



Mapping ACNS Software CLI Commands to the Content Distribution Manager GUI

This appendix lists the CLI commands that are supported and unsupported in the ACNS 5.4 Content Distribution Manager GUI. It contains the following sections:

- [CLI Commands Supported in the Content Distribution Manager GUI, page D-1](#)
- [CLI Commands Not Supported in the Content Distribution Manager GUI, page D-27](#)

CLI Commands Supported in the Content Distribution Manager GUI

[Table D-1](#) maps ACNS software CLI commands to the corresponding Content Distribution Manager GUI procedure. Software CLI commands are listed in alphabetical order in the first column. The second column indicates the GUI navigation path to the device group configuration window for each command. The third column provides a link to the GUI configuration procedure found elsewhere in this guide. In most cases, the procedure provides an illustration of the configuration window and a table at the end of the procedure that maps each field in the GUI window to its corresponding CLI command.



Note

Most of the procedures in this guide document the configuration steps for individual devices, whereas this table provides the GUI navigation path to the device group configuration window, unless otherwise indicated. The procedures for configuring device groups and individual devices are the same in most cases.

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map

Command	GUI Navigation Path	Procedure Reference
aaa accounting { commands {0 15} default { start-stop stop-only wait-start } tacacs exec default { start-stop stop-only wait-start } tacacs system default { start-stop stop-only } tacacs }	Devices > Device Groups > General Settings > Authentication > AAA Accounting	Configuring AAA Accounting, page 12-27
access-lists 300 { deny groupname { any [position number] groupname [position number]}} { permit groupname { any [position number] groupname [position number]}}	Devices > Devices ¹ > General Settings > Authentication > Access List > Configure Access Control List	Configuring an Access Control List for Group Authorization, page 18-1
access-lists enable	Devices > Devices > General Settings > Authentication > Access List > Enable Access Control List	Enabling the Access Control List, page 18-2
acquirer proxy authentication outgoing <i>ipaddress port_num username</i> [password password] [ntlm domain [basic-auth-disable]]	Devices > Device Groups > Applications > Web > HTTP > HTTP Connections	Configuring Authentication for an HTTP Proxy Using the Content Distribution Manager GUI, page 6-45
acquirer proxy authentication transparent <i>username</i> [password password] [ntlm domain [basic-auth-disable]]	Devices > Device Groups > Prepositioning > Acquirer WCCP Proxy Authentication	Configuring Authentication for a WCCP Proxy Using the Content Distribution Manager GUI, page 6-46
asset tag <i>name</i>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Asset Tag	Configuring SNMP Asset Tag Settings, page 22-11
authentication { configuration login } { local radius tacacs } enable primary [secondary tertiary]	Devices > Device Groups > General Settings > Authentication > Login Authentication	Configuring Devices for Login Authentication and Authorization, page 12-7
authentication fail-over server-unreachable		
bandwidth { real-proxy { incoming <i>kbits</i> outgoing <i>kbits</i> } real-server <i>kbits</i> wmt { incoming <i>kbits</i> outgoing <i>kbits</i> } cisco-streaming-engine <i>kbits</i> http <i>kbits</i> } { start-time <i>weekday time</i> end-time <i>weekday time</i> }	Devices > Device Groups > Applications > Bandwidth Schedules	Configuring Scheduled Bandwidth Settings, page 9-39
bandwidth { real-proxy { incoming <i>kbits</i> outgoing <i>kbits</i> } real-server <i>kbits</i> wmt { incoming <i>kbits</i> outgoing <i>kbits</i> } cisco-streaming-engine <i>kbits</i> http <i>kbits</i> } { default max-bandwidth }	Devices > Device Groups > Applications > Default and Maximum Bandwidth	Configuring Content Services Default and Maximum Bandwidth Settings, page 9-38
banner { motd login exec } message <i>message_text</i> banner enable	Devices > Device Groups > General Settings > Login Access Control > Message of the Day	Configuring Message of the Day Settings for the Content Engine, page 20-5

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
bitrate http default <i>bitrate</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
bitrate wmt incoming <i>bitrate</i>		
bitrate wmt outgoing <i>bitrate</i>		
bypass auth-traffic enable	Devices > Device Groups > Request Routing > WCCP > Bypass	Configuring WCCP Bypass Settings, page 4-23
bypass load {enable in-interval <i>seconds</i> out-interval <i>seconds</i> time-interval <i>minutes</i> }		
bypass static { <i>clientip</i> { <i>serverip</i> any-server} any-client <i>serverip</i> }	Devices > Device Groups > Request Routing > WCCP > Bypass List	Creating WCCP Bypass List Entries, page 4-25
bypass timer <i>minutes</i>	Devices > Device Groups > Request Routing > WCCP > Bypass	Configuring WCCP Bypass Settings, page 4-23
bypass gateway <i>ipaddress</i>		
error-handling {reset-connection send-cache-error transparent}		
cdp enable	Devices > Device Groups > General Settings > Services > CDP	Configuring CDP Settings, page 20-7
cdp holdtime <i>seconds</i>		
cdp timer <i>seconds</i>		
clock timezone <i>timezone offset</i>	Devices > Device Groups > General Settings > Services > Date/Time > Time Zone	Configuring Device Clock and Time Zone Settings, page 20-12
clock summertime <i>timezone</i> {date recurring}		
cms database maintenance full enable	Devices > Device Groups > General Settings > Services > Database Maintenance	See the <i>Cisco ACNS Software Update and Maintenance Guide, Release 5.x</i>
cms database maintenance full schedule {every-day weekday at time}		
cms database maintenance regular enable		
cms database maintenance regular schedule {every-day weekday at time}		
Content Router global configuration command: contentrouting leastloaded	Devices > Devices > Device Activation	Enabling Load-Based Routing on the Content Router, page 4-55
contentrouting servicemonitor {numberofsamples {all number cpu number disk number wmt number} sampleperiod {all seconds cpu seconds disk seconds wmt seconds} threshold {cpu percentage wmt percentage} type {all cpu disk wmt}}	Devices > Device Groups > General Settings > Notification and Tracking > Service Monitor	Configuring Content Engine Threshold Limits for Load-Based Routing, page 4-56
dns min-ttl <i>seconds</i>	Devices > Devices ¹ > Applications > DNS > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
dns max-ttl <i>seconds</i>		
dns user-expired enable		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
dns max-cache-memory <i>mbytes</i>	Devices > Device Groups > General Settings > Services > DNS	Configuring the DNS Server for HTTP Proxy Caching, page 8-78
	Devices > Devices ¹ > Applications > DNS > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
dns enable	Devices > Device Groups > General Settings > Services > DNS	Configuring the DNS Server for HTTP Proxy Caching, page 8-78
	Devices > Devices ¹ > Applications > DNS > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
dns listen { all <i>ipaddress</i> } port <i>port_num</i> hostname <i>hostname</i>	Devices > Devices ¹ > Applications > DNS > DNS Server Binding	Configuring DNS Server Bindings for the Content Engine, page 8-74
dns use-original-server { only after-configured before-configured }	Devices > Devices ¹ > Applications > DNS > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
dns pin { forward <i>hostname ipaddress</i> reverse <i>hostname ipaddress</i> both <i>hostname ipaddress</i> cname <i>records</i> }	Devices > Device Groups > Request Routing > DNS > A-Record Mapping	Configuring DNS Address Record Mappings for the Content Engine, page 8-76
	Devices > Device Groups > Request Routing > DNS > CNAME Record Mapping	Configuring DNS Canonical Name Record Mappings for the Content Engine, page 8-77
dns retry-period <i>seconds</i>	Devices > Devices ¹ > Applications > DNS > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
dns retry-timeout <i>seconds</i>		
dns serial-lookup	Devices > Device Groups > General Settings > Services > DNS	Configuring the DNS Server for HTTP Proxy Caching, page 8-78
	Devices > Devices ¹ > Applications > DNS > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
exec-timeout <i>minutes</i>	Devices > Device Groups > General Settings > Login Access Control > Exec Timeout	Configuring Exec Timeout Settings, page 20-6
ftp-native access-list { in out } { <i>std_acl_number</i> <i>acl_name</i> }	Devices > Devices > General Settings > Network > IP ACL Feature Usage	Associating an IP ACL with an Application, page 17-12

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
EXEC mode ftp-native custom-message {download {acl-denied url welcome url} reset {acl-denied all welcome} upload host directory filename {welcome acl-denied}}	Devices > Devices > Applications > Web > FTP > FTP Messages > Upload Devices > Device Groups > Applications > Web > FTP > FTP Messages > Download	Configuring Native FTP Custom Messages, page 8-62
ftp-native object max-size kilobytes	Devices > Device Groups > Applications > Web > FTP > Native FTP Cache Freshness	Configuring Native FTP Cache Freshness, page 8-61
ftp-native proxy active-mode enable	Devices > Device Groups > Applications > Web > FTP > Native FTP Connections	Configuring Native FTP Connections, page 8-58
ftp-native proxy authentication enable		
ftp-native proxy incoming portnum		
ftp-over-http age-multiplier directory-listing dl_time file fo_time	Devices > Device Groups > Applications > Web > FTP > FTP Over HTTP Cache Freshness	Configuring FTP-Over-HTTP Cache Freshness, page 8-55
ftp-over-http max-ttl {days directory-listing dlmax_days file fmax_days hours directory-listing dlmax_hours file fmax_hours minutes directory-listing dlmax_min file fmax_min seconds directory-listing dlmax_sec file fmax_sec}		
ftp-over-http min-ttl min_minutes		
ftp-over-http object max-size size		
ftp-over-http proxy incoming ports		
ftp-over-http proxy outgoing origin-server	Devices > Device Groups > Applications > Web > FTP > FTP Over HTTP Connections	Configuring FTP-Over-HTTP Connection Settings, page 8-52
ftp-over-http proxy outgoing connection-timeout		
ftp-over-http proxy outgoing monitor		
ftp-over-http proxy outgoing host {hostname ipaddress} port		
ftp-over-http proxy anonymous-pswd passwd		
ftp-over-http proxy active-mode enable		
ftp-over-http reval-each-request {all none directory-listing}	Devices > Device Groups > Applications > Web > FTP > FTP Over HTTP Cache Freshness	Configuring FTP-Over-HTTP Cache Freshness, page 8-55
gui-server enable	Devices > Device Groups > General Settings > Login Access Control > GUI Server	Configuring the Content Engine GUI for Secure or Nonsecure Access, page 16-54
gui-server secure enable		
gui-server port port_num		
gui-server secure port port_num		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
<code>hostname name</code>	Devices > Devices > Device Activation	Modifying Content Engine Properties, page 13-9
<code>http add-method method</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Method	Adding or Modifying Additional HTTP Request Methods for the Content Engine, page 8-23
<code>http age-multiplier text num binary num</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache Freshness	Configuring HTTP Cache Freshness Settings, page 8-10
<code>http always-resolve-host</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching	Configuring HTTP Cache Settings, page 8-6
<code>http anonymizer enable</code>		
<code>http append via-header</code>	Devices > Device Groups > Applications > Web > HTTP > Authenticated HTTP Caching	Configuring Authenticated HTTP Cache Settings, page 8-13
<code>http append host-header</code>		
<code>http append x-forwarded-for-header</code>		
<code>http append x-forwarded-for-header multiple-ip-address</code>		
<code>http append proxy-auth-header {ipaddress hostname}</code>		
<code>http append www-auth-header {hostname ipaddress}</code>		
<code>http authenticate-strip-ntlm</code>		
<code>http authentication cache timeout minutes</code>	Devices > Device Groups > Applications > Web > HTTP > Authenticated HTTP Caching	Configuring Authenticated HTTP Cache Settings, page 8-13
<code>http authentication cache max-entries entries</code>		
<code>http authentication header {401 407}</code>		
<code>http authentication realm line</code>		
<code>http cache-authenticated basic</code>		
<code>http cache-authenticated ntlm</code>		
<code>http cache-authenticated all</code>		
<code>http cache-cookies</code>		
<code>http cache-on-abort enable</code>	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching	Configuring Advanced HTTP Cache Settings, page 8-19
<code>http cache-on-abort max-threshold max_thresh</code>		
<code>http cache-on-abort min-threshold min_thresh</code>		
<code>http cache-on-abort percent percentthresh</code>		
<code>http cache-vary-user-agent sub-string string cache-string string</code>	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache User Agent	Configuring HTTP Cache Vary User Agent, page 8-25

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
http cache-vary-user-agent enable	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching	Configuring HTTP Cache Settings, page 8-6
http client-no-cache-request {ignore revalidate}		
http cluster max-delay seconds	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching	Configuring Advanced HTTP Cache Settings, page 8-19
http cluster misses num		
http cluster http-port num		
http cluster heal-port num		
http destination-port {allow deny}	Devices > Device Groups > Web > HTTP > HTTP Destination Port Restrictions	Configuring HTTP Destination Port Restrictions, page 8-26
http dns-cache size max-num	Devices > Device Groups > Request Routing > DNS Caching > DNS Caching Server	Configuring DNS Caching Server Settings for the Content Engine, page 8-71
http dns-cache serial-lookup		
http fast-response enable	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching	Configuring HTTP Cache Settings, page 8-6
http l4-switch {enable spoof-client-ip enable}		
http max-ttl {days text textdays binary bindays hours text texthours binary binhours minutes text textminutes binary binminutes seconds text textseconds binary binseconds}	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache Freshness	Configuring HTTP Cache Freshness Settings, page 8-10
http min-ttl minutes		
http monitor url {url {interval seconds acceptable-delay seconds}}	Devices > Device Groups > Applications > Web > HTTP > HTTP Monitor URL	Monitoring Specified HTTP URLs, page 21-20
http object max-size kbytes	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching	Configuring HTTP Cache Settings, page 8-6
http object url-validation enable		
http persistent-connections [all server-only client-only]	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching	Configuring Advanced HTTP Cache Settings, page 8-19
http persistent-connections timeout seconds		
http proxy incoming ports	Devices > Device Groups > Applications > Web > HTTP > HTTP Connections	Configuring HTTP Cache Settings, page 8-6
http proxy outgoing {connection-timeout microsecs host {hostname ipaddress} port [primary] monitor seconds origin-server preserve-407}		
http request-header host unmodified	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching	Configuring HTTP Cache Settings, page 8-6

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
http reval-each-request all	Devices > Device Groups > Applications > Web > HTTP > HTTP Cache Freshness	Configuring HTTP Cache Freshness Settings, page 8-10
http reval-each-request none		
http reval-each-request text		
http serve-ims text <i>percentage</i> binary <i>percentage</i>		
http smart-range enable	Devices > Device Groups > Applications > Web > HTTP > HTTP Caching	Configuring HTTP Cache Settings, page 8-6
http smart-range max-start <i>offset</i> max-interval <i>interval</i>		
http strict-request-content-length-checking enable		
http tcp-keepalive enable	Devices > Device Groups > Applications > Web > HTTP > Advanced HTTP Caching	Configuring Advanced HTTP Cache Settings, page 8-19
https proxy incoming <i>ports</i>	Devices > Device Groups > Applications > Web > HTTPS > HTTPS Proxy	Configuring HTTPS Proxy Settings, page 8-37
https proxy outgoing host {<i>ipaddress</i> <i>hostname</i>} <i>port</i>		
https destination-port {allow deny} {<i>range</i> all}		
https tcp-rw-timeout <i>seconds</i>		
https server <i>name</i>	Devices > Device Groups > Applications > Web > HTTPS > HTTPS Servers	Configuring HTTPS Servers, page 8-42
https server <i>name</i> {cert <i>cert_name</i> certgroup {chain <i>chainname</i> serverauth <i>chainname</i>} enable host {<i>hostname</i> <i>ipaddress</i>} key <i>keyname</i> password <i>password</i> protocol-version {ssl2-only ssl23-tls1 ssl3-only tls1-only} serverauth {enable ignore {cert-not-yet-valid domain-name expired-date invalid-ca}} session-cache {size <i>size</i> timeout <i>timeout</i>}}	Devices > Device Groups > Applications > Web > HTTPS > Certificates	Configuring HTTPS Certificates, page 8-27
	Devices > Device Groups > Applications > Web > HTTPS > Certificate Groups	Configuring HTTPS Certificate Groups, page 8-31
	Devices > Device Groups > Applications > Web > HTTPS > Keys	Configuring HTTPS Keys, page 8-34
icap append-x-headers {x-client-ip x-server-ip}	Devices > Device Groups > Request Processing > ICAP	Configuring ICAP Settings, page 16-2
icap apply {all rules-template}		
icap bypass streaming-media		
icap logging {format standard enable}		
icap rescan-cache IStag-change		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
icap service <i>service_id</i>	Devices > Device Groups > Request Processing > ICAP Services	Configuring ICAP Services, page 16-5
ICAP service configuration mode (config-icap-service)# icap service <i>service_id</i> [enable vector-point { reqmod-precache reqmod-postcache respmod-precache } error-handling { bypass return-error } load-balancing { round-robin client-ip-hash server-ip-hash weighted-load }]		
ICAP service configuration mode (config-icap-service)# icap service server <i>server server_url</i> { max-connections <i>num</i> weight <i>num</i> }	Devices > Device Groups > Request Processing > ICAP Services	Configuring an ICAP Server for ICAP Service, page 16-8
icp client add-remote-server { <i>hostname</i> <i>ipaddress</i> } { parent sibling } icp-port <i>icpport</i> http-port <i>httpport</i> [restrict <i>domainnames</i>]	Devices > Device Groups > Applications > Web > HTTP > ICP > Remote Servers	ICP Remote Server Settings, page 8-84
icp client enable	Devices > Device Groups > Applications > Web > HTTP > ICP > Client	ICP Client Settings, page 8-80
icp client exclude <i>domainnames</i>		
icp client max-fail <i>retries</i>		
icp client max-wait <i>timeout</i>		
icp client modify-remote-server { <i>hostname</i> <i>ipaddress</i> } { http-port <i>port</i> icp-port <i>port</i> parent restrict <i>domainnames</i> sibling }	Devices > Device Groups > Applications > Web > HTTP > ICP > ICP Remote Servers	ICP Remote Server Settings, page 8-84
icp server enable	Devices > Device Groups > Applications > Web > HTTP > ICP > Server	ICP Server Settings, page 8-82
icp server http-port <i>httpport</i>		
icp server port <i>icpport</i>		
icp server remote-client { <i>hostname</i> <i>ipaddress</i> } { fetch no-fetch }	Devices > Device Groups > Applications > Web > HTTP > ICP > Remote Clients	ICP Remote Client Settings, page 8-82
inetd enable ftp	Devices > Device Groups > Applications > Web > FTP > Inetd FTP	Enabling Inetd FTP Service, page 8-61
inetd enable tftp	Devices > Device Groups > Applications > Web > TFTP > TFTP General Settings	Configuring TFTP General Settings, page 8-65
inetd enable rcp	Devices > Device Groups > General Settings > Network > Inetd RCP	Enabling RCP Services on the Content Engine, page 20-8

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
interface { FastEthernet GigabitEthernet } <i>slot/port</i> cdp enable	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Modifying Fast Ethernet or Gigabit Ethernet Interface Settings, page 14-7
interface { FastEthernet GigabitEthernet } <i>slot/port</i> shutdown		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> autosense		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> bandwidth { 10 100 1000 }		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> [full-duplex half-duplex]		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> mtu size		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> ip address <i>ipaddress netmask</i> [secondary]		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> standby groupnum ip <i>ipaddress netmask</i>	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Configuring a Standby Interface Using the Content Distribution Manager GUI, page 14-3
interface { FastEthernet GigabitEthernet } <i>slot/port</i> standby groupnum errors num		
interface { FastEthernet GigabitEthernet } <i>slot/port</i> standby groupnum priority <i>priority</i>	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Configuring the Interface Priority Setting, page 14-4
interface { FastEthernet GigabitEthernet } <i>slot/port</i> ip address dhcp { client-id <i>id hostname name</i> hostname name client-id <i>id</i> }		Configuring Interfaces for DHCP, page 14-13
interface FibreChannel <i>slot/port</i> [mode { autosense direct-attached switched } speed { 1 2 autosense }]		Configuring the Fibre Channel Interface, page 14-9
interface PortChannel { 1 2 } [ip address <i>ipaddress netmask</i> shutdown]	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Configuring EtherChannel, page 14-11
interface { FastEthernet GigabitEthernet } <i>slot/port</i> ip access-group { <i>accesslistnumber</i> <i>accesslistname</i> } { in out }	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Applying an IP ACL to an Interface, page 17-13
ip access-list { standard extended } { <i>acl_name</i> <i>acl_num</i> } Includes other configuration commands for standard and extended IP ACLs.	Devices > Devices ¹ > General Settings > Network > IP ACL	Creating or Modifying an IP ACL, page 17-2

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
Extended ACL configuration mode (config-ext-nacl)# [insert line_num] {deny permit} {gre ip proto_num} {source_ip [wildcard] host source_ip any} {dest_ip [wildcard] host dest_ip any} [insert line_num] {deny permit} tcp {source_ip [wildcard] host source_ip any} [operator port [port]] {dest_ip [wildcard] host dest_ip any} [operator port [port]] [established] [insert line_num] {deny permit} udp {source_ip [wildcard] host source_ip any} [operator port [port]] {dest_ip [wildcard] host dest_ip any} [operator port [port]] [insert line_num] {deny permit} icmp {source_ip [wildcard] host source_ip any} {dest_ip [wildcard] host dest_ip any} [icmp_type [code] icmp_msg] delete line_num list [start_line_num [end_line_num]] move oldline_num newline_num exit	Devices > Devices ¹ > General Settings > Network > IP ACL	Adding Conditions to an IP ACL, page 17-3
Standard ACL configuration mode (config-std-nacl)# [insert line_num] {deny permit} {source_ip [wildcard] host source_ip any} delete line_num list [start_line_num [end_line_num]] move oldline_num newline_num exit	Devices > Devices ¹ > General Settings > Network > IP ACL	Adding Conditions to an IP ACL, page 17-3
ip default-gateway ipaddress	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Configuring a Standby Interface Using the Content Distribution Manager GUI, page 14-3 Modifying Fast Ethernet or Gigabit Ethernet Interface Settings, page 14-7
ip domain-name name1 name2 name3 ip name-server ipaddress	Devices > Device Groups > General Settings > Network > DNS	Configuring the DNS Server for HTTP Proxy Caching, page 8-78
ip dscp {client {cache-hit {match-server set-dscp dscp-packets set-tos tos-packets} cache-miss {match-server set-dscp dscp-packets set-tos tos-packets}} server {match-client set-dscp dscp-packets set-tos tos-packets}}	Devices > Device Groups > General Settings > Network > IP General Settings	Configuring IP Differentiated Services, page 10-9
ip path-mtu-discovery enable		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
ip route <i>dest_addrs netmask gateway_addrs</i>	Devices > Devices ¹ > General Settings > Network > IP Routes	Configuring Static IP Routes, page 14-15
kernel kdb	Devices > Device Groups > General Settings > Troubleshooting > Kernel Debugger	Enabling Kernel Debugger, page 21-23
ldap server administrative-dn <i>name</i>	Devices > Device Groups > General Settings > Authentication > LDAP Server	Configuring LDAP Server Settings, page 15-15
ldap server administrative-password <i>passwd</i>		
ldap server allow-mode		
ldap server base <i>baseword</i>		
ldap server enable	Devices > Device Groups > General Settings > Authentication > Authentication Scheme	Setting the Authentication Scheme for Request Authentication, page 15-34
ldap server filter <i>filterword</i>	Devices > Device Groups > General Settings > Authentication > LDAP Server	Configuring LDAP Server Settings, page 15-15
ldap server group active-directory enable		
ldap server group { organizationUnit enable custom <i>name enable</i> static { group-attribute <i>name</i> member-attribute { member uniquemember custom-member <i>name</i> } enable nested { enable level <i>number</i> }}}	Devices > Device Groups > General Settings > Authentication > LDAP Server	Configuring LDAP Server Settings, page 15-15
ldap server host { <i>hostipaddress</i> <i>hostname</i> } [primary secondary]		
ldap server password-expiry { enable redirect-url <i>url</i> }		
ldap server policy-redirect { enable redirect-url <i>url</i> attribute <i>name</i> version-number <i>number</i> }		
ldap server policy-redirect append-request-url		
ldap server port <i>port_num</i>		
ldap server retransmit <i>retries</i>		
ldap server timeout <i>seconds</i>		
ldap server userid-attribute <i>useridword</i>		
ldap server version <i>ver_num</i>		
line console carrier-detect	Devices > Device Groups > General Settings > Login Access Control > Console Carrier Detect	Configuring Line Console Carrier Detection, page 20-6

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
logging host { <i>ipaddress</i> <i>hostname</i> }	Devices > Device Groups > General Settings > Notification and Tracking > System Logs	Configuring System Event Logging Using the Content Distribution Manager GUI, page 21-5
logging host priority { alert critical debug emergency error information notice warning }		
logging disk enable		
logging disk filename <i>filename</i>		
logging disk recycle <i>size</i>		
logging disk priority { alert critical debug emergency error information notice warning }		
logging console enable		
logging console priority { alert critical debug emergency error information notice warning }		
logging facility { auth daemon kernel local0 local1 local2 local3 local4 local5 local6 local7 mail news syslog user uucp }		
multicast license-key <i>key</i>	Devices > Device Groups > Prepositioning > Multicast Distribution License	Enabling Content Engines for Multicasting, page 5-32
multicast accept-license-agreement multicast enable		
multicast evaluate		
network-filesystem server { samba cifs } { enable authentication-mode { public ce-user cifs-user password-server } max-connections <i>num</i> }	Devices > Device Groups > General Settings > File Sharing > CIFS Server	Configuring CIFS Server Settings, page 13-17
network-filesystem server { samba cifs } { share-web-site <i>site_name</i> [share-auth-content protect-auth-content]}	Devices > Device Groups > General Settings > File Sharing > CIFS Server Access Control	Configuring CIFS Server Website Access Control Settings, page 13-19
network-filesystem client { cifs { <i>hostname</i> <i>ipaddress</i> } directory { cdnfs mediafs } reserved-disk-space <i>space</i> username <i>name</i> password <i>password</i> [domain <i>domain</i>] nfs { <i>hostname</i> <i>ipaddress</i> } directory { cdnfs mediafs } reserved-disk-space <i>space</i> }	Devices > Devices ¹ > General Settings > Storage > NAS	See “Attaching and Detaching NAS Shares Using the Content Distribution Manager GUI” in the <i>Cisco ACNS Software Update and Maintenance Guide, Release 5.x</i> .
ntlm server ad-group-search { enable enum-user gc-server groupname-attribute ldap-referral ldap-search-port membership-attribute user-objectclass username-attribute }	Devices > Device Groups > General Settings > Authentication > NTLM Server	Configuring NTLM Server Settings, page 15-21

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
ntlm server ad-group-search mem-cache {enable size <i>kilobytes</i> max-ttl <i>minutes</i> }	Devices > Device Groups > General Settings > Authentication > NTLM Server	Configuring the NTLM Server LDAP Memory Cache Settings, page 15-26
ntlm allow-domain {enable domain <i>domainname</i> }	Devices > Device Groups > General Settings > Authentication > NTLM Allow Domain	Configuring NTLM Allowed Domains for HTTP Request Authentication, page 15-29
ntlm server enable	Devices > Device Groups > General Settings > Authentication > Authentication Scheme	Setting the Authentication Scheme for Request Authentication, page 15-34
ntlm server host { <i>hostname</i> <i>ipaddress</i> }	Devices > Device Groups > General Settings > Authentication > NTLM Server	Configuring NTLM Server Settings, page 15-21
ntlm server domain <i>name</i>		
ntp server { <i>hostname</i> <i>ipaddress</i> }	Devices > Device Groups > General Settings > Network > NTP	Configuring NTP Settings, page 20-11
offline-operation enable	Devices > Device Groups > Applications > Web > Offline Operations	Enabling Offline Operation of Network Devices, page 20-27
port-channel load-balance { <i>dst-ip</i> <i>dst-mac</i> <i>round-robin</i> }	Devices > Devices ¹ > General Settings > Network > Network Interfaces	Configuring EtherChannel, page 14-11
proxy-auto-config enable	Devices > Device Groups > Applications > Web > Client Proxy Autoconfiguration	Configuring Client Proxy Autoconfiguration Settings, page 4-38
proxy-protocols outgoing-proxy exclude {enable list <i>word</i> }	Devices > Device Groups > Applications > Web > Outgoing Proxy Exclusions	Configuring HTTP and HTTPS Outgoing Proxy Exclusion Settings, page 8-48
proxy-protocols transparent { <i>default-server</i> <i>original-proxy</i> <i>reset</i> }		
qos camiant-cdn-am-service config-file <i>filename</i> or <i>URL</i>	Devices > Device Groups > Request Processing > PCMM > QoS Policy Service	Setting QoS Policy Server Settings for Content Engines, page 16-58
qos camiant-cdn-am-service enable		
radius-server key <i>key</i>	Devices > Device Groups > General Settings > Authentication > RADIUS Server	Configuring RADIUS Server Settings, page 15-30
radius-server timeout <i>seconds</i>		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
radius-server enable	Devices > Device Groups > General Settings > Authentication > Authentication Scheme	Setting the Authentication Scheme for Request Authentication, page 15-34
radius-server host {hostname ipaddress} {auth-port port}	Devices > Device Groups > General Settings > Authentication > RADIUS Server	Configuring RADIUS Server Settings, page 15-30
radius-server retransmit retries		
radius-server redirect enable		
radius-server redirect message reply location url		
rtsp advanced max-initial-setup-delay seconds	Devices > Device Groups > Applications > Streaming > RTSP Gateway	Configuring the RTSP Gateway, page 9-3
rtsp advanced max-request-rate number		
rtsp proxy media-real enable	Devices > Device Groups > Applications > Streaming > Real Networks > Real Proxy License	Enabling RealProxy, page 9-5
rtsp proxy media-real evaluate		
rtsp proxy media-real license-key key		
rtsp proxy media-real accept-license-agreement		
rtsp server real-subscriber license-key key	Devices > Device Groups > Applications > Streaming > Real Networks > Real Subscriber License	Enabling RealSubscriber, page 9-7
rtsp server real-subscriber accept-license-agreement		
rtsp server real-subscriber evaluate		
rtsp server real-subscriber enable		
rtsp l4-switch enable	Devices > Device Groups > Applications > Streaming > RTSP Gateway	Configuring the RTSP Gateway, page 9-3
rtsp port incoming port_num		
rtsp ip-address ipaddress		
rtsp server cisco-streaming-engine enable	Devices > Device Groups > Applications > Streaming > Cisco Streaming Engine	Enabling the Cisco Streaming Engine, page 9-9
rtsp server cisco-streaming-engine broadcast port-list list_num port_num	Services > Video > Programs > Live Streaming (indirect support)	Configuring Live Stream Settings for a Cisco Streaming Engine Live Program, page 7-19
rtsp server cisco-streaming-engine broadcast id id source {source-rtsp rtsp_url source-udp url srce_ip_addr rcv_ip_addr rcv_port_list_num} {track-count 1-4} destination {destination-pull destination-udp ttl dest_ip_addr dest_list_num}		
rule enable	Devices > Device Groups > Request Processing > Enable Rules	Enabling Rule Settings, page 16-11

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
rule action rule action allow pattern-list <i>list_num</i> [protocol {all http https mms rtsp}] rule action append-username-header pattern-list <i>list_num</i> [protocol {all http https mms rtsp}] rule action block pattern-list <i>list_num</i> [protocol {all http https mms rtsp}] rule action cache-non-cacheable ttl {day <i>days</i> pattern-list <i>list_num</i> [protocol {all http https}] hours <i>hours</i> pattern-list <i>list_num</i> [protocol {all http https}] minutes <i>minutes</i> pattern-list <i>list_num</i> [protocol {all http https}] seconds <i>seconds</i> pattern-list <i>list_num</i> [protocol {all http https}]}	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11
rule action cache-only pattern-list <i>list_num</i> [protocol {all http https mms}] rule action dscp client cache-hit {match-server pattern-list <i>list_num</i> [protocol {all http https}] set-dscp <i>dscpvalue</i> set-tos <i>tosvalue</i> } rule action dscp client cache-miss {match-server pattern-list <i>list_num</i> [protocol {all http https}] set-dscp <i>dscpvalue</i> set-tos <i>tosvalue</i> } rule action dscp server {match-client pattern-list <i>list_num</i> [protocol {all http https}] set-dscp <i>dscpvalue</i> set-tos <i>tosvalue</i> }	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11
rule action freshness-factor <i>exp_time</i> pattern-list <i>list_num</i> [protocol {all http https}] rule action generate-url-signature [include-client-src-ip] key-id-owner <i>owner_num</i> key-id-number <i>id_num</i> pattern-list <i>list_num</i> [protocol {all http}] rule action insert-no-cache pattern-list <i>list_num</i> [protocol {all http https}] rule action no-auth pattern-list <i>list_num</i> [protocol {all http https mms rtsp}] rule action no-cache pattern-list <i>list_num</i> [protocol {all http https mms}] rule action no-persistent-connection {all client server} pattern-list <i>list_num</i> [protocol {all http https}]	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
rule action no-proxy pattern-list <i>list_num</i> [protocol {all http https}] rule action redirect url pattern-list <i>list_num</i> [protocol {all http https rtsp}] rule action redirect-url-for-cdn pattern-list <i>list_num</i> [protocol {all http https rtsp}] rule action refresh pattern-list <i>list_num</i> [protocol {all http https}] rule action reset pattern-list <i>list_num</i> [protocol {all http https mms rtsp}] rule action rewrite pattern-list <i>list_num</i> [protocol {all http https mms rtsp}]	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11
rule action use-dns-server { <i>hostname</i> <i>ipaddress</i> } pattern-list <i>list_num</i> [protocol {all http https}] rule action use-icap-service <i>service_name</i> pattern-list <i>list_num</i> [protocol {all http https mms}] rule action use-proxy { <i>hostname</i> <i>ipaddress</i> } <i>port</i> pattern-list <i>list_num</i> [protocol {all http https}] rule action use-proxy { <i>hostname</i> <i>ipaddress</i> } <i>port</i> [failover] pattern-list <i>list_num</i> [protocol {all http https}] rule action use-server { <i>hostname</i> <i>ipaddress</i> } <i>port</i> pattern-list <i>list_num</i> [protocol {all http https}] rule action use-xforward-clt-ip pattern-list <i>list_num</i> [protocol {all http https}] rule action validate-url-signature error-redirect-url <i>url</i> pattern-list <i>list_num</i> [protocol {all http rtsp}]	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
rule pattern-list <i>list_num</i> domain <i>dn_regex</i> rule pattern-list <i>list_num</i> dst-ip <i>d_ipaddress</i> <i>d_subnet</i> rule pattern-list <i>list_num</i> dst-port <i>port</i> rule pattern-list <i>list_num</i> groupname <i>name</i> rule pattern-list <i>list_num</i> groupname-regex <i>group_name_regex</i> rule pattern-list <i>list_num</i> group-type { and or } rule pattern-list <i>list_num</i> header-field { referer <i>ref_regex</i> request-line <i>req_regex</i> user-agent <i>ua_regex</i> } rule pattern-list <i>list_num</i> header-field-sub { referer <i>ref_regex</i> <i>ref_sub</i> request-line <i>req_regex</i> <i>req_sub</i> user-agent <i>ua_regex</i> <i>ua_sub</i> }	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11
rule pattern-list <i>list_num</i> icap-attribute <i>icap_attribute</i> <i>icap_value</i> rule pattern-list <i>list_num</i> mime-type <i>mt_regex</i> rule pattern-list <i>list_num</i> src-ip <i>s_ipaddress</i> <i>s_subnet</i> rule pattern-list <i>list_num</i> url-regex <i>url_regex</i> rule pattern-list <i>list_num</i> url-regexsub <i>url_regex</i> <i>url_sub</i> rule pattern-list <i>list_num</i> username <i>user_name</i>	Devices > Device Groups > Request Processing > Service Rules	Configuring Service Rules, page 16-11
snmp-server contact <i>line</i> snmp-server enable traps [config content-engine [disk-fail disk-read disk-write overload-bypass transaction-log] entity event snmp [authentication cold-start]]	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > General Settings	Configuring SNMP Traps, page 22-2
snmp-server host { <i>hostname</i> <i>ipaddress</i> } <i>communitystring</i> [v2c [retry <i>num</i>] [timeout <i>seconds</i>]] [v3 { auth [retry <i>num</i>] [timeout <i>seconds</i>] noauth [retry <i>num</i>] [timeout <i>seconds</i>] priv [retry <i>num</i>] [timeout <i>seconds</i>]}]	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Host	Configuring SNMP Host Settings, page 22-10
snmp-server location <i>line</i>	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > General Settings	Configuring SNMP Traps, page 22-2

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
snmp-server user <i>name group</i> [auth { md5 password [priv password] sha password [priv password]} remote octetstring [auth { md5 password [priv password] sha password [priv password]}]]	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > User	Configuring SNMP User Settings, page 22-8
snmp-server group <i>name</i> { v1 [notify name] [read name] [write name] v2c [notify name] [read name] [write name] v3 { auth [notify name] [read name] [write name] noauth [notify name] [read name] [write name] priv [notify name] [read name] [write name]}}	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Group	Configuring SNMP Group Settings, page 22-6
snmp-server community <i>string</i> [group groupname rw]	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > Community	Configuring SNMP Community Settings, page 22-5
snmp-server view <i>viewname MIBfamily</i> { excluded included }	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > View	Configuring SNMPv2 View Settings, page 22-9
snmp-server notify inform	Devices > Device Groups > General Settings > Notification and Tracking > SNMP > General Settings	Configuring SNMP Traps, page 22-2
snmp-server mib persist event		
snmp-server access-list { <i>std_acl_number</i> <i>acl_name</i> }	Devices > Devices ¹ > General Settings > Network > IP ACL Feature Usage	Associating an IP ACL with an Application, page 17-12
sshd enable	Devices > Device Groups > General Settings > Network > SSH	Configuring Secure Shell Settings, page 20-2
sshd timeout <i>seconds</i>		
sshd password-guesses <i>num</i>		
ssh-key-generate key-length <i>length</i>		
tacacs enable	Devices > Device Groups > General Settings > Authentication > TACACS+ Server	Configuring TACACS+ Server Settings, page 15-32
tacacs password ascii		
tacacs timeout		
tacacs retransmit		
tacacs key		
tacacs host { <i>ipaddress</i> <i>hostname</i> } [primary]		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
tcp ecn enable	Devices > Device Groups > General Settings > Network > TCP	Configuring TCP Settings for Increased Cache Performance, page 10-1
tcp type-of-service enable		
tcp cwnd-base <i>segments</i>		
tcp increase-xmit-timer-value <i>value</i>		
tcp init-ss-threshold <i>value</i>		
tcp keepalive-probe-cnt <i>count</i>		
tcp keepalive-probe-interval <i>seconds</i>		
tcp keepalive-timeout <i>seconds</i>		
tcp client-satellite		
tcp client-mss <i>max_seg_size</i>		
tcp client-receive-buffer <i>kbytes</i>		
tcp client-rw-timeout <i>seconds</i>		
tcp client-send-buffer <i>kbytes</i>		
tcp server-satellite		
tcp server-mss <i>max_seg_size</i>		
tcp server-receive-buffer <i>kbytes</i>		
tcp server-rw-timeout <i>seconds</i>		
tcp server-send-buffer <i>kbytes</i>		
telnet enable	Devices > Device Groups > General Settings > Network > Telnet	Enabling the Telnet Service on the Content Engine, page 20-1
tftp max-connections <i>number</i>	Devices > Device Groups > Applications > Web > TFTP > TFTP General Settings	Configuring TFTP General Settings, page 8-65
tftp-server dir <i>directory</i>	Devices > Device Groups > Applications > Web > TFTP > TFTP Directory	Configuring TFTP Directory Settings, page 8-69
tftp-server access-list { <i>std_acl_number</i> <i>acl_name</i> }	Devices > Devices ¹ > General Settings > Network > IP ACL Feature Usage	Associating an IP ACL with an Application, page 17-12
tftp-server gw proto ftp server { <i>hostname</i> <i>ipaddress</i> } pri <i>priority</i> [name <i>name</i> passwd <i>password</i>] [path <i>directory</i>]	Devices > Device Groups > Applications > Web > TFTP > TFTP Proxy	Configuring TFTP Proxy Server Settings, page 8-66
tftp-server gw proto http server { <i>hostname</i> <i>ipaddress</i> } [port <i>port_num</i>] pri <i>priority</i> [name <i>name</i> passwd <i>password</i>] [path <i>directory</i>]		

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference		
transaction-logs archive max-file-size <i>kbytes</i>	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs	Enabling Transaction Logging with the Content Distribution Manager GUI, page 19-10		
transaction-logs archive interval { <i>seconds</i> every-week [on <i>weekdays</i> at <i>hour:minute</i>] every-day {at <i>hour:minute</i> every hours } every-hour {at <i>minute</i> every minutes }}				
transaction-logs enable				
transaction-logs export enable				
transaction-logs export ftp-server { <i>hostname</i> <i>ipaddress</i> } <i>login password directory</i>				
transaction-logs export sftp-server { <i>hostname</i> <i>ipaddress</i> } <i>login password directory</i>				
transaction-logs export compress	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs	Enabling Transaction Logging with the Content Distribution Manager GUI, page 19-10		
transaction-logs export interval { <i>minutes</i> every-week [on <i>weekdays</i> at <i>hour:minute</i>] every-day {at <i>hour:minute</i> every hours } every-hour {at <i>minute</i> every minutes }}				
transaction-logs file-marker				
transaction-logs sanitize				
transaction-logs log-windows-domain				
transaction-logs format { <i>squid</i> <i>extended-squid</i> <i>apache</i> <i>custom string</i> }				
tvout signal { <i>ntsc</i> <i>pal</i> }			Devices > Device Groups > Applications > Set Top Box > TV-out	Enabling the TV-Out Feature, page 7-30
tvout enable				
url-filter http { <i>bad-sites-deny</i> <i>good-sites-allow</i> } { enable <i>file filename</i> }			Devices > Device Groups > Request Processing > URL Filter > HTTP > URL Filter Settings for HTTP Protocol	Configuring URL Filter Settings Using the Content Distribution Manager GUI, page 16-22
url-filter http websense allowmode enable				
url-filter http websense enable				
url-filter http websense server { <i>ipaddress</i> <i>hostname</i> } port <i>1-65535</i> timeout <i>seconds</i> connections <i>1-250</i>				
url-filter http N2H2 allowmode enable	Configuring URL Filtering with the N2H2 Server, page 16-29			
url-filter http N2H2 enable				
url-filter http N2H2 server { <i>ipaddress</i> <i>hostname</i> } port <i>1-65535</i> timeout				
url-filter http smartfilter enable	Configuring URL Filtering with SmartFilter Software, page 16-51			

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
<code>url-filter http custom-message dirname</code>	Devices > Device Groups > Request Processing > URL Filter	Configuring URL Filter Settings Using the Content Distribution Manager GUI, page 16-22 Configuring Custom Blocking Messages Using the CLI, page 16-27
<code>url-filter wmt { bad-sites-deny good-sites-allow } { enable file filename }</code>	Devices > Device Groups > Request Processing > URL Filter > WMT > URL Filter Settings for WMT Protocol	Configuring URL Filter Settings Using the Content Distribution Manager GUI, page 16-22
<code>url-filter rtsp { bad-sites-deny good-sites-allow } { enable file filename }</code>	Devices > Device Groups > Request Processing > URL Filter > RTSP > URL Filter Settings for RTSP Protocol	
<code>url-signature key-id-owner number key-id-number number key encryption_key</code>	Devices > Device Groups > Request Processing > PCMM > URL Signature Key	Creating New URL Signature Keys for Content Engines, page 16-59
<code>username name { cifs-password password privilege }</code>	Devices > Device Groups > General Settings > Login Access Control > Users > Usernames	Creating User Accounts for Centrally Managed Devices, page 12-14
<code>wccp access-list { std_acl_number ext_acl_number acl_name }</code>	Devices > Devices ¹ > General Settings > Network > IP ACL Feature Usage	Associating an IP ACL with an Application, page 17-12
<code>wccp custom-web-cache mask { [dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num] }</code>	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
<code>wccp custom-web-cache router-list-num num port port [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [password key] [weight percentage]</code>	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
<code>wccp dns mask { [dst-ip-mask hex_num] [dst-port-mask port_hex_num] [src-ip-mask hex_num] [src-port-mask port_hex_num] }</code>	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
<code>wccp dns router-list-num num [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [password key] [weight percentage]</code>	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
<code>wccp flow-redirect enable</code>	Devices > Device Groups > Request Routing > WCCP > General Settings	Configuring WCCP General Settings for the Content Engine, page 4-7

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
wccp ftp router-list-num <i>num</i> [assign-method-strict] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp ftp mask {[dst-ip-mask <i>hex_num</i>] [src-ip-mask <i>hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp home-router <i>ipaddress</i>	Devices > Device Groups > Request Routing > WCCP > General Settings	Configuring WCCP General Settings for the Content Engine, page 4-7
wccp https-cache accept-all	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp https-cache mask {[dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp https-cache router-list-num <i>num</i> port <i>port</i> [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Port Lists for the Content Engine, page 4-17
wccp port-list <i>list_num</i> <i>port_num</i>	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp rtsp mask {[dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp rtsp router-list-num <i>num</i> [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp reverse-proxy mask [dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp reverse-proxy router-list-num <i>num</i> [assign-method-strict] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Creating WCCP Router Lists, page 4-14
wccp router-list <i>list_num</i> <i>ipaddress</i>	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp service-number <i>service_num</i> router-list-num <i>num</i> port-list-num <i>port</i> application { <i>cache</i> <i>streaming</i> } [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [match-source-port] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
wccp service-number <i>service_num</i> mask {[dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp shutdown max-wait <i>seconds</i>	Devices > Device Groups > Request Routing > WCCP > General Settings	Configuring WCCP General Settings for the Content Engine, page 4-7
wccp slow-start enable		
wccp spoof-client-ip enable		
wccp version {1 2}		
wccp web-cache mask {[dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp web-cache router-list-num <i>num</i> [assign-method-strict] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp wmt mask {[dst-ip-mask <i>hex_num</i>] [dst-port-mask <i>port_hex_num</i>] [src-ip-mask <i>hex_num</i>] [src-port-mask <i>port_hex_num</i>]}	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Masks for the Content Engine, page 4-18
wccp wmt router-list-num <i>num</i> [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]	Devices > Device Groups > Request Routing > WCCP > Services	Configuring WCCP Service Settings for the Content Engine, page 4-10
wccp wmt-rtspu router-list-num <i>num</i> [assign-method-strict] [hash-destination-ip] [hash-destination-port] [hash-source-ip] [hash-source-port] [I2-redirect] [mask-assign] [password <i>key</i>] [weight <i>percentage</i>]		
websense-server enable	Devices > Device Groups > Request Processing > URL Filter > HTTP > URL Filter Settings for HTTP Protocol	Configuring URL Filter Settings Using the Content Distribution Manager GUI, page 16-22
websense-server service { edir-agent { activate edir-server administrative-passwd <i>password</i> } eim activate logon-agent activate network-agent activate policy { local activate remote host <i>hostname</i> or <i>IP address</i> port <i>portnum</i> } radius-agent activate user activate }	Devices > Device Groups > Request Processing > Websense Server	Installing Websense Server Components for the Content Engine, page 16-46
wmt accelerate live-split enable	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
wmt accelerate proxy-cache enable		
wmt accelerate vod enable		
wmt accept-license-agreement	Devices > Device Groups > Applications > Streaming > Windows Media > License	Enabling Windows Media Services, page 9-11

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
wmt advanced client idle-timeout <i>seconds</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
wmt advanced client max-packet-size <i>bytes</i>		
wmt advanced server log-forwarding enable		
wmt bandwidth incoming bypass-list { <i>ipaddress</i> <i>hostname</i> } [<i>ipaddress</i> <i>hostname</i>]	Devices > Devices ¹ > Applications > Streaming > Windows Media > Bypass List	Configuring the Windows Media Incoming Bandwidth Bypass List, page 9-44
wmt broadcast { <i>alias-name name source url</i> }	Devices > Device Groups > Applications > Streaming > Windows Media > Broadcast Alias	Configuring Multicast-In Unicast-Out, page 9-31 Configuring Unicast-In Unicast-Out, page 9-33
wmt cache enable	Devices > Device Groups > Applications > Streaming > Windows Media > License	Enabling Windows Media Services, page 9-11
wmt cache max-obj-size <i>mbytes</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
wmt cache unique-stream-key		
wmt disallowed-client-protocols {[<i>http</i> <i>mmst</i> <i>mmsu</i> <i>rtsp</i> <i>rtspu</i>]}		
wmt enable	Devices > Device Groups > Applications > Streaming > Windows Media > License	Enabling Windows Media Services, page 9-11
wmt evaluate		
wmt extended transaction-log enable	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs	Using WMT Transaction Logging, page 19-15
wmt fast-cache enable	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
wmt fast-cache max-delivery-rate <i>num</i>		
wmt fast-start enable		
wmt fast-start max-bandwidth <i>kbits</i>		
wmt http allow extension <i>file_extensions</i>		
wmt incoming <i>port_num</i>		
wmt l4-switch enable		
wmt license-key <i>key</i>	Devices > Device Groups > Applications > Streaming > Windows Media > License	Enabling Windows Media Services, page 9-11
wmt live-url-stripping enable	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13

Table D-1 ACNS Software CLI to Content Distribution Manager GUI Map (continued)

Command	GUI Navigation Path	Procedure Reference
wmt multicast { station-configuration <i>name</i> [<i>dest_addr dest_port media_source</i>] [log { local webserver <i>webserver_url</i> }] [play-forever] [unicast-url <i>url</i>] failover { alternate-source <i>alt_src_url</i> retry-count <i>number</i> retry-interval <i>number</i> } schedule-start { <i>minute hour day month</i> now }] time-to-live <i>ttl</i> }	Devices > Device Groups > Applications > Streaming > Windows Media > Multicast Stations	Configuring Unicast-In Multicast-Out, page 9-25 Configuring Multicast-In Multicast-Out, page 9-28
wmt max-concurrent-sessions <i>num</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
wmt multicast schedule-start <i>name minute hour day month</i>	Devices > Device Groups > Applications > Streaming > Windows Media > Multicast Station Schedules	Configuring Windows Media Multicast Station Schedules, page 9-35
wmt multicast time-to-live <i>ttl</i>	Devices > Device Groups > Applications > Streaming > Windows Media > General Settings	Configuring Windows Media Proxy Settings for the Content Engine, page 9-13
wmt proxy outgoing http host { <i>hostname</i> <i>ipaddress</i> } <i>port</i>		
wmt proxy outgoing mms host { <i>hostname</i> <i>ipaddress</i> } <i>port</i>		
wmt proxy outgoing rtsp host { <i>hostname</i> <i>ipaddress</i> } <i>port</i>		
wmt transaction-logs format { extended wms-41 wms-90 } wms-41 wms-90 }	Devices > Device Groups > General Settings > Notification and Tracking > Transaction Logs	Using WMT Transaction Logging, page 19-15

1. This command can only be configured on individual devices; the Content Distribution Manager GUI does not support this command for device group configuration.

CLI Commands Not Supported in the Content Distribution Manager GUI

The following CLI commands are not supported in the Content Distribution Manager GUI:

- **auto-register enable** {FastEthernet *number number* | GigabitEthernet *number number*}
- **bandwidth advanced config-file** *string*
- **cdm ip** *string*
- **cdm** {role {primary | standby} | ui port *number*}
- **cms enable**
- **cms rpc timeout** {connection *number transfer number* | incoming-wait *number*}
- **content-routing-api enable**
- **device mode**
- **exception** {debug | coredump}
- **multicast back-version-compatibility acns-5-0**
- **multicast sender-delay** *number*
- **multicast max-concurrent-jobs** *number minimal-target-rate number*
- **multicast priority-weight** *number*
- **multicast fixed-carousel enable**
- **pre-load**
- **rtsp server cisco-streaming-engine broadcast port-list** *number number*
- **rtsp server cisco-streaming-engine broadcast id** *string* source {source-rtsp *string* | source-udp *string ipaddress ipaddress number*} {track-count *number*} destination {destination-pull | destination-udp *number ipaddress number*}

