FortiGate CLI system global
Version 3.0 MR6

FORTINET

www.fortinet.com

FortiGate CLI Reference
Version 3.0 MR6
22 FEB 08
01-30006-0354-20080222

Trademarks

global

Use this command to configure global settings that affect various FortiGate systems and configurations.

Runtime-only config mode was introduced in FortiOS v3.0 MR2. This mode allows you to try out commands that may put your FortiGate unit into an unrecoverable state normally requiring a physical reboot. In runtime-only config mode you can set a timeout so after a period of no input activity the FortiGate unit will reboot with the last saved configuration. Another option in runtime-only configuration mode is to manually save your configuration periodically to preserve your changes. For more information see `set cfg-save {automatic | manual | revert}`, `set cfg-revert-timeout <seconds>`, and `execute cfg reload`.

Switch mode is available on FortiWiFi 60B, FortiGate 60B, 100A (Rev2.0 and higher), and 200A (Rev2.0 and higher) models where the internal interface is a four or six port switch. Normally the internal interface is configured as one interface shared by all four ports. Switch mode allows you to configure each interface on the switch separately with their own interfaces. Consult your release notes for the most current list of supported models for this feature. The keywords internal-switch-mode {interface | switch} and internal-switch-speed {100full | 100half | 10full | 10half | auto} apply only to switch mode enabled FortiGate models.

Syntax

```
config system global
  set access-banner {enable | disable}
  set admin-https-pki-required {enable | disable}
  set admin-maintainer {enable | disable}
  set admin-port <port_number>
  set admin-scp {enable | disable}
  set admin-server-cert { self-sign | <certificate>}
  set admin-sport <port_number>
  set admin-ssh-port <port_number>
  set admin-ssh-v1 {enable | disable}
  set admin-telnet-port <port_number>
  set admintimeout <admin_timeout_minutes>
  set allow-interface-subnet-overlap {enable | disable}
  set auth-cert <cert-name>
  set auth-http-port <http_port>
  set auth-https-port <https_port>
  set auth-keepalive {enable | disable}
  set av-failopen {idledrop | off | one-shot | pass}
  set av-failopen-session {enable | disable}
  set batch_cmdb {enable | disable}
  set CC-mode {enable | disable}
  set cfg-save {automatic | manual | revert}
  set cfg-revert-timeout <seconds>
  set check-reset-range {enable | disable}
  set clt-cert-req {enable | disable}
  set conn-tracking {enable | disable}
  set daily-restart {enable | disable}
  set detection-summary {enable | disable}
  set dst {enable | disable}
  set failtime <failures_count>
  set fds-statistics {enable | disable}
  set fds-statistics-period <minutes>
  set forticlient-portal-port <port>
  set fsae-burst-size <packets>
  set fsae-rate-limit (pkt_sec)
  set gui-lines-per-page <gui_lines>
  set hostname <unithostname>
  set http-obfuscate {header-only | modified | no-error | none}
  set ie6workaround {enable | disable}
  set internal-switch-mode {interface | switch}
  set internal-switch-speed {100full | 100half | 10full | 10half | auto}
  set interval <deadgw_detect_seconds>
  set ip-src-port-range <start_port>-<end_port>
  set language <language>
  set lcdpin <pin_number>
  set lcdprotection {enable | disable}
  set ldapconntimeout <ldaptimeout_msec>
  set loglocaldeny {enable | disable}
  set management-vdom <domain>
  set ntpserver <ntp_server_address>
  set ntpsync {enable | disable}
  set optimize {antivirus | throughput}
  set phase1-rekey {enable | disable}
  set radius-port <radius_port>
  set refresh <refresh_seconds>
  set remoteauthtimeout <remoteauth_timeout_mins>
  set reset-sessionless-tcp {enable | disable}
  set restart-time <hh:mm>
  set show-backplane-intf {enable | disable}
  set sslvpn-sport <port_number>
  set strong-crypto {enable | disable}
  set syncinterval <ntpsync_minutes>
  set tcp-halfclose-timer <seconds>
  set tcp-halfopen-timer <seconds>
  set tcp-option {enable | enable}
  set timezone <timezone_number>
  set tos-based-priority {low | medium | high}
  set tp-mc-skip-policy {enable | disable}
  set udp-idle-timer <seconds>
  set user-server-cert <cert_name>
  set vdom-admin {enable | disable}
  set vip-arp-range {unlimited | restricted}
end
```

Keywords and variables	Description	Default
`access-banner {enable | disable}`	Enable to display the admin access disclaimer message. For more information see “system replacemsg admin” command.	`disable`
`admin-https-pki-required {enable | disable}`	Enable to allow user to login by providing a valid certificate if PKI is enabled for HTTPS administrative access. Default setting `disable` allows admin users to log in by providing a valid certificate or password.	`disable`
`admin-maintainer {enable | disable}`	Enabled by default. Disable for CC.	`enable`
`admin-port <port_number>`	Enter the port to use for HTTP administrative access.	80

Keywords and variables	Description	Default
`admin-scp {enable | disable}`	Enable to allow system configuration download by the secure copy (SCP) protocol.	`disable`
`admin-server-cert { self-sign | <certificate>}`	Select the admin https server certificate to use. Choices include self-sign, and the filename of any installed certificates. Default setting is `Fortinet_Factory,` if available, otherwise `self-sign`.	See definition under Description.
`admin-sport <port_number>`	Enter the port to use for HTTPS administrative access.	443
`admin-ssh-port <port_number>`	Enter the port to use for SSH administrative access.	22
`admin-ssh-v1 {enable | disable}`	Enable compatibility with SSH v1.0.	`disable`
`admin-telnet-port <port_number>`	Enter the port to use for telnet administrative access.	21
`admintimeout <admin_timeout_minutes>`	Set the number of minutes before an idle administrator times out. This controls the amount of inactive time before the administrator must log in again. The maximum `admintimeout` interval is 480 minutes (8 hours). To improve security keep the idle timeout at the default value of 5 minutes.	5
`allow-interface-subnet-overlap {enable | disable}`	Enable or disable limited support for interface and VLAN subinterface IP address overlap. Use this command to enable limited support for overlapping IP addresses in an existing network configuration. Caution: for advanced users only. Use this only for existing network configurations that cannot be changed to eliminate IP address overlapping.	`disable`
`auth-cert <cert-name>`	Https server certificate for policy authentication. Self-sign is the built in certificate but others will be listed as you add them.	`self-sign`
`auth-http-port <http_port>`	Set the HTTP authentication port. `<http_port>` can be from 1 to 65535.	1000
`auth-https-port <https_port>`	Set the HTTPS authentication port. `<https_port>` can be from 1 to 65535.	1003
`auth-keepalive {enable | disable}`	Enable to extend the authentication time of the session through periodic traffic to prevent an idle timeout.	`disable`
`av-failopen {idledrop | off | one-shot | pass}`	Set the action to take if there is an overload of the antivirus system. Valid options are off, one-shot, and pass. • Enter `idledrop` to drop connections based on the clients that have the most connections open. This is most useful for Windows applications, and can prevent malicious bots from keeping a connection open to a remote server. • Enter `off` to continue to handle and deliver connections regardless of free memory. • Enter `one-shot` to bypass the antivirus system when memory is low. You must enter `off` or `pass` to restart antivirus scanning. • Enter `pass` to bypass the antivirus system when memory is low. Antivirus scanning resumes when the low memory condition is resolved. This applies to FortiGate models numbered 300A and higher.	`pass`
`av-failopen-session {enable | disable}`	When `enabled` and a proxy for a protocol runs out of room in its session table, that protocol goes into failopen mode and enacts the action specified by `av-failopen`. This applies to models numbered 300A and higher.	`disable`

Keywords and variables	Description	Default
`batch_cmdb {enable | disable}`	Enable/disable batch mode run in cmdbsvr.	`enable`
`CC-mode {enable | disable}`	Enable Federal Information Processing Standards/ Common Criteria (FIPS/CC) mode. This is an enhanced security mode that is valid only on FIPS/CC-certified versions of the FortiGate firmware.	`disable`
`cfg-save {automatic | manual | revert}`	Set the method for saving the FortiGate system configuration and enter into runtime-only configuration mode. Methods for saving the configuration are: • automatic - automatically save the configuration after every change • manually - manually save the configuration using the execute cfg save command • revert - manually save the current configuration and then revert to that saved configuration after `cfg-revert-timeout` expires Switching to automatic mode disconnects your session. This command is used as part of the runtime-only configuration mode. See ”execute cfg reload” command for more information.	`automatic`
`cfg-revert-timeout <seconds>`	Enter the timeout interval in seconds. If the administrator makes a change and there is no activity for the timeout period, the FortiGate unit will automatically revert to the last saved configuration. Default timeout is 600 seconds. This command is available only when `cfg-save` is set to `revert`. This command is part of the runtime-only configuration mode. See ”execute cfg reload” command for more information.	`600`
`check-reset-range {enable | disable}`	Set whether RST out-of-window checking is performed. If set to strict (enable), RST must fall between the last ACK and the next send. If set to disable, no check is performed.	`disable`
`clt-cert-req {enable | disable}`	Enable to require a client certificate before an administrator logs on to the web-based manager using HTTPS.	`disable`
`conn-tracking {enable | disable}`	Enable to have the firewall drop SYN packets after the connection has been established with the remote system. This will help prevent a SYN flood and free up system resources.	`enable`
`daily-restart {enable | disable}`	Enable to restart the FortiGate unit every day. The time of the restart is controlled by `restart-time`.	`disable`
`detection-summary {enable | disable}`	Disable to prohibit the collection of detection summary statistics for FortiGuard.	`enable`
`dst {enable | disable}`	Enable or disable daylight saving time. If you enable daylight saving time, the FortiGate unit adjusts the system time when the time zone changes to daylight saving time and back to standard time.	`disable`
`failtime <failures_count>`	Set the dead gateway detection failover interval. Enter the number of times that ping fails before the FortiGate unit assumes that the gateway is no longer functioning. 0 disables dead gateway detection.	5
`fds-statistics {enable | disable}`	Enable or disable AV/IPS signature reporting. If necessary, disable to avoid error messages on HA slave units during an AV/IPS update.	enable
`fds-statistics-period <minutes>`	Select the number of minutes in the FDS report period. Range is 1 to 1440 minutes.	60

Keywords and variables	Description	Default
`forticlient-portal-port <port>`	Enter the HTTP port used to download a copy of FortiClient. Valid numbers are from 0 to 65535. On the FortiGate models 1000A, 3600A, and 5005FA2, firewall policies can deny access for hosts that do not have FortiClient Host Security software installed and operating. For more information see the Firewall chapter and System Maintenance chapter of the *FortiGate Administration Guide*.	8009
`fsae-burst-size <packets>`	Set the FSAE burst size in packets.	`300`
`fsae-rate-limit (pkt_sec)`	Set the FSAE message rate limit in packets per second.	`100`
`gui-lines-per-page <gui_lines>`	Set the number of lines displayed on table lists. Range is from 20 - 1000 lines per page.	50
`hostname <unithostname>`	Enter a name for this FortiGate unit. A hostname can not include spaces or punctuation other than hyphens and underlines. By default the hostname of your FortiGate unit is its serial number which includes the model.	FortiGate serial number.
`http-obfuscate {header-only | modified | no-error | none}`	Set the level at which the identity of the FortiGate web server is hidden or obfuscated. • none does not hide the FortiGate web server identity • `header-only` hides the HTTP server banner • `modified` provides modified error responses • `no-error` suppresses error responses	`none`
`ie6workaround {enable | disable}`	Enable or disable the work around for a navigation bar freeze issue caused by using the FortiGate web-based manager with Internet Explorer 6.	`disable`
`internal-switch-mode {interface | switch}`	Set the mode for the internal switch to be one of interface, or switch. The internal interface refers to a switch that has 4 network connections. The switch option is regular operation with one internal interface that all 4 network connections access. The interface option splits the internal interface into 4 separate interfaces, one for each network connection. The default value is switch. This applies only to FortiWiFi 60B, FortiGate 60B, 100A (Rev2.0 and higher), and 200A (Rev2.0 and higher) models.	`switch`
`internal-switch-speed {100full | 100half | 10full | 10half | auto}`	Set the speed of the switch used for the internal interface. Choose one of: • 100full • 100half • 10full • 10half • auto 100 and 10 refer to 100M or 10M bandwidth. Full and half refer to full or half duplex. Default value is auto. This applies only to FortiWiFi 60B, FortiGate 60B, 100A (Rev2.0 and higher), and 200A (Rev2.0 and higher) models.	`auto`
`interval <deadgw_detect_seconds>`	Select the number of seconds between pings the FortiGate unit sends to the target for dead gateway detection. Selecting 0 disables dead gateway detection.	5

Keywords and variables	Description	Default
ip-src-port-range <start_port>-<end_port>	Specify the IP source port range used for traffic originating from the FortiGate unit. The valid range for <start_port> and <end_port> is from 1 to 65535 inclusive. You can use this setting to avoid problems with networks that block some ports, such as FDN ports.	1024-4999
language <language>	Set the web-based manager display language. You can set <language> to one of english, french, japanese, korean, simch (Simplified Chinese) or trach (Traditional Chinese).	english
lcdpin <pin_number>	Set the 6 digit PIN administrators must enter to use the LCD panel. This applies to FortiGate models numbered 300 to 3600.	123456
lcdprotection {enable | disable}	Enable or disable LCD panel PIN protection. This applies to FortiGate models numbered 300 to 3600.	disable
ldapconntimeout <ldaptimeout_msec>	LDAP connection timeout in msec	500
loglocaldeny {enable | disable}	Enable or disable logging of failed connection attempts to the FortiGate unit that use TCP/IP ports other than the TCP/IP ports configured for management access (443 for https, 22 for ssh, 23 for telnet, and 80 for HTTP by default).	disable
management-vdom <domain>	Enter the name of the management virtual domain. Management traffic such as FortiGuard traffic originates from the management VDOM.	root
ntpserver <ntp_server_address>	Enter the domain name or IP address of a Network Time Protocol (NTP) server.	132.246.168.148
ntpsync {enable | disable}	Enable or disable automatically updating the system date and time by connecting to a Network Time Protocol (NTP) server. For more information about NTP and to find the IP address of an NTP server that you can use, see http://www.ntp.org.	disable
optimize {antivirus | throughput}	Set firmware performance optimization to either antivirus or throughput. This is available on FortiGate models numbered 1000 and higher.	No default
phase1-rekey {enable | disable}	Enable or disable automatic rekeying between IKE peers before the phase 1 keylife expires.	enable
radius-port <radius_port>	Change the default RADIUS port. The default port for RADIUS traffic is 1812. If your RADIUS server is using port 1645 you can use the CLI to change the default RADIUS port on your FortiGate unit.	1812
refresh <refresh_seconds>	Set the Automatic Refresh Interval, in seconds, for the web-based manager System Status Monitor. Enter 0 for no automatic refresh.	0
remoteauthtimeout <remoteauth_timeout_mins>	Timeout for RADIUS/LDAP authentication in minutes. To improve security keep the remote authentication timeout at the default value of 5 minutes.	5

Keywords and variables	Description	Default
`reset-sessionless-tcp {enable | disable}`	Enabling this option may help resolve issues with a problematic server, but it can make the FortiGate unit more vulnerable to denial of service attacks. In most cases you should leave `reset-sessionless-tcp` disabled. The `reset-sessionless-tcp` command determines what action the FortiGate unit performs if it receives a TCP packet but cannot find a corresponding session in its session table. This happens most often because the session has timed out. If you disable `reset-sessionless-tcp`, the FortiGate unit silently drops the packet. The packet originator does not know that the session has expired and might re-transmit the packet several times before attempting to start a new session. This is normal network operation. If you enable `reset-sessionless-tcp`, the FortiGate unit sends a RESET packet to the packet originator. The packet originator ends the current session, but it can try to establish a new session. This is available in NAT/Route mode only.	disable
`restart-time <hh:mm>`	Enter daily restart time in hh:mm format (hours and minutes). This is available only when `daily-restart` is enabled.	No default.
`show-backplane-intf {enable | disable}`	Select enable to show FortiGate-5000 backplane interfaces as port9 and port10. Once these backplanes are visible they can be treated as regular physical interfaces. This is only available on FortiGate-5000 models.	`disable`
`sslvpn-sport <port_number>`	Enter the port to use for SSL-VPN access (HTTPS).	`443`
`strong-crypto {enable | disable}`	Enable to use strong encryption and only allow strong ciphers (AES, 3DES) and digest (SHA1) for HTTPS/SSH admin access. When strong encryption is enabled, HTTPS is supported by the following web browsers: Netscape 7.2, Netscape 8.0, Firefox, and Microsoft Internet Explorer 7.0 (beta). Note that Microsoft Internet Explorer 5.0 and 6.0 are not supported in strong encryption.	`disable`
`syncinterval <ntpsync_minutes>`	Enter how often, in minutes, the FortiGate unit should synchronize its time with the Network Time Protocol (NTP) server. The `syncinterval` number can be from 1 to 1440 minutes. Setting to 0 disables time synchronization.	`0`
`tcp-halfclose-timer <seconds>`	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent a FIN packet but the other has not responded. The valid range is from 1 to 86400 seconds.	`120`
`tcp-halfopen-timer <seconds>`	Enter how many seconds the FortiGate unit should wait to close a session after one peer has sent an open session packet but the other has not responded. The valid range is from 1 to 86400 seconds.	`60`
`tcp-option {enable | enable}`	Enable SACK, timestamp and MSS TCP options. For normal operation `tcp-option` should be enabled. Disable for performance testing or in rare cases where it impairs performance.	`enable`
`timezone <timezone_number>`	The number corresponding to your time zone from 00 to 72. Press ? to list time zones and their numbers. Choose the time zone for the FortiGate unit from the list and enter the correct number.	`00`

Keywords and variables	Description	Default
`tos-based-priority {low | medium | high}`	Select the default system-wide level of priority for Type of Service (TOS). TOS determines the priority of traffic for scheduling. Typically this is set on a per service type level. See the “config system tos-based priority” command for more information. The value of this keyword is the default setting for when TOS is not configured on a per service level.	`high`
`tp-mc-skip-policy {enable | disable}`	Enable to allow skipping of the policy check, and to enable multicast through.	`disable`
`udp-idle-timer <seconds>`	Enter the number of seconds before an idle udp connection times out. The valid range is from 1 to 86400 seconds.	`180`
`user-server-cert <cert_name>`	Select the certificate to use for https user authentication. Default setting is `Fortinet_Factory,` if available, otherwise `self-sign.`	See definition under Description.
`vdom-admin {enable | disable}`	Enable to configure multiple virtual domains.	`disable`
`vip-arp-range {unlimited | restricted}`	`vip-arp-range` controls the number of ARP packets the FortiGate unit sends for a VIP range. If `restricted`, the FortiGate unit sends ARP packets for only the first 8192 addresses in a VIP range. If `unlimited`, the FortiGate unit sends ARP packets for every address in the VIP range.	`restricted`

Related topics

- execute cfg reload
- execute cfg save

www.fortinet.com

FORTINET®

www.fortinet.com