disabled in the following formats: <ul style="list-style-type: none"> • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv4 list

This command displays the current configuration of the IPv4 firewall.

utils firewall ipv4 list

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv4 status

This command displays the current status of the IPv4 firewall.

utils firewall ipv4 status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv6 debug

This command turns IPv6 firewall debugging on for the configured time period. The default value of time period is 5 minutes.

utils ipv6 firewall debug {off[time]}

| Syntax Description | Parameters Description |
|--------------------|---|
| | off (Optional) Turns off the IPv6 firewall debugging. If you do not enter the time parameter, this command disables the firewall as per the default time period value. |
| | time (Optional) Sets the duration for which the firewall debugging is to be enabled in the following formats: <ul style="list-style-type: none"> Minutes: 0–1440m Hours: 0–23h Hours and minutes: 0–23h 0–60m |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

```
utils firewall ipv6
```

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, and Cisco Unity Connection.

utils firewall ipv6

This command enables and disables IPv6 firewall.

```
utils firewall ipv6 {enable | disable[time]}
```

| Syntax Description | Parameters Description |
|-------------------------|---|
| | enable Turns on the IPv6 firewall. |
| | disable Turns off the IPv6 firewall. If you do not enter the time parameter, this command disables the firewall for 5 minutes. |
| | time (Optional) Sets the duration for which the firewall is to be disabled in the following formats: <ul style="list-style-type: none"> • Minutes: 0–1440m • Hours: 0–23h • Hours and minutes: 0–23h 0–60m |
| Command Modes | Administrator (admin): |
| Usage Guidelines | You can use this command to enable or disable firewall tables. If you are testing the Unified Communications Manager for compliance with the USGv6 Profile, you must disable the IPv6 firewall tables for a duration of 23 hours before you begin the test. |
| Requirements | <p>Command privilege level: 0</p> <p>Allowed during upgrade: Yes</p> <p>Applies to: Unified Communications Manager and Cisco Unity Connection.</p> |

utils firewall ipv6 list

This command displays the current configuration of the IPv6 firewall.

```
utils firewall ipv6 list
```

| Command Modes | Administrator (admin): |
|---------------------|--|
| Requirements | <p>Command privilege level: 0</p> <p>Allowed during upgrade: Yes</p> |

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils firewall ipv6 status

This command displays the current status of the IPv6 firewall.

utils firewall ipv6 status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils ha failover

This command initiates a manual failover for a specified node, where the Cisco Server Recovery Manager stops the critical services on the failed node and moves all users to the backup node.

For IM and Presence nodes, the backup node must be another IM and Presence server. Two servers must be assigned to the same presence redundancy group before you specify the backup server. The back-up server you specify is the other server that is assigned to the presence redundancy group.

utils ha failover {node name}

| Syntax Description | Parameters | Description |
|--------------------|------------------|---|
| | node name | Specifies the node on which to perform the manual failover. |

Command Modes Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Failover Example

```
admin: ha failover shorty-cups
Initiate Manual Failover for Node > shorty-cups
Request SUCCESSFUL.
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Taking Over Reason: On Admin Request
Node 2 Name : shorty-cups State: Failover Reason: On Admin Request
```

utils ha fallback

utils ha fallback

This command initiates a manual fallback for a specified node, where the Cisco Server Recovery Manager restarts the critical services on the active node and moves users back to the active node.

utils ha fallback *node name*

Syntax Description

| Parameters | Description |
|------------------|---|
| <i>node name</i> | Specifies the node on which to perform a manual fallback. |

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Fallback Example

```
admin: ha fallback shorty-cups
Initiate Manual fallback for Node >shorty-cups<
Request SUCCESSFUL.
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Falling Back Reason: On Admin Request
Node 2 Name : shorty-cups State: Taking Back Reason: On Admin Request
```

utils haproxy set {required|optional|disable} client-auth

This command sets the value of client authentication on a specified port. The supported values for authentication are Required, Optional, or Disable.

The following table depicts the default values for the ports.

Table 2: Default Values for the Ports

| Port | Default Value |
|------|---------------|
| 6971 | Optional |
| 6972 | Optional |
| 9443 | Required |



Warning

Setting the client authentication to anything other than default value could have serious implications. Please change these values only as per Cisco TAC team advise.

```
utils haproxy set {required|optional|disable}client-auth portnum
```

| Syntax Description | Parameter | Description |
|--------------------|-----------------|--|
| | <i>portnum</i> | Enter the port number to set HAProxy client authentication. Note The supported port numbers are 6971, 6972 and 9443. |
| | required | Sets the value of client authentication to “required” on a specified port. |
| | optional | Sets the value of client authentication to “optional” on a specified port. |
| | disable | Sets the value of client authentication to “disable” on a specified port. |

Command Modes Administrator (admin:)

Usage Guidelines

- If the user enters a *portnum* value other than 6971, 6972 or 9443, an error message is displayed to enter a valid port number.
- Administrator can execute the **help utils haproxy set optional client-auth** command to view the help content.
- The configured client-auth value for the *portnum* is retained during the upgrades and while performing a backup using Disaster Recovery System (DRS) and restore.
- If you set client authentication to “required”, then server requests for a certificate from the clients. The client must present the requested certificate to the server. Hence, the request can forward to the further services.
- If you set client authentication to “optional”, then server requests for a certificate from the clients. Although if the client does not present the requested certificate to the server, the request can forward to the further services.
- If you set client authentication to “disable”, then the server will not request for a certificate from the clients.
- The HAProxy process restarts when you execute this command.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager

Example

```
admin:utils haproxy set required client-auth 6971
```

```
utils haproxy set num-threads
```

This command will result in the HA Proxy service set the client authentication as per your specification and restart the HAProxy process. Restarting of the HAProxy process might result in momentary disconnection of all Phones and Jabber clients that are accessing this service for secure configuration file downloads. It is recommended this operation be performed during off-busy hours and ensure there are no TFTP operations in progress.

Warning: Setting the client authentication to anything other than default value could have serious implications.

Please change these values only as per Cisco TAC team's advise

Do you want to continue (yes/no) ? **yes**

Successfully set client authentication to required

HAProxy Process already running .. restarting
admin:

admin:utils haproxy set disable client-auth 6972

HAProxy client authentication is already set to disable on port 6972 . No action will be taken.

admin:utils haproxy client-auth set 1234 disable
Please enter valid values for the port.
Supported values are 6971, 6972 and 9443

admin:help utils haproxy set required client-auth 6971

utils haproxy set required client-auth
This command updates the value of client authentication as required on specified port.

Example:

admin:utils haproxy set required client-auth 6971
HAProxy client authentication is already set to required on port 6971. No action will be taken.

admin:

utils haproxy set num-threads

This command sets the number of threads, spawn by the HAProxy service.



Warning

Setting this parameter to anything other than default value could have serious implications. Please change these values only as per Cisco TAC team's advice.

utils haproxy set num-threads *numThreads*

| Syntax Description | Parameter | Description |
|--------------------|-------------------|--|
| | <i>numThreads</i> | <p>Enter the number of HAProxy threads to be configured.</p> <p>Note The default value is 1.</p> <p>The supported values for the number of threads are 1, 2, 3 and 4.</p> |

Command Modes Administrator (admin:)

Usage Guidelines

- If the user enters a *numThreads* value other than 1, 2, 3 or 4, an error message is displayed to enter a valid number of HAProxy threads.
- Administrator can execute the **help utils haproxy set num-threads** command to view the help content.
- The configured *numThreads* value is retained during the upgrades as well as while performing a backup using Disaster Recovery System (DRS) and restore.
- The HAProxy process restarts when you execute this command.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager

Example

```
admin:utils haproxy set num-threads 3
```

This command will result in the HAProxy service spawning as many threads as you have specified and restarting the HAProxy process. Restarting of the HAProxy process might result in momentary disconnection of all Phones and Jabber clients that are accessing this service for secure configuration file downloads and authenticated users data access. It is recommended this operation be performed during off-busy hours and ensure there are no TFTP operations in progress. Warning: Setting this parameter to anything other than default value could have serious implications. Please change these values only as per Cisco TAC team's advise

Do you want to continue (yes/no) ? **yes**

Successfully set number of HAProxy threads to 3

Restarting HAProxy process
admin:

```
admin:utils haproxy set num-threads 5
Please enter a valid number of HAProxy threads.
Supported values are 1, 2, 3 and 4
```

utils ha recover

This command initiates a manual recovery of the presence redundancy group (when nodes are in a Failed state), where IM and Presence restarts the Cisco Server Recovery Manager service in that presence redundancy group.

utils ha recover *presence redundancy group name*

| Syntax Description | Parameters | Description |
|--------------------|---------------------------------------|---|
| | <i>presence redundancy group name</i> | Specifies the presence redundancy group on which to monitor HA status. If no presence redundancy group name is provided, all cluster information is provided. |

Command Modes Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Recover Example

```
admin: ha recover Defaultcluster
Stopping services... Stopped
Starting services... Started
admin:
```

utils ha status

This command displays the HA status for a specified presence redundancy group.

utils ha status *presence redundancy group name*

| Syntax Description | Parameters | Description |
|--------------------|---------------------------------------|---|
| | <i>presence redundancy group name</i> | Specifies the presence redundancy group for which to monitor HA status. If no presence redundancy group name is provided, all cluster information is displayed. |

Command Modes Administrator (admin:)

Requirements

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

Status Example with HA Not Enabled

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Unknown Reason: High Availability Not Enabled
Node 2 Name : shorty-cups State: Unknown Reason: High Availability Not Enabled
```

Status Example with HA Enabled

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Normal
Node 2 Name : shorty-cups State: Normal
```

Status Example with a Critical Service Down

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Failed Over with Critical Services not Running Reason:
Critical Service Down
Node 2 Name : shorty-cups State: Running in Backup Mode Reason: Critical Service Down
```

Status Example Failed

```
admin: ha status
Subcluster Name: DefaultCluster
Node 1 Name : kal-cup1 State: Failed Reason: Critical Service Down
Node 2 Name : shorty-cups State: Failed Reason: Critical Service Down
```

utils ils showpeerinfo

This command returns the peer info vector for either a single cluster in an ILS network, or for all the clusters in an ILS network.

utils ils showpeerinfo *clustername*

Syntax Description

Parameters Description

clustername Specifies the fully qualified domain name of the publisher node for a Unified Communications Manager cluster in an ILS network.

Command Modes

Administrator (admin:)

Usage Guidelines

The peer info vector contains information about a cluster in an ILS network. The available information includes clustername, cluster ID and IP addresses for the cluster nodes. If you want information about a specific cluster in an ILS network, enter the *clustername* parameter. If you want information on all the clusters in the network, leave the *clustername* parameter empty

utils import config**Requirements**

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager

utils import config

This command takes data from the platformConfig.xml file on the virtual floppy drive and modifies the system to match the configuration file. The system reboots after the command successfully completes.

utils import config**Command Modes**

Administrator (admin:)

Usage Guidelines

This command can be executed on any VMware deployment.

1. Power on the VMware.
2. Use the Answer File Generator (AFG) tool (http://www.cisco.com/web/cuc_afg/index.html) to create a platformConfig.xml file.
3. Insert the Config.xml file into a virtual floppy instance (see http://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=1739 for directions).
4. Mount the .flp file in the floppy drive of the new VMware.
5. Sign in to the CLI of the VM (with console or SSH) and execute the **utils import config** command.

The command cycles through all of the data found in the xml file and if data is found that is different than what is currently set on the VM, it modifies the VM to match the new data.

6. The system reboots with the new identity.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Execute utils import config in Vmware Deployment

Procedure

utils iostat

This command displays the iostat output for the given number of iterations and intervals.

utils iostat {interval | iterations | filename}

Syntax Description

Parameters Description

| | |
|-------------------|--|
| interval | Sets the seconds between two iostat readings. You must set this value if you are using the iteration parameter |
| iterations | Sets the number of iostat iterations. You must set this value if you are using the interval parameter. |
| filename | Redirects the output to a file. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils iothrottle

This command allows you to manage and monitor IO throttling on the server.

utils iothrottle {enable | disable | status}

Syntax Description

Parameters Description

| | |
|----------------|--|
| Enable | Enables I/O throttling enhancements which lowers the impact of upgrades on an active system. |
| Disable | Disables I/O throttling enhancements. |
| Status | Displays the status of I/O throttling enhancements. |

Command Modes

Administrator (admin:)

Usage Guidelines

Disabling I/O throttling enhancements can adversely affect the system during upgrades.

Requirements

Command privilege level: 1 for **Enable** and **Disable**, 0 for **Status**

utils itl reset

utils itl reset

This command is used when endpoints are unable to validate their configuration files.

utils itl reset {localkey | remotekey}

| | |
|---------------------------|--|
| Syntax Description | localkey Generates a new ITL file by taking the existing ITL file on the publisher. The command replaces the signature of that ITL file and signs the new ITL file with the ITL recovery key. remotekey Generates a new ITL file after importing the PKCS 12 bag that contains the recovery certificate key pair from the remote location. It then signs the newly generated ITL file with the recovery private key. remotekey has the following parameters: <ul style="list-style-type: none"> • IP address or hostname • User ID • ITLRecovery.p12 |
|---------------------------|--|

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Usage Guidelines



Note You must run this command on the Unified Communications Manager publisher node.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager

Example

```
admin:utils itl reset
Name is None

Generating the reset ITL file.....
The reset ITL file was generated successfully
Locating active Tftp servers in the cluster.....
Following is the list of Active tftp servers in the cluster
=====
=====
```

```
se032c-94-42
=====
Number of Active TFTP servers in the cluster : 1
Transferring new reset ITL file to the TFTP server nodes in the cluster.....
Successfully transferred reset ITL to node se032c-94-42
```

utils ipsec restart

This command is used to restart the ipsec service.

utils ipsec restart

Command Modes Administrator (admin:)

Requirements

Command privilege level:1

Allowed during upgrade: No

Applies to: Unified Communications Manager

Example

```
admin:utils ipsec restart
ipsec_setup: Stopping Openswan IPsec...
ipsec_setup: stop ordered, but IPsec appears to be already stopped!
ipsec_setup: doing cleanup anyway...
ipsec_setup: Starting Openswan IPsec U2.6.32/K2.6.32-573.18.1.e16.x86_64...
ipsec_setup: /usr/libexec/ipsec/addconn Non-fips mode set in /proc/sys/crypto/fips_enabled
ipsec_setup: pluto appears to be running already (`/var/run/pluto/pluto.pid' exists), will
not start another
Successfully Restarted IPsec Service
admin:
```

utils ldap config

This command configures the system LDAP authentication.

utils ldap config {fqdnipaddr}

Syntax Description

Parameters Description

| | |
|---------------|--|
| <i>fqdn</i> | Configures the system to use an FQDN for LDAP authentication. |
| <i>ipaddr</i> | Configures the system to use an IP address for LDAP authentication |

Command Modes

Administrator (admin:)

utils ldap config status**Usage Guidelines**

- **utils ldap config fqdn**—This command is preferred for LDAP authentication, however, you can only use this command if DNS is configured on the system; if the system is not configured to use DNS, use **utils ldap config ipaddr**.
- **utils ldap config ipaddr**—This command is not preferred and should only be used if the system is not, or can not be, configured to use DNS; if the system is configured to use DNS, use **utils ldap config fqdn**.

Requirements

Command privilege level: 1

Applies to: Unified Communications Manager and Cisco Unity Connection

utils ldap config status

This command displays the utils ldap configuration status.

utils ldap config status**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

utils managementAgent alarms minpushLevel

If Push Notifications is enabled, run this command to configure the minimum alarm severity for which Unified Communications Manager sends push notifications alarms to the Cisco cloud.

utils managementAgent alarms minpushLevel*severity***Syntax Description****Parameters** **Description**

| | |
|-----------------|---|
| <i>severity</i> | This value represents the minimum alarm severity for which Unified Communications Manager sends Push Notifications alarms to the Cisco cloud. The possible options are: <ul style="list-style-type: none"> • Critical • Error (this is the default) • Warning • Notice • Information |
|-----------------|---|

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence Service

utils managementAgent alarms pushfrequency

If Push Notifications is enabled, run this command to configure the interval following which Unified Communications Manager sends push notifications alarms to the Cisco cloud.

utils managementAgent alarms pushfrequency*minutes*

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>minutes</i> The upload frequency in minutes. This value must be an integer between 5 and 90 with a default of 30 minutes. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence Service

utils managementAgent alarms pushnow

If Push Notifications is enabled, run this command to send push notifications alarms to the Cisco cloud immediately, without having to wait for the next scheduled upload.

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence Service

utils network arp delete

This command deletes an entry in the Address Resolution Protocol table.

utils network arp delete *host*

utils network arp set

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>host</i> (Optional) Represents the host name or IP address of the host to delete from the table. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Delete Example

```
admin:utils network arp delete myhost
```

utils network arp set

This command sets an entry in the Address Resolution Protocol table.

utils network arp set {host} {addr}

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>host</i> Represents the host name or IP address of the host to add to the table. |
| | <i>addr</i> Represents the hardware address (MAC) of the host to be added in the format: XX:XX:XX:XX:XX:XX |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

Set Example

```
admin:utils network arp set myhost 11:22:33:44:55:66
```

utils network arp list

This command lists the contents of the Address Resolution Protocol table.

utils network arp list host *hostname* [*options*]

| Syntax Description | Parameters Description |
|--------------------|--|
| | host |
| | <i>hostname</i> |
| | <i>options</i> (Optional) page, numeric |
| | <ul style="list-style-type: none"> • Page: Pauses to display the output one page at a time. • Numeric: Shows hosts as dotted IP addresses. |

| | |
|------------------|--|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | In the Flags column, C=cached, M=permanent, P=published. |

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

List example

```
admin:admin: utils network arp listAddress HWtype HWaddress
Flags Mask Iface
sjc21-3f-hsrp.cisco.com ether 00:00:0C:07:AC:71 C
eth0
philly.cisco.com ether 00:D0:B7:85:98:8E C
eth0
Entries: 2 Skipped: 0 Found: 2
```

utils network capture

This command captures IP packets on the specified Ethernet interface.

**utils network capture eth0 [*page*] [*numeric*] [*{filename}*] [*{countnum}*] [*{sizebytes}*] [*{srcaddr}*]
 [*{destaddr}*] [*{portnum}*]**

utils network capture-rotate

| Syntax Description | Parameters | Description |
|--------------------|--------------------------|---|
| | eth0 | Specifies Ethernet interface 0. |
| | page | (Optional) Displays the output one page at a time. When you use the page or file options, the complete capture of all requested packets must occur before the command completes. |
| | numeric | (Optional) Displays hosts as dotted IP addresses. |
| | file <i>fname</i> | (Optional) Outputs the information to a file. The file option saves the information to <code>platform/cli/fname.cap</code> . The filename cannot contain the “.” character. |
| | countnum | (Optional) Sets a count of the number of packets to capture. For screen output, the maximum count equals 1000, and, for file output, the maximum count equals 10,000. |
| | sizebytes | (Optional) Sets the number of bytes of the packet to capture. For screen output, the maximum number of bytes equals 128, for file output, the maximum of bytes can be any number or ALL. |
| | src <i>addr</i> | (Optional) Specifies the source address of the packet as a host name or IPV4 address. |
| | destaddr | (Optional) Specifies the destination address of the packet as a host name or IPV4 address. |
| | portnum | (Optional) Specifies the port number of the packet, either source or destination. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network capture-rotate

This command captures IP packets beyond the 100,000 packet limit of **utils network capture**.

```
utils network capture-rotate {filename} [{sizebytes}] [{sizePerFilemegabytes}] {maxFiles
num} [{srcaddr}] [{destaddr}] [{portnum}][{host protocoladdr}]
```

| Syntax Description | Parameters | Description |
|--------------------|---|--|
| | file <i>fname</i> | Outputs the information to a file. Note The file will be saved in platform/cli/fname. fname should not contain the "." character. |
| | sizebytes | The number of bytes of the packet to capture. Valid values include any number up to 65535 or ALL. The default is ALL. |
| | sizePerFile <i>megabytes</i> | The sizePerFile sets the value for the size of the log files. (Unit is millions of bytes.) The default value of sizePerFile is 25 MB. |
| | maxFiles <i>num</i> | the maxFiles indicates the maximum number of log files to be created. The default value of maxFiles is 10. |
| | src <i>addr</i> | (Optional) Specifies the source address of the packet as a hostname or IPV4 address. |
| | dest <i>addr</i> | (Optional) Specifies the destination address of the packet as a host name or IPV4 address. |
| | port <i>num</i> | (Optional) Specifies the port number of the packet, either source or destination. |
| | host <i>protocol</i> <i>addr</i> | (Optional) Limits capture to traffic to and from a specific host. Options for <i>protocol</i> are IP, arp, rarp, all, and <i>addr</i> must be in IPv4 or hostname format. If host is used, do not provide src or dest . |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network connectivity

This command verifies the node network connection to the first node in the cluster (this connection is only valid on a subsequent node) and to a remote node.

utils network connectivity [{reset}] [hostname/ip address]

utils network connectivity [hostname/ip address] [port-number] [timeout]

| Syntax Description | Parameters | Description |
|--------------------|----------------------------|---|
| | connectivity | This command verifies the node network connection to the first node in the cluster. It is also used to check connectivity to a remote node, where there are two mandatory parameters, hostname/ip address and port-number . |
| | reset | (Optional) Clears previous return codes. |
| | <i>hostname/ip address</i> | <ul style="list-style-type: none"> • (Optional) Hostname or IP address of cluster node to check network connectivity with the publisher or the first node. • (Mandatory) Hostname or IP address of the host that has to be tested for the TCP connection, to check network connectivity on the remote server. |
| | port-number | (Mandatory) Port number of the host that requires connection test. |
| | timeout | (Optional) Specifies the time in seconds after which port connectivity message is displayed. |

Command Modes

Administrator (admin:)

Usage Guidelines

- The **utils network connectivity [reset] [hostname/ip address]** command is used to check the network connectivity to the publisher or the first node.
- The **utils network connectivity [hostname/ip address] [port-number] [timeout]** command is used to check the network connectivity to a remote server.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network host

This command resolves a host name to an address or an address to a host name.

utils network host *name* [{server} *serv*] [page] [detail] [srv]

Syntax Description

| Parameters Description | |
|------------------------|--|
| <i>name</i> | Represents the host name or IP address that you want to resolve. |
| <i>serv</i> | (Optional) Specifies an alternate domain name server. |
| [page] | (Optional) Displays the output one screen at a time. |
| [detail] | (Optional) Displays a detailed listing. |
| [srv] | (Optional) Displays DNS SRV records. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network ipv6 host

This command does an IPv6 host lookup (or IPv6 address lookup) for the specified host name or IPv6 address.

utils network ipv6 host {host_name} {ip6_address}

Syntax Description

| Parameters Description | |
|------------------------|---|
| <i>host_name</i> | Specifies the name of the server. |
| <i>ip6_address</i> | Specifies the IPv6 address of the server. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils network ipv6 traceroute

utils network ipv6 traceroute

This command traces an IPv6 address or hostname.

utils network ipv6 traceroute [{*ipv6-address* | *hostname*}]

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>ipv6-address</i> Specifies IPv6 address that you want to trace. |
| | <i>hostname</i> Specifies the host name that you want to trace. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils network ipv6 ping

This command allows you to ping an IPv6 address or hostname.

utils network ipv6 ping *destination* [*count*]

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>destination</i> Specifies a valid IPv6 address or host name that you want to ping. |
| | [<i>count</i>] Specifies the number of times to ping the external server. The default count equals 4. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection.

utils network ping

This command allows you to ping another server.

utils network ping *destination* [*count*] [*size*]

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>destination</i> Represents the ip address or host name of the server that you want to ping. |
| | <i>[count]</i> Specifies the number of times to ping the external server. The default count is 4. |
| | <i>[size]</i> Specifies the size of ping packets in bytes. The default value is 56. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network traceroute

This command traces IP packets that are sent to a remote destination.

utils network traceroute [destination]

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>destination</i> Represents the hostname or IP address of the server to which you want to send a trace. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection.

utils network name-service {hosts|services} cache invalidate

This command clears the name service cache.

utils network name-service {hosts \ services} [cache invalidate]

| Syntax Description | Parameters Description |
|--------------------|--|
| | Hosts Host services cache |
| | Services Services service cache |

utils ntp auth symmetric-key

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Consider the following example for flushing/clearing the cache:

```
admin:utils network name-service hosts cache invalidate
admin:
Successful
```

utils ntp auth symmetric-key

utils ntp auth symmetric-key {enable | disable | status}

This command helps you enable or disable authentication of the selected NTP server. The authentication is based on symmetric keyID and key. The symmetric key is stored in the encrypted format in Unified Communications Manager.



Note Before you run this command, ensure that you know the NTP server keyID and its corresponding key.

Syntax Description

Parameters Description

enable Choose one of the NTP servers from the list of available servers and enable it for authentication.

disable Choose one of the NTP servers from the list of available servers and disable it for authentication.

status Shows the authentication status of all the listed NTP servers.

Usage Guidelines

The system prompts you to enter the KeyID or Symmetric key for authentication of an NTP server.



Note

- Unified Communications Manager sends Syslog alert messages when the authentication status of an NTP server changes. You can secure the connections to the syslog server with TLS.
- You can configure the NTP server authentication after you install Unified Communications Manager.

Requirements

Command privilege level: Level 1 can execute all commands, Level 0 can execute only status command

Allowed during upgrade: No

Applies to: Unified Communications Manager

Example: utils ntp auth symmetric-key status - View status when NTP authentication is not enabled

```
admin:utils ntp auth symmetric-key status
10.77.32.92 : NTP Authentication is disabled.
10.77.46.203 : NTP Authentication is disabled.

ind assid status conf reach auth condition last_event cnt
=====
1 8468 963a yes yes none sys.peer sys_peer 3
2 8469 9024 yes yes none reject reachable 2
```

Example: utils ntp auth symmetric-key enable - Enable NTP authentication

```
admin:utils ntp auth symmetric-key enable
The List of NTP servers Configured:
1. 10.77.32.92
2. 10.77.46.203
q. press q to exit
Enter the selection for which to configure NTP authentication: 1
Please enter the Key ID [1-65534]:
2
Please enter the Symmetric Key of the NTP Server (SHA1):
Restarting NTP
please run the utils ntp auth symmetric-key status to check the status of NTP Authentication
```

Example: utils ntp auth symmetric-key status - View status after NTP authentication is enabled

```
admin:utils ntp auth symmetric-key status
10.77.46.203 : NTP Authentication is disabled.
10.77.32.92 : NTP Authentication is enabled.

ind assid status conf reach auth condition last_event cnt
=====
1 57733 9044 yes yes none reject reachable 4
2 57734 f014 yes yes ok reject reachable 1
```

Example: utils ntp auth symmetric-key disable - Disable NTP authentication

```
admin:utils ntp auth symmetric-key disable
The List of NTP servers Configured:
0. All
1. 10.77.46.203
2. 10.77.32.92
q. press q to exit
Enter the selection for which to disable NTP authentication: 2
NTP authentication has been disabled on the particular server.
Restarting NTP
```

Example: utils ntp auth symmetric-key status - View status after NTP authentication is disabled

```
10.77.46.203 : NTP Authentication is disabled.
10.77.32.92 : NTP Authentication is disabled.

ind assid status conf reach auth condition last_event cnt
```

```
utils ntp auth auto-key
```

```
=====
1 42767 9144 yes yes none falsetick reachable 4
2 42768 912a yes yes none falsetick sys_peer 2
```

Example: `utils ntp auth symmetric-key status` - View status of NTP authentication

```
admin:utils ntp auth symmetric-key status
10.77.32.92 : NTP authentication is failed. Please check the NTP authentication Key ID
and Symmetric Key entered is correct. To update, disable and reenable authentication for
this NTP server.
10.77.32.78 : NTP Authentication is disabled.

ind assid status conf reach auth condition last_event cnt
=====
1 31609 c02c yes no bad reject 2
2 31610 803a yes no none reject sys_peer 3
```

utils ntp auth auto-key

utils ntp auth auto-key {enable | disable | status}

This command helps you enable or disable authentication of the selected NTP server. The authentication is based on the client key. It also allows you to check the authentication status of the ntp servers.



Note You can configure the PKI-based authentication with the IFF identity scheme on the NTP server only if you enable common criteria mode on the Unified Communication Manager.

You can enable either symmetric key or PKI-based NTP authentication on Unified Communications Manager. If you try to enable the symmetric key on the PKI enabled server, the following warning message is displayed:



Warning NTP authentication using Autokey is currently enabled and must be disabled before the symmetric key is enabled. Use the command 'utils ntp auth auto-key disable' to disable NTP authentication, then retry this command.

If you try to enable the Autokey on the symmetric key enabled server, the following warning message is displayed:



Warning NTP authentication using symmetric key is currently enabled and must be disabled before Autokey is enabled. Use the command 'utils ntp auth symmetric-key disable' to disable NTP authentication, then retry this command.



Note NTP servers require ntp version 4 and the rpm version `ntp-4.2.6p5-1.el6.x86_64.rpm` and above.

Syntax Description

| Parameters | Description |
|----------------|---|
| enable | Choose one of the NTP servers from the list of available servers and enable it for authentication. |
| disable | Choose one of the NTP servers from the list of PKI authentication enabled NTP servers and disable authentication. |
| status | Shows the authentication status of all the listed NTP servers. |

Usage Guidelines

While enabling NTP authentication, system prompts you to enter the IFF client key for authentication of an NTP server. When the client key is uploaded successfully, it restarts the NTP service on the Unified Communications Manager publisher node. Post that authentication is enabled between the Unified Communications Manager and NTP server.

**Note**

- You can configure the NTP server authentication after you install or upgrade the Unified Communications Manager.
- Do not terminate the execution by pressing “Ctrl-C” key during the CLI execution.

Requirements

Command privilege level:: Level 1 can execute all commands, Level 0 can execute only status command

Allowed during upgrade: No

Applies to:: Unified Communications Manager

admin:utils ntp auth auto-key enable-Enable NTP authentication

```
1: 10.78.83.146
2: 10.77.46.203
3: 10.77.32.92
```

Select the server for which auto-key based NTP authentication is to be enabled (Enter q to exit):2

Enter the IFF client key for the 10.77.46.203:

```
# ntpkey_ifffpar_ccm203.3705887848
# Thu Jun  8 10:47:28 2017
```

-----BEGIN PRIVATE KEY-----

```
MIGzAgEAMIGoBgcqhkjOOQBMIGcAkEA4r3EkDFdP05QSpzVpGHnZN3JgOkW0Ch9
erxLB7zSxrwNdndI1Wg5bUhZZWKZceQd/nyD6FLpZNFrpHnylkBuqQIVAJEjgjZM
r2aaMGSN5x2yUmhT4MqNAkBp2gkQNi8sluLre0YKyc+kdiCiRkEK2jKwBETXs7Mh
aEd/c4DQnZkd5U9gco4v9zPpsfPOqftvymVyVmRyKX0NBAMCAQE=
```

-----END PRIVATE KEY-----

The Client key does not match the hostname of the selected NTP server. This could be because a DNS server is not configured or the DNS entry for this host is not present.

Please verify the client key uploaded corresponds to the selected NTP server and that the DNS configuration is correct.

Do you want to continue with this operation?<yes/no>:

Client key uploaded successfully

utils ntp auth auto-key

Restarting NTP service.
Please run 'utils ntp auth auto-key status' to check the status of NTP authentication.



Note The above user warning prompt is not displayed, if the DNS server is able to resolve the hostname of the selected NTP server and if it matches with the hostname in the client key provided.

admin:utils ntp auth auto-key status - View status when NTP authentication is enabled

```
1.10.78.83.146 : NTP Authentication is disabled.
2.10.77.46.203 : NTP Authentication is enabled.
3.10.77.32.92 : NTP Authentication is disabled.
Select the server for which auto-key based NTP authentication details is to be displayed
(Enter q to exit):
2
      NTP public certificate:
# ntpkey_RSA-SHA1cert_ccm-90.3708840303
# Wed Jul 12 14:55:03 2017

-----BEGIN CERTIFICATE-----
MIICwTCCAamgAwIBAgIFAN0QaW8wDQYJKoZIhvcNAQEFBQAwETEPMA0GA1UEAxMG
Y2NtLTkwMB4XDTE3MDcxMjA5MjUwM1oXDTE4MDcxMjA5MjUwM1owETEPMA0GA1UE
AxMGY2NtLTkwMIIBiJANBgkqhkiG9w0BAQEFAOCAQ8AMIBCgKCAQEAv0no6hNu
C88VXYcKCMCJ6w6hny7eG6JU8LzEjMIN5aqD0FDjnRzIKK/DL5DMReRy4j/4YQTR7
nT9ThudFwyUu0y860pPWBgfKeII6kjtkElo4mp8RyMLJDp4e0jOh63wCP0cJsdZ1
dXfvx0/Ojk6ZdX70eHtcZn2ycLkSZP6hkos6Un//5zfulIG47QEliIh3bpPWq647
JiHELeuigCNm2p1LsorXgmA3LFB199pamwF19Lmqb49y0Ie/QchXhudOOsG0zuaL
PaEnkPdyNtxvQbCQ24cVBmHup7UBkdZYA+5unpbczMzzE3tQsl/CvizmUbfA+gi
/DWSBC4Hfc011QIDAQABoAyWbjAPBgNVHRMBAf8EBTADAQH/MAsgA1UdDwQEAWIC
hDANBgkqhkiG9w0BAQUFAAOCAQEAttJbav0+qVpk9abAWlWcmhQubjW58qrLE9A0
2ZvIvHKq2TyBAIxYcUSQQ3GXSwBDHKZUNSAzrFrTQ+vLFqFvoSH0o5EFruIdrwn
zCD1OqNjXsCPsxyofSDuT/+pxvVxGX1cIpmda2tieEUcdSvaGx0l+ABhOO8YI6uf
bHNUCdjNSYbF6W0Lms643VS1NEUmBE4Tp+YwpLgbmXDXGalwHlog5fZfnywk161J
n34asWwWmR467WADnPBfMJDWzU1GMceh11XQ/gbYYX3+rpileAZF6x9Z/goexhNc
L4WyzBr1R7iueJ1wYdFZ5THXoat3bxWMWU4fDzqTWA7G9hpP6w==
-----END CERTIFICATE-----
      Client Key:
# ntpkey_ifffpar_ccm203.3705887848
# Thu Jun  8 10:47:28 2017

-----BEGIN PRIVATE KEY-----
MIGzAgEAMIGoBgcqhkjOOAQBMIGcAkEA4r3EkDFdP05QSpzVpGHnZN3JgOkW0Ch9
erxLB7zSxrwNdnDI1Wg5bUhZZWKZceQd/nyD6FLpZNFrpHnylkBuqQIVAJEjgjZM
r2aaMGSN5x2yUmhT4MqNAkBp2gkQNi8sluLre0YKyc+kdiCiRkEK2jKwBETXs7Mh
aEd/c4DQnZkd5U9gco4v9zPpsfOqftvymVvMryKX0NBMCAQE=
-----END PRIVATE KEY-----
admin:
```

admin:utils ntp auth auto-key disable-Disable NTP authentication

```
The List of NTP servers Configured:
1. 10.77.46.203
Enter the NTP server in which the authentication needs to be disabled(Enter q to exit): 1
NTP authentication has been disabled on 10.77.46.203
Restarting NTP
admin:
```

utils ntp server add

The command adds a maximum of five specified NTP servers.

utils ntp server add *s1* [{*s1s2s3s4s5*}] [norestart]

Syntax Description

Parameters Description

s1... Specifies the NTP servers.

norestart Causes the NTP service to not restart after you add the servers.

Command Modes

Administrator (admin):

Usage Guidelines

If you use **norestart**, an explicit restart of the NTP service is required for the changes to take effect.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager

Example: Attempting to Add Servers with Incorrect Command Line Parameters

```
admin: admin:utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8
Incorrect number of parameters entered for add
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
```

Example: Attempting to Add a Server Using norestart Without Specifying a Server

```
admin: utils ntp server add s1 s2 s3 s4 s5 s6 s7 s8
Incorrect number of parameters entered for add
usage: utils ntp server add s1 [s2 s3 s4 s5] [norestart]
```

Example: Adding servers without norestart

```
admin: utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : added successfully.
clock2.cisco.com : added successfully.
Restarting NTP on the server.
```

Example: Adding Servers That Are Already Added, Without norestart

```
admin: utils ntp server add clock1.cisco.com clock2.cisco.com
clock1.cisco.com : [The host has already been added as an NTP server.]
clock2.cisco.com : [The host has already been added as an NTP server.]
```

Example: Adding Server to Self Without norestart

```
admin: utils ntp server add bg1r-ccm26
bg1r-ccm26 : [This server cannot be added as an NTP server.]
```

utils ntp server delete

Example: Adding Inaccessible Server Without norestart

```
admin: utils ntp server add clock3.cisco.com
clock3.cisco.com : [ Inaccessible NTP server. Not added. ]
```

Example: Adding Servers with norestart

```
admin: utils ntp server add ntp01-syd.cisco.com ntp02-syd.cisco.com clock.cisco.com norestart
ntp01-syd.cisco.com : added successfully.
ntp02-syd.cisco.com : added successfully.
clock.cisco.com : added successfully.
The NTP service will need to be restarted for the changes to take effect.
```

Example: Adding Servers When Five Are Already Configured

```
admin:utils ntp server add clock3.cisco.com
The maximum permissible limit of 5 NTP servers is already configured.
```

utils ntp server delete

This command deletes NTP servers that are configured.

utils ntp server delete

Command Modes

Administrator (admin:)

Usage Guidelines

This command allows you to delete a configured Network Time Protocol (NTP) server or multiple NTP servers. When you choose the server to delete, you are prompted to indicate if you want to restart the NTP service. If you choose no, the NTP service does not get restarted after the server is deleted.



Note

It is required to have at least 1 NTP server configured. Therefore, you cannot delete an NTP server if only one is configured. If you select the option to delete all the NTP servers, the NTP servers are deleted in top down order and the last NTP server on the list does not get deleted. The process is similar to the top down order followed during `utils ntp config` or `utils ntp status`

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager

Example: Deleting Servers with Incorrect Command Line Parameters

```
admin: utils ntp server delete clock1.cisco.com clock2.cisco.com
Incorrect number of optional parameters entered for delete
usage: utils ntp server delete
```

Example: Deleting Single Server with NTP Restart

```
admin: utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: 1

Restart NTP (y/n): y

clock1.cisco.com will be deleted from the list of configured NTP servers.
Continue (y/n)?y

clock1.cisco.com : deleted successfully.
Restarting NTP on the server.
```

Example: Deleting All Servers Without NTP Restart

```
admin: utils ntp server delete
1: clock1.cisco.com
2: clock2.cisco.com
3: ntp01-syd.cisco.com
4: ntp02-syd.cisco.com
5: clock.cisco.com
a: all
q: quit

Choice: a

Restart NTP (y/n): n

This will result in all the configured NTP servers being deleted.
Continue (y/n)?y

clock1.cisco.com : deleted successfully.
clock2.cisco.com : deleted successfully.
ntp01-syd.cisco.com : deleted successfully.
ntp02-syd.cisco.com : deleted successfully.
clock.cisco.com : [The NTP server was not deleted. At least one NTP server is required.]
The NTP service will need to be restarted for the changes to take effect.
```

Example: Deleting All Servers When No Servers Are Configured

```
admin: utils ntp server delete
There are no NTP servers configured to delete.
```

utils ntp config

This command displays the current configuration of the NTP client and server.



Note To avoid potential compatibility, accuracy, and network jitter problems, the external NTP servers that you specify for the primary node should be NTP v4 (version 4).

utils ntp restart**utils ntp config****Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence server on Unified Communications Manager, Cisco Unity Connection

utils ntp restart

This command restarts the NTP service.

utils ntp restart**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils ntp server list

This command lists all NTP servers.

utils ntp server list**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: IM and Presence server on Unified Communications Manager

utils ntp start

This command starts the NTP service if it is not already running.



Note You can not stop the NTP service from the command line interface. Use this command when the utils ntp status command returns stopped.

utils ntp start

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence server on Unified Communications Manager, and Cisco Unity Connection

utils ntp status

This command displays the current status of NTP.

utils ntp status

Command Modes Administrator (admin:)

Requirements

Command privilege level:

Allowed during upgrade:

Applies to: IM and Presence service on Unified Communications Manager.

utils os kerneldump

This command configures kerneldump to provide a kernel crash dumping mechanism. The kernel captures the dump to the local disk, in case of a kernel crash.



Note The netdump commands have been removed from release 8.6(1) and have been replaced with the kerneldump commands.

utils os kerneldump {enable | disable}

Command Modes Administrator (admin:)

```
utils os kerneldump ssh
```

Usage Guidelines

If a kernel crash occurs, the capture kernel dumps the core on the local disk of the server. The primary kernel reserves 128MB of physical memory that the capture kernel uses to boot. The kerneldump uses the **kexec** command to boot into a capture kernel whenever the kernel crashes.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

Example

```
admin: utils os kerneldump enable
*****WARNING*****
Enabling kerneldump requires system reboot
Would you like to boot the machine (y/n):y
kerneldump enable operation succeeded
System going for a reboot
```

utils os kerneldump ssh

This command enables, disables, or displays the status of an external SSH server.

```
utils os kerneldump ssh {enable | disable | status}
```

Syntax Description

Parameters Description

enable Configures an external SSH server as a kerneldump server to kernel dumps.

disable Removes support of the external SSH server that is configured to collect kernel dumps.

status Indicates whether an external SSH server is configured or not, to collect kernel dumps.

Command Modes

Administrator (admin):

Usage Guidelines

If external SSH server has the kerneldump service enabled and a kernel crash occurs, the capture kernel dumps the core on the external server that is configured to collect the dump.

Enabling and disabling kerneldump require a system reboot for the changes to come into effect.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

Example

```
admin: utils os kerneldump ssh disable 10.77.31.60
Disabling kerneldump requires system reboot
```

```
Would you like to continue (y/n): y
kerneldump disable operation succeeded
System going for a reboot
```

utils os kerneldump status

This command provides the status of the kdump service.

utils os kerneldump status

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils os secure

This command is used to specify the level of security provided by selinux.

utils os secure {enforce | permissive | status}

| Syntax Description | Parameters Description |
|--------------------|------------------------|
| | enforce |
| | permissive |
| | status |

| | |
|----------------------|------------------------|
| Command Modes | Administrator (admin:) |
|----------------------|------------------------|

| | |
|-------------------------|---|
| Usage Guidelines | Note that selinux does not handle rate limiting. Rate limiting is handled by ipprefs and ip tables. |
|-------------------------|---|

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence service on Unified Communications Manager

utils os secure dynamic-policies compile

utils os secure dynamic-policies compile

This command generates the selinux policy module and type enforcement that resolves the recorded denials under the dynamic policy.

utils os secure dynamic-policies compile *policy name*

| Syntax Description | Parameters | Description |
|--------------------|---|---|
| | <i>policy name</i> | Type the dynamic policy name under which the compilation of the selinux policy module and type enforcement is done. |
| Command Modes | Administrator (admin:) | |
| Usage Guidelines | Requirements <ul style="list-style-type: none"> Command privilege level: 1 Allowed during upgrade: Yes <p>Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager</p> | |

utils os secure dynamic-policies list

This command lists all the operating system dynamic policies with their statuses.

utils os secure dynamic-policies list

| | |
|------------------|---|
| Command Modes | Administrator (admin:) |
| Usage Guidelines | Requirements <ul style="list-style-type: none"> Command privilege level: 1 Allowed during upgrade: Yes <p>Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager</p> |

utils os secure dynamic-policies load

This command loads the selinux policy module for the dynamic policy into selinux. This command applies new rules into selinux that prevent the denials that are recorded under the dynamic policy from reoccurring.

utils os secure dynamic-policies load *policy name*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>policy name</i> Type the dynamic policy name that has a generated selinux policy module, which is not loaded into selinux.. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | Requirements |
| | Command privilege level: 1 Allowed during upgrade: Yes Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager |

utils os secure dynamic-policies remove

This command deletes all the data for the dynamic policy from the operating system. The data includes unloading the policy module from selinux and deleting the generated policy module, type enforcements, recorded denials, and delta logs.

utils os secure dynamic-policies remove *policy name*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>policy name</i> Type the dynamic policy name that is unnecessary or no longer required. |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | Requirements |
| | Command privilege level: 1 Allowed during upgrade: Yes Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager |

utils os secure dynamic-policies show

This command displays the rules to be introduced by loading the generated selinux policy module of the dynamic policy. Run this command after the successful compilation to verify that the rules to be loaded are secure.

utils os secure dynamic-policies show *policy name*

utils os secure dynamic-policies start-recording

| Syntax Description | Parameters Description |
|--------------------|---|
| | <p><i>policy name</i> Type the dynamic policy name for which you want to view the rules.</p> |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | <p>Requirements</p> <p>Command privilege level: 1</p> <p>Allowed during upgrade: Yes</p> <p>Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager</p> |

utils os secure dynamic-policies start-recording

This command starts recording the selinux denials and organizes them under the new dynamic policy.



Note

- This command sets the system into the permissive mode.
- The dynamic-policies are generated on a per-node basis. As a restriction, these policies cannot be exported or imported. This restriction has the following advantages:
 - Prevent loading external and unsigned policy modules into selinux that may create security vulnerabilities.
 - Prevent the transfer of policy modules between Unified Communications Manager clusters with different configurations.

utils os secure dynamic-policies start-recording *policy name*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <p><i>policy name</i> Type the dynamic policy name where the selinux denials and future policy data is to be organized.</p> |
| Command Modes | Administrator (admin:) |
| Usage Guidelines | <p>Requirements</p> <p>Command privilege level: 1</p> <p>Allowed during upgrade: Yes</p> <p>Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager</p> |

utils os secure dynamic-policies stop-recording

This command stops recording the selinux denials for the dynamic policy. This command switches the system back to the original enforcement mode—either permissive mode or enforcing mode. This log generates a delta log for all selinux denials that occurred between the start of the recording till it ends.



Note

This command fails if the delta log has no new denials. Then, the dynamic policy is purged and you will have to use this command again.

utils os secure dynamic-policies stop-recording *policy name*

Syntax Description

Parameters Description

policy name Type the dynamic policy name the recording of which you want to stop.

Command Modes

Administrator (admin:)

Usage Guidelines

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and IM and Presence Service on Unified Communications Manager

utils PlatformWebAccess disable

Use this command to restrict the user sign-in to Cisco OS Administration and Disaster Recovery System applications when SSO is enabled.

utils PlatformWebAccess disable

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

```
utils PlatformWebAccess enable
```

utils PlatformWebAccess enable

Use this command to enable the user sign-in to Cisco OS Administration and Disaster Recovery System applications.

```
utils PlatformWebAccess enable
```

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils PlatformWebAccess status

Use this command to display the status of the web access of the system—whether the platform web access is enabled or disabled for Cisco OS Administration and Disaster Recovery System applications.

```
utils PlatformWebAccess status
```

Command Modes Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils processCoreDumps disable

This command disables the process core dumps.

```
utils processCoreDumps disable
```

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils processCoreDumps enable

This command enables the process core dumps.

utils processCoreDumps enable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils processCoreDumps status

This command provides the status of the kdump service.

utils processCoreDumps status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remote_account create

This command creates a remote account.

utils remote_account create

Command Modes Administrator (admin:)

Usage Guidelines A remote account generates a pass phrase that allows Cisco Systems support personnel to get access to the system for the specified life of the account.

utils remote_account disable

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remote_account disable

This command allows you to disable a remote account.

utils remote_account disable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils remote_account enable

This command allows you to enable a remote account.

utils remote_account enable

Command Modes Administrator (admin:)

Usage Guidelines You can have only one remote account that is enabled at a time.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils remote_account status

This command allows you to check the status of a remote account.

utils remote_account status

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils remotesyslog set protocol tcp

This command configures the protocol for communication with remote syslog server as TCP on the system. Restart the node for changes to take effect.

utils remotesyslog set protocol tcp

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remotesyslog set protocol udp

This command configures the protocol for communication with remote syslog server as UDP on the system. Restart the node for changes to take effect.

utils remotesyslog set protocol udp

Command Modes Administrator (admin:)**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils remotesyslog set protocol tls

This command configures the protocol for communication with remote syslog server as Transport Layer Security (TLS) 1.2 on the system. TLS 1.2 enables Unified Communications Manager and IM and Presence

utils remotesyslog show protocol

Service to establish a secure connection with syslog servers. This enables Unified Communications Manager and IM and Presence Service to comply with Common Criteria guidelines.



Note

- Ensure that the syslog server supports TLS 1.2 protocol as a secure connection will be established only if the syslog server supports TLS 1.2 protocol.
- In Common Criteria Mode, strict host name verification is implemented. Hence, it is required to configure the server with a fully qualified domain name (FQDN) which matches the certificate.

Restart the node for changes to take effect.

utils remotesyslog set protocol tls

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: Unified Communications Manager and IM and Presence service on Unified Communications Manager

A security certificate has to be uploaded from the syslog server to the tomcat trust store on Unified Communications Manager and IM and Presence service.

utils remotesyslog show protocol

This command shows whether the protocol for communication with remote syslog server is TCP or UDP on the system.

utils remotesyslog show protocol

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils reset_application_ui_administrator_name

This command resets the application user interface administrator name.

utils reset_application_ui_administrator_name**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils reset_application_ui_administrator_password

This command resets the application user interface administrator password.

**Note**

For password changes on IM and Presence nodes, stop the Cisco Presence Engine service in all IM and Presence nodes before resetting the administrator password. After the password reset, restart Cisco Presence Engine service in all the nodes. Make sure that you perform this task during maintenance because you may face presence issues when the PE is stopped. If you change the password from IM and Presence nodes, make sure the new password is same as the current administrator password in Unified Communication Manager.

utils reset_application_ui_administrator_password**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

utils restore_application_ui_administrator_account

This command restores the application user interface administrator account.

utils restore_application_ui_administrator_account**Command Modes** Administrator (admin:)**Requirements**

Command privilege level: 1

Allowed during upgrade: No

utils rosters list limited

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils rosters list limited

Run this command on the database publisher node to obtain a count of invalid watchers and invalid contacts. The total counts display in the CLI.

Command Modes Administrator (admin:)

Usage Guidelines We recommend that you run this command only during a maintenance window. This command will list only the count and no details of the invalid records. For details on the invalid records, try **utils rosters list [watchers | contacts] full**.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters list full

Run this command on the database publisher node to write the details of all invalid watchers and invalid contacts to a file. The command also displays the total counts in the CLI.

Command Modes Administrator (admin:)

Usage Guidelines We recommend that you run this command only during a maintenance window.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters list watchers

Run this command on the database publisher node to write the details of all invalid watchers in the cluster to a file. The total count of invalid contacts also displays in the CLI.

Command Modes Administrator (admin:)

Usage Guidelines We recommend that you run this command only during a maintenance windows. While executing, progress is displayed in the CLI as well as in a log file.

Requirements

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters list contacts

Run this command on the database publisher node to write the details of all invalid contacts in the cluster to a file. The total count of invalid contacts also displays in CLI.

Command Modes Administrator (admin:)

Usage Guidelines We recommend that you run this command only during a maintenance window.**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils rosters delete

Run this command on the database publisher node to delete all invalid watchers and invalid contacts in the IM and Presence cluster.

Command Modes Administrator (admin:)

Usage Guidelines We recommend that you run this command only during a maintenance windows. While executing, progress is displayed in the CLI as well as in a log file.**Requirements**

Command privilege level: 4

Allowed during upgrade: No

Applies to: IM and Presence Service

utils scheduled-task disable

This command disables the scheduled-task.

utils scheduled-task disable scheduled-task

utils scheduled-task enable

| Syntax Description | Parameters | Description |
|----------------------|---|--|
| | scheduled-task | Enter the name of the task that you need to disable. |
| Command Modes | Administrator (admin:) | |
| | Requirements | |
| | Command privilege level: 1 | |
| | Allowed during upgrade: No | |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

utils scheduled-task enable

This command enables the scheduled-task.

utils scheduled-task enable scheduled-task

| Syntax Description | Parameters | Description |
|----------------------|---|---|
| | scheduled-task | Enter the name of the task that you need to enable. |
| Command Modes | Administrator (admin:) | |
| | Requirements | |
| | Command privilege level: 1 | |
| | Allowed during upgrade: No | |
| | Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection | |

utils scheduled-task list

This command lists all the scheduled tasks.

utils scheduled-task list

| Command Modes | Administrator (admin:) |
|---------------|----------------------------|
| | Requirements |
| | Command privilege level: 0 |
| | Allowed during upgrade: No |

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils set urlpattern disable

This command disables the URL pattern and modifies the `zzz20_product_profile.sh` file. After the URL pattern is disabled, this command appends the following line:

```
export TOMCAT_EXCLUDE_URLPATTERNS="/ucmuser"
```

utils set urlpattern disable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils set urlpattern enable

This command enables the URL pattern and modifies the `zzz20_product_profile.sh` file. After the URL pattern is enabled, this command appends the following line:

```
export TOMCAT_EXCLUDE_URLPATTERNS=""
```

utils set urlpattern enable

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils service

This command activates, deactivates, starts, stops, or restarts a service.

```
utils service {activate | deactivate | start | stop | restart} service_name
```

| Syntax Description | Parameters | Description |
|--------------------|---------------------|--|
| | <i>service_name</i> | Represents the name of the service you want to affect, for example: <ul style="list-style-type: none">• System NTP• System SSH• Service Manager• A Cisco DB• Cisco Database Layer Monitor• Cisco Unified Serviceability |
| | | This list is not exhaustive. For a full list of services for the node enter the command: utils service list |

Note If you want to restart the Cisco Tomcat service for standalone Cisco Prime License Manager, execute the following command or reboot the server: **utils service restart Cisco Prime LM Server.**

| | |
|---|------------------------|
| Command Modes | Administrator (admin:) |
| Requirements | |
| Command privilege level: 1 | |
| Allowed during upgrade: No | |
| Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection | |

utils service list

This command retrieves a list of all services.

utils service list [page]

| Syntax Description | Parameters | Description |
|--------------------|------------|---|
| | [page] | Displays the output one page at a time. |

| | |
|---|------------------------|
| Command Modes | Administrator (admin:) |
| Requirements | |
| Command privilege level: 0 | |
| Allowed during upgrade: No | |
| Applies to: IM and Presence service on Unified Communications Manager | |

utils service auto-restart

This command starts or stops a specified service.

```
utils service auto-restart {enable | disable | show}
  service-name
```

| Syntax Description | Parameters | Description |
|--------------------|---------------------|---|
| | enable | Starts auto-restart. |
| | disable | Stops auto-restart. |
| | show | Shows the status of a service. |
| | <i>service-name</i> | Represents the name of the service that you want to start, stop, or show: <ul style="list-style-type: none"> • System NTP • System SSH • Service Manager • A Cisco DB • Cisco Tomcat • Cisco Database Layer Monitor • Cisco Unified Serviceability |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils service start

This command starts a service.

```
utils service start
```

utils service stop

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>service</i> Enter the name of a service, which can consist of multiple words. |
| Command Modes | Administrator (admin:) |
| Requirements | |
| | Command privilege level: 1 |
| | Allowed during upgrade: No |
| | Applies to: Unified Communications Manager, IM and Presence service onUnified Communications Manager, and Cisco Unity Connection |

utils service stop

This command stops a service.

utils service stop

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>service</i> Enter the name of a service, which can consist of multiple words. |
| Command Modes | Administrator (admin:) |
| Requirements | |
| | Command privilege level: 1 |
| | Allowed during upgrade: No |
| | Applies to: Unified Communications Manager, IM and Presence service onUnified Communications Manager, and Cisco Unity Connection |

utils snmp config 1/2c community-string

This interactive command adds, deletes, lists or updates a community string.

utils snmp config 1/2c community-string {add | delete | list | update}

| Syntax Description | Parameters Description |
|--------------------|---|
| | add Adds a new community string. |
| | delete Deletes a community string. |
| | list Lists all community strings. |
| | update Updates a community string. |

Command Modes Administrator (admin:)

Usage Guidelines The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status of “SNMP Master Agent” by using `utils service list`. If service is down, start it by using `utils service start SNMP Master Agent`

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 1/2c inform

This interactive command adds, deletes, lists or updates inform notification destinations.

utils snmp config 1/2c inform {add | delete | list | update}

Syntax Description

Parameters Description

| | |
|---------------|--------------------------------------|
| add | Adds a notification destination. |
| delete | Deletes a notification destination. |
| list | Lists all notification destinations. |
| update | Updates a notification destination. |

Command Modes

Administrator (admin:)

Requirements

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 1/2c trap

This interactive command affects trap notifications.

utils snmp config 1/2c trap {add | delete | list | update}

Syntax Description

Parameters Description

| | |
|------------|---|
| add | Adds a new v1/2c trap notification destination associated with a configured v1/2c community string. |
|------------|---|

utils snmp config 3 inform

Parameters Description

delete Deletes the configuration information for an existing v1/2c trap notification destination.

list Lists the v1/2c trap notifications currently configured.

update Updates configuration information for an existing v1/2c trap notification destination.

Command Modes Administrator (admin):

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

utils snmp config 3 inform

This interactive command affects the v3 inform notification.

utils snmp config 3 inform {add | delete | list | update}

Syntax Description

Parameters Description

add Adds a new v3 inform notification destination associated with a configured v3 username.

delete Deletes the configuration information for an existing v3 inform notification destination.

list Lists the v3 inform notifications currently configured.

update Updates configuration information for an existing v3 inform notification destination.

Command Modes Administrator (admin):

Usage Guidelines

The system prompts you for the parameters.

The SNMP Master Agent service is restarted for configuration changes to take effect. Do not abort command after execution until restart is complete. If the command is aborted during service restart, verify service status of “SNMP Master Agent” by using `utils service list`. If service is down, start it by using `utils service start SNMP Master Agent`

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config mib2

This interactive command affects the Mib2 configuration information.

utils snmp config mib2 {add | delete | list | update}

Syntax Description

Parameters Description

| | |
|---------------|---|
| add | Adds the Mib2 configuration information. |
| delete | Deletes the Mib2 configuration information. |
| list | Lists the Mib2 configuration information. |
| update | Updates the Mib2 configuration information. |

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 3 trap

This interactive command affects trap notifications.

utils snmp config 3 trap {add | delete | list | update}

Syntax Description

Parameters Description

| | |
|---------------|--|
| add | Adds a new v3 trap notification destination associated with a configured v3 username. |
| delete | Deletes the configuration information for an existing v 3 trap notification destination. |
| list | Lists the v3 trap notifications currently configured. |
| update | Updates configuration information for an existing v3 trap notification destination. |

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

utils snmp config 3 user

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp config 3 user

This interactive command affects v3 user configuration.

utils snmp config 3 user {add | delete | list | update}

Syntax Description

Parameters Description

| | |
|---------------|--|
| add | Adds a new v3 user with the v3 authentication and privacy passwords. |
| delete | Deletes the configuration information for an existing v3 user. |
| list | Lists the v3 users currently configured. |
| update | Updates configuration information for an existing v3 user. |

Command Modes

Administrator (admin:)

Usage Guidelines

The system prompts you for the parameters.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp get

This interactive command gets the SNMP data using the specified version for the specified MIB OID.

utils snmp get version

Syntax Description

Parameters

Description

| | |
|------------------|---|
| <i>version</i> | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| <i>community</i> | Specifies the SNMP community string. |

| Parameters | Description |
|-------------------|---|
| <i>ip-address</i> | Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node. |
| <i>object</i> | Specifies the SNMP Object ID (OID) to get. |
| <i>file</i> | Specifies a file in which to save the command output. |

Command Modes Administrator (admin:)

Usage Guidelines If you run the command on a specific OID (leaf) in the MIB, you get the value of the MIB. For example to get the system uptime: `iso.3.6.1.2.1.25.1.1.0 = Timeticks: (19836825) 2 days, 7:06:08.25`

If you provide the IPv4/IPv6 address of a remote host, the command gets executed on the remote host.

The IPv4/IPv6 address is required. You cannot use a domain name.

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp get 1

This command gets the SNMP data using version 1 for the specified MIB OID.

utils snmp get 1 *version*

Syntax Description

| Parameters | Description |
|-------------------|---|
| <i>version</i> | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| <i>community</i> | Specifies the SNMP community string. |
| <i>ip-address</i> | Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node. |
| <i>object</i> | Specifies the SNMP Object ID (OID) to get. |
| <i>file</i> | Specifies a file in which to save the command output. |

 **utils snmp get 2c**

Command Modes Administrator (admin:)
Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp get 2c

This command gets the SNMP data using version 2c for the specified MIB OID.

utils snmp get 2c *version*

| Syntax Description | Parameters | Description |
|--------------------|-------------------|---|
| | <i>version</i> | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| | <i>community</i> | Specifies the SNMP community string. |
| | <i>ip-address</i> | Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node. |
| | <i>object</i> | Specifies the SNMP Object ID (OID) to get. |
| | <i>file</i> | Specifies a file in which to save the command output. |

Command Modes Administrator (admin:)
Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp get 3

This command gets the SNMP data for the specified MIB OID.

utils snmp get 3 *version*

| Syntax Description | Parameters | Description |
|--------------------|------------------|---|
| | <i>version</i> | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| | <i>community</i> | Specifies the SNMP community string. |

| Parameters | Description |
|-------------------|---|
| <i>ip-address</i> | Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node. |
| <i>object</i> | Specifies the SNMP Object ID (OID) to get. |
| <i>file</i> | Specifies a file in which to save the command output. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp hardware-agents

This command affects the SNMP agents on the server.

utils snmp hardware-agents {status | start | stop | restart}

Syntax Description

| Parameters | Description |
|----------------|--|
| status | Displays the status of the SNMP agents provided by the vendor of the hardware. Note Only agents that provide status get displayed by this command. Not all hardware agents provide status. |
| stop | Stops all SNMP agents provided by the hardware vendor. |
| restart | Restarts all of the SNMP agents provided by the vendor of the hardware. |
| start | Starts all of the SNMP agents provided by the vendor of the hardware. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils snmp test

This command sends sample alarms to local syslog and remote syslog.

utils snmp test

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

Example

```
admin: admin:utils snmp test
Service Manager is running
Test SNMP Trap starts with Local Host Name, Specify a Remote Sever Name to test Remote
Syslog
TestAlarmInformational sent [Returncode=0]
TestAlarmEmergency sent [Returncode=0]
TestAlarmAlert sent [returncode=0]
TestAlarmCritical sent [Returncode=0]
TestAlarmDebug sent [Returncode=0]
TestAlarmNotice sent [Returncode=0]
TestAlarmWarning sent [Returncode=0]
TestAlarmError sent [Returncode=0]
TestAlarmWindows sent [Returncode=0]
Message from syslogd@ipcbu-plat44 at Sat Jul 17 03:56:11 2010 ...
ipcbu-plat44 local7 0 : 1: ipcbu-plat44.blr.eng: Jul 16 2010 22:26:11.53 UTC :
%UC_-0-TestAlarmEmergency: %[AppID=Cisco CallManager] [ClusterID=] [NodeID=ipcbu-plat44]:
Testing EMERGENCY_ALARM
```

utils snmp walk

This interactive command command walks through the SNMP MIB using the specified version, starting with the specified OID.

utils snmp walk *version*

Syntax Description

| Parameters Description | |
|-------------------------------|---|
| <i>version</i> | Specifies the SNMP version. Possible values include 1, 2c or 3. |
| <i>community</i> | Specifies the SNMP community string. |
| <i>ip-address</i> | Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node. |
| <i>object</i> | Specifies the SNMP Object ID (OID) to walk |
| <i>file</i> | Specifies a file in which to save the command output. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

Example

For the below example, community string is created using the `utils snmp config 1/2c community-string` command.

```
admin:utils snmp walk 1
ctrl-c: To quit the input.
```

```
Enter the community string:: public
Enter the ip address of the Server, use 127.0.0.1 for localhost.
Note that you need to provide the IP address, not the hostname:: <enter the IP address of
your server>
The Object ID (OID):: iso.3.6.1.2.1.1.1.0
Enter parameter as "file" to log the output to a file. [nofile]::
This command may temporarily impact CPU performance.
Continue (y/n)?y
SNMPv2-MIB::sysDescr.0 = STRING: Linux release:3.10.0-1062.18.1.el7.x86_64 machine:x86_64
#####
utils snmp walk 2c -> same as utils snmp walk 1
#####
For the below example, user is created using
utils snmp config 3 user add
```

```
utils snmp walk 3
admin:utils snmp walk 3
ctrl-c: To quit the input.
```

```
Enter the user name:: test
Enter the authentication protocol [SHA]:: SHA
Enter the authentication protocol pass phrase:: ****
Enter the privacy protocol [AES128]:: AES128
```

utils snmp walk 1

```

Enter the privacy protocol pass phrase:: *****
Enter the ip address of the Server, use 127.0.0.1 for localhost.
Note that you need to provide the IP address, not the hostname::: <enter the IP address of
your server>
The Object ID (OID):: iso.3.6.1.2.1.1.0
Enter parameter as "file" to log the output to a file. [nofile]::
This command may temporarily impact CPU performance.
Continue (y/n)?y
SNMPv2-MIB::sysDescr.0 = STRING: Linux release:3.10.0-1062.18.1.el7.x86_64 machine:x86_64

```

utils snmp walk 1

This interactive command walks through the SNMP MIB using SNMP version 1 starting with the specified OID

utils snmp walk 1 *version*

| Syntax Description | Parameters Description |
|--------------------|---|
| | <i>version</i> Specifies the SNMP version. Possible values include 1, 2c or 3. |
| | <i>community</i> Specifies the SNMP community string. |
| | <i>ip-address</i> Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node. |
| | <i>object</i> Specifies the SNMP Object ID (OID) to walk |
| | <i>file</i> Specifies a file in which to save the command output. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp walk 2c

This interactive command walks through the SNMP MIB using SNMP version 2c starting with the specified OID.

utils snmp walk 2c *version*

| Syntax Description | Parameters Description |
|--------------------|--|
| | <i>version</i> Specifies the SNMP version. Possible values include 1, 2c or 3. |

Parameters Description

community Specifies the SNMP community string.

ip-address Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.

object Specifies the SNMP Object ID (OID) to walk

file Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils snmp walk 3

This interactive command walks through the SNMP MIB starting with the specified OID.

utils snmp walk 3 *version***Syntax Description**

Parameters Description

version Specifies the SNMP version. Possible values include 1, 2c or 3.

community Specifies the SNMP community string.

object Specifies the SNMP Object ID (OID) to walk

ip-address Specifies the IPv4/IPv6 address of the server. Enter 127.0.0.0 to specify the local host. You can enter the IPv4/IPv6 address of another node in the cluster to run the command on that node.

file Specifies a file in which to save the command output.

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, Cisco Unity Connection

utils soap realtimeservice test

utils soap realtimeservice test

This command executes a number of test cases on the remote server.

utils soap realtimeservice test [remote-ip]remote-httpsremote https-password

| Syntax Description | Parameters | Description |
|--------------------|------------------------------|--|
| | <i>remote-ip</i> | Specifies the IP address of the server under test. |
| | <i>remote-https-user</i> | Specifies a username with access to the SOAP API. |
| | <i>remote-https-password</i> | Specifies the password for the account with SOAP API access. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on IM and Presence, Cisco Unity Connection

utils sso

This command provides information about SAML SSO authentication.

utils sso {enable | disable | status}

| Syntax Description | Parameters | Description |
|--------------------|----------------|---|
| | enable | Provides the location in Cisco Unified CM Administration where you can enable SAML SSO. |
| | disable | Disables SAML SSO based authentication. |
| | status | Provides the status of SAML SSO. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

Example

```
Admin: utils sso enable
*** W A R N I N G ***
SSO cannot be enabled using CLI command
=====
To enable Cluster wide SAML SSO please access
Cisco Unified CM Administration Page->System->SAML Single Sign On
=====
```

utils sso recovery-url

This command enables or disables recovery URL for SAML SSO based authentication.

utils sso recovery-url {enable | disable}

| Syntax Description | Parameters Description |
|--------------------|---|
| | enable Enables recovery URL for SAML SSO based authentication. |
| | disable Disables recovery URL for SAML SSO based authentication. |

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system restart

This command allows you to restart the system on the same partition.

utils system restart

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils system shutdown

utils system shutdown

This command allows you to shut down the system.

utils system shutdown

Command Modes

Administrator (admin:)

Usage Guidelines

This command has a five-minute timeout. If the system does not shut down within five minutes, the command gives you the option of doing a forced shutdown.



Caution If the server is forced to shutdown and restart from your virtual machine, the file system may become corrupted.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils system switch-version

This command allows you to restart the system on the inactive partition.

utils system switch-version

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system boot

This command redirects where the system boot output gets sent.

utils system boot {console | serial}

| Syntax Description | Parameters | Description |
|--------------------|----------------|---|
| | <i>console</i> | Redirects the system boot output to the console. |
| | <i>serial</i> | Redirects the system boot output to the COM1 (serial port 1). |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager and Cisco Unity Connection

utils system upgrade

This command allows you to install upgrades and Cisco Option (COP) files from both local and remote directories.

utils system upgrade {initiate | cancel | status}

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | cancel | Cancels the active upgrade. |
| | initiate | Starts a new upgrade wizard or assumes control of an existing upgrade wizard. The wizard prompts you for the location of the upgrade file from the source. |
| | status | Displays the status of an upgrade. |

| | |
|---------------|------------------------|
| Command Modes | Administrator (admin:) |
|---------------|------------------------|

| | |
|------------------|---|
| Usage Guidelines | The wizard prompts you to enter information about your upgrade: |
|------------------|---|

- Credentials Information—Make sure that you have the credentials of the server on which the upgrade image is saved. If you are not upgrading the Unified Communications Manager publisher node, and you have previously upgrade this node, you can use download credentials from the publisher node. The default value of the Use download credentials from Publisher is yes.



Note You can use download credentials from the publisher node only when you upgrade individual cluster node. This option is not applicable for cluster-wide upgrade.

- Upgrade file source—Enter the location for the server where your upgrade file is saved. You can upgrade from a local source(CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.

- Continue with upgrade after download—You must indicate whether you want the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you choose to upgrade automatically, no checksum or SHA details get displayed. If you set the value of to yes or no, the setting remains in the system.
- Version switching—You must indicate whether you want to switch to the new version automatically once the upgrade completes (the default value is no). If you enter yes, the system switches to the new version and reboots automatically after the upgrade completes. If you set the value to yes or no, the setting remains in the system.

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection.



Note If a cluster upgrade is in progress, and another upgrade is initiated using CLI, then the following message is displayed:

A cluster upgrade is in progress. You can check the status of the cluster upgrade using the CLI or GUI of the CUCM Publisher.

Example:

```
admin:utils system upgrade initiate

Warning: Do not close this window without first canceling the upgrade.
Warning: A cluster upgrade is in progress. You can check the status of the cluster upgrade
using the CLI or GUI of the CUCM Publisher.

Use download credentials from Publisher(yes/no) [yes]:no

Source:

1) Remote Filesystem via SFTP
2) Remote Filesystem via FTP
3) Local DVD/CD
4) Local Image<UCSInstall_UCOS_12.5.0.98000-889.iso>
q) quit
Please select an option (1 - 4 or "q" ): 4

Please enter SMTP Host Server (optional):
Checking for valid upgrades.
Please wait...
Available options and upgrades in "upgrade" directory:
1) UCSInstall_UCOS_12.5.0.98000-338.iso
q) quit
Please select an option (1 - 1 or "q" ): 1
Accessing the file.
Please wait...
Validating the file...
A system reboot is required when the upgrade process completes or is canceled.
This will ensure services affected by the upgrade process are functioning properly.
Downloaded: UCSInstall_UCOS_12.5.0.98000-338.iso
File version: 12.5.0.98000-338
```

```
File checksum : (MD5): 8f:ce:0b:12:6b:d5:6f:d5:fd:25:d9:aa:12:d0:d5:30
(SHA512):
84ac0fd21723173ae89f1c01926a0852f46941c1785ae8e55dc8eb426dd9fb42fd1ce07e0c9e3ac7db01a4f7812f239fc38390dc2bc44d5161ebf13617c3050
Automatically switch versions if the upgrade is successful (yes/no): yes
Start installation (yes/no): yes
```

Example:

```
admin:utils system upgrade initiate

Warning: Do not close this window without first canceling the upgrade.

Use download credentials from Publisher (yes/no) [yes]:yes
Using publisher setting
Checking for valid upgrades. Please wait...
Available options and upgrades in "10.65.104.39:/var/sftp/uploads":
1.dp-ffr.3-1-7.NL.k3.cop q) quit
Please select an option (1 - 1 or "q" ):
```

Example:

```
admin:utils system upgrade initiate

Warning: Do not close this window without first canceling the upgrade.
Use download credentials from Publisher(yes/no) [yes]:no

Source:

1) Remote Filesystem via SFTP
2) Remote Filesystem via FTP
3) Local DVD/CD
4) Local Image<UCSInstall_UCOS_12.5.0.98000-889.iso>
q) quit
Please select an option (1 - 4 or "q" ): 4

Please enter SMTP Host Server (optional):
Continue with upgrade after download (yes/no) [yes]:
switch-version server after upgrade (yes/no) [no]
Checking for valid upgrades.
Please wait...
Available options and upgrades in "upgrade" directory:
1) UCSInstall_UCOS_12.5.0.98000-338.iso
q) quit
Please select an option (1 - 1 or "q" ): 1
Accessing the file.
Please wait...
Validating the file...
A system reboot is required when the upgrade process completes or is canceled.
This will ensure services affected by the upgrade process are functioning properly.
Downloaded: UCSInstall_UCOS_12.5.0.98000-338.iso
File version: 12.5.0.98000-338
Automatically switch versions if the upgrade is successful (yes/no): yes
Start installation (yes/no): yes
```

utils system upgrade cluster

utils system upgrade cluster

This command allows you to install upgrades for cluster nodes (Unified Communications Manager and IM and Presence) and Cisco Option Package (COP) files from both local and remote directories.

utils system upgrade cluster {initiate | cancel | status}

| Syntax Description | Parameters | Description |
|--------------------|-----------------|--|
| | cancel | Cancels the active upgrade. |
| | initiate | <p>Starts a new upgrade wizard or assumes control of an existing cluster upgrade wizard.</p> <p>This option allows you to perform a cluster-wide upgrade from the Unified Communications Manager publisher.</p> <p>This option is available only for the Unified Communications Manager publisher and not for the Unified Communications Manager subscriber or IM and Presence nodes.</p> |
| | status | <p>Displays the status of an upgrade for each node in the cluster with the following fields:</p> <ul style="list-style-type: none"> • Node—The hostname of the node. • Role—The role of the node. • Step—The current Step number or the Total number of steps to be executed for upgrade completion. • Description—The current component which is currently upgrading for the particular node. • Historical Time—The amount of time taken to complete the current component/step for the respective node based on previous clusterwide upgrade runs. • Elapsed Time—The amount of time that passes from the start of the current component/step to its finish for the respective node. |

Command Modes Administrator (admin:)

Usage Guidelines The wizard prompts you to enter information about your upgrade:

- Credentials Information—Make sure that you have the credentials of the server on which the upgrade image is saved.
- Upgrade file source—Enter the location for the server where your upgrade file is saved. You can upgrade from a local source(CD or DVD), or you can use FTP or SFTP to download a remote upgrade file, or if you want to resume an upgrade after a cancel operation, you can use the previously downloaded upgrade file through the local image source option.

- Continue with upgrade after download—You must indicate whether you want the upgrade to proceed automatically once the upgrade file is downloaded (the default value is yes). If you choose to upgrade automatically, no checksum or SHA details get displayed. If you set the value of to yes or no, the setting remains in the system.
- Version switching—You must indicate whether you want to switch to the new version automatically once the upgrade completes (the default value is no). If you enter yes, the system switches to the new version and reboots automatically after the upgrade completes. If you set the value to yes or no, the setting remains in the system.

Requirements

Command privilege level: 0

Applies to: Unified Communications Manager on Unified Communications Manager.



Note If a single-node upgrade is in progress, and a cluster upgrade is initiated, then, the following message is displayed:

```
failed (Local upgrade is in progress.)
```

If a single-node upgrade is in progress in Unified Communication Manager publisher, either using CLI or User Interface, if you initiate a cluster upgrade using CLI, then the following message is displayed:

```
A Single-node upgrade is in progress. You can cancel the upgrade to initiate Cluster upgrade.
```

If a cluster upgrade session is in progress in Unified Communication Manager publisher either using User Interface or CLI, if you initiate another cluster session using CLI, then the following message is displayed:

```
Another user session is currently configuring a cluster upgrade. Assume control (yes/no):  
yes
```

Example:

```
admin:utils system upgrade cluster initiate
```

```
Warning: Do not close this window without first canceling the upgrade.
```

Source:

```
1) Remote Filesystem via SFTP  
2) Remote Filesystem via FTP  
3) Local DVD/CD  
4) Local Image<None>  
q) quit  
Please select an option (1 - 4 or "q" ): 1  
Directory [/home/image/BOTH]:  
Server [10.65.104.19]:  
User Name [image]:  
Password [*****]:  
Please enter SMTP Host Server (optional):  
Continue with upgrade after download (yes/no) [no]:  
Switch-version cluster after upgrade [valid only for ISO] (yes/no) [no]:
```

```
Checking for valid upgrades. Please wait...
```

```
Available CUCM options and upgrades in "10.65.104.19:/home/image/BOTH":
```

utils system upgrade cluster

```

1) UCSInstall_UCOS_12.5.0.98000-541.iso
2) UCSInstall_UCOS_UNRST_12.5.0.98000-541.iso
3) ciscocomm.free_common_space_v1.1.cop
4) ciscocomm.migrate-export-v1.20.cop.sgn
q) quit
Please select an option (1 - 4 or "q" ): 1

Available IMP options and upgrades in "10.65.104.19:/home/image/BOTH":

1) UCSInstall_CUP_12.5.0.98000-661.iso
2) UCSInstall_CUP_UNRST_12.5.0.98000-661.iso
3) ciscocomm.free_common_space_v1.1.cop
4) ciscocomm.migrate-export-v1.20.cop.sgn
q) quit

Please select an option (1 - 4 or "q" ): 1
Processing the cluster wide download ...
UCM1-PUB.ciscoctg.com           Downloading..287mb
UCM1-SUB-1B.ciscoctg.com         Downloading..115mb
UCM1-SUB-1A.ciscoctg.com         Downloading..347mb
IMP1-SUB-1B.ciscoctg.com         failed (Local upgrade is in progress.)
UCM1-SUB-2B.ciscoctg.com         Downloading..490mb
IMP1-PUB.ciscoctg.com            Downloading..55mb
UCM1-SUB-2A.ciscoctg.com         failed
Exiting upgrade command. Please wait...

```

Example:

```

admin:utils system upgrade cluster initiate

Warning: Do not close this window without first canceling the upgrade.
Cluster upgrade is in progress. You may not take over the installation.
Source:
1) Remote Filesystem via SFTP
2) Remote Filesystem via FTP
3) Local DVD/CD
4) Local Image <UCSInstall_UCOS_12.5.0.98000-569.iso>
q) quit

Please select an option (1 - 4 or "q" ): 4
Please enter SMTP Host Server (optional):
Continue with upgrade after download (yes/no) [no]: no
Switch-version cluster after upgrade [valid only for ISO] (yes/no) [no]: no
Checking for valid upgrades. Please wait...
Available CUCM options and upgrades in "upgrade" directory:
1) UCSInstall_UCOS_12.5.0.98000-569.iso
q) quit
Please select an option (1 - 1 or "q" ): 1
Available IMP options and upgrades in "upgrade" directory:
1) UCSInstall_CUP_12.5.0.98000-695.iso
q) quit
Please select an option (1 - 1 or "q" ): 1
Processing the cluster wide download ...
UCM1-SUB-1B.ciscoctg.com         Download complete
UCM1-SUB-2A.ciscoctg.com         Download complete
IMP1-SUB-1B.ciscoctg.com         Download complete
UCM1-SUB-1A.ciscoctg.com         Download complete
UCM1-PUB.ciscoctg.com            Download complete
UCM1-SUB-2B.ciscoctg.com         Download complete
IMP1-PUB.ciscoctg.com            Download complete

```

```

Cluster wide Download complete
A system reboot is required when the upgrade process is complete or cancelled.
This will ensure the services affected by the upgrade process are functioning properly
Downloaded UCM Image: UCSInstall_UCOS_12.5.0.98000-569.iso
File version: 12.5.0.98000-569
File checksum : (MD5): 66:93:bc:4d:c5:ae:19:34:72:77:96:5a:be:1a:28:3d
                  (SHA512): fdaab4a67072528927a2a6c9600b761e086af4894ac0b
                               85221e731fea864567674f6ac2c806fb2a8a05d
                               fe31485ef92ca63f8f4d37448d30715c79bf2738dfd2
Downloaded IMP Image: UCSInstall_CUP_12.5.0.98000-695.iso
File version: 12.5.0.98000-695
File checksum : (MD5): 9e:f3:4e:e0:49:e3:c5:44:16:a5:f9:0e:8d:d5:a7:36
                  (SHA512): 57393dd5e70d43137d5ffb906fd815097f66a5a33e1fc
                               24bf4b6ed86894a6e0794f5f2165bc8395d2217
                               e24ae0b05b4d168b52ae480e5c9f7a29b7170f2ed92a
The IMP servers in the cluster must be rebooted after Unified CM publisher is switched
to the new version, even IF IMP servers are not being being upgraded
Automatically switch versions if the upgrade is successful (yes/no): no
Start installation (yes/no): yes
Cluster-wide upgrade has been initiated...

```

| Node | Role | Step | Description | Historical time to complete | Elapsed Time |
|-----------|-----------------|---------|-----------------|-----------------------------|--------------|
| Ucm_Pub1 | CUCM Publisher | 1/15 | Installing | 1:37:13 | 00:07:14 |
| IM&P_Pub1 | IM&P Publisher | 0/15 | Waiting on Pub | 1:20:13 | |
| Ucm_Sub1 | CUCM Subscriber | 0/15 | Waiting on Pub | 1:37:13 | |
| Cluster | None | overall | Overall upgrade | 4:34:26 | 00:07:14 |

utils system enableAdministration

Configuration changes are not permitted during an upgrade; however, you can use this command to enable emergency provisioning during an upgrade.



Caution

Once you begin the upgrade process, configuration changes are not permitted until the upgrade is complete and you have performed all of the post-upgrade tasks. Configuration changes include:

- changes made through any of the Unified Communications Manager or IM and Presence Service graphical user interfaces (GUI), the command line interface (CLI), or the AXL API
- LDAP synchronizations, including incremental synchronizations that are pushed to Unified Communications Manager from an Oracle LDAP
- automated jobs
- devices attempting to autoregister

Any configuration changes that you make during an upgrade may be lost, and some configuration changes can cause the upgrade to fail.

utils system enableAdministration

Command Modes

Administrator (admin:)

utils update dst

Requirements

Command privilege level: 1 and 4

utils update dst

This command updates the daylight saving time (DST) rules for the current year.

utils update dst

Command Modes

Administrator (admin:)

Usage Guidelines

This command takes a backup of the existing DST rules file and creates a new DST rules file for the current year.



Caution Restart the phones after you execute the command. Not restarting the phones results in wrong DST start and stop dates.

Requirements

Command privilege level: 0

Allowed during upgrade: No

Applies to Unified Communications Manager and IM and Presence service.

utils users validate

This command checks user records across all nodes and clusters in the deployment to identify duplicate or invalid userid or directory URI values.

utils users validate {all | userid | uri}

Syntax Description

Parameters Description

| | |
|---------------|---|
| all | Validate the userid and directory URI values for all users in the nodes and clusters. |
| userid | Validate the userid value for all users in the nodes and clusters. |
| uri | Validate the directory URI value for all users in the nodes and clusters. |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: IM and Presence Service on Unified Communications Manager

utils vmtools refresh

This command refreshes the currently installed VMware Tools to the latest version that is prescribed by the ESXi host for that VM.



Note After the initial reboot, VMware Tools are in the **running** state. When you upgrade to a newer version of VMware Tools, selinux may initially block the installation. In this case, the system still allows VMware Tools to install, but a new dynamic policy is generated to suppress any additional selinux blockage. You can view the new dynamic policy with the **utils os secure dynamic-policies list** command. For more information, see the **utils os secure dynamic-policies** CLI command.



Note This is applicable for native vmtools.

utils vmtools refresh

Command Modes Administrator (admin:)

Usage Guidelines To update the current version of the VMware Tools, select **Guest > Install/Upgrade VMWare Tools > Interactive Tools Upgrade**.

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection.

Example

```
admin:utils vmtools refresh
VMware Tools match host. Upgrade allowed, though not required.
```

```
*** W A R N I N G ***
Running this command will update your current version of VMware Tools
to the latest version prescribed by the ESXi host on which this VM is
running. The tools install will cause your system to reboot twice.
```

utils vmtools status

This command displays the type and the version of currently installed VMware Tools.

utils vmtools switch open

utils vmtools status

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils vmtools switch open

This command uninstalls the currently installed native VMware Tools and installs the open VMware Tools.

utils vmtools switch open

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils vmtools switch native

This command uninstalls the currently installed open VMware Tools and installs the native VMware Tools.

utils vmtools switch native

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: No

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system boot status

This command shows the location where the system boot messages are to be sent. The location is either console or serial port one.

utils system boot status**Command Modes**

Administrator (admin:)

Requirements

Command privilege level: 0

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, Cisco Unity Connection

utils system upgrade dataexport initiate

This command exports the nodes configuration and user data to a remote SFTP server, for use in a later fresh install with data import.

utils system upgrade dataexport initiate**Syntax Description**

| Parameters | Description |
|---------------------------------|----------------------------|
| Export Data Directory | Remote directory |
| Remote Server Name or IP | Remote SFTP |
| Remote Server Login ID | Username of remote server |
| Remote Server Password | Password for remote server |
| New Hostname | Destination hostname |
| New IP Address | Destination IP |

Command Modes

Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence Service on Unified Communications Manager, and Cisco Unity Connection

**Note**

This command should be executed on Publisher first followed by all subscriber nodes in the cluster. Same SFTP Remote server details should be configured for all nodes in the cluster.

```
utils system upgrade dataexport status
```

utils system upgrade dataexport status

This command displays the status of the dataexport operation for this cluster node.

```
utils system upgrade dataexport status
```

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection

utils system upgrade dataexport cancel

This command cancels the ongoing dataexport operation.

```
utils system upgrade dataexport cancel
```

Command Modes Administrator (admin:)

Requirements

Command privilege level: 1

Allowed during upgrade: Yes

Applies to: Unified Communications Manager, IM and Presence service on Unified Communications Manager, and Cisco Unity Connection