Cheat Sheet - General

FortiGate
for FortiOS 7.6

The cheat sheet from BOLL. Here you can find all important FortiGate CLI commands for the operation and troubleshooting of FortiGates with FortiOS 7.6.

System

General Troubleshooting Commands	
get system status	General system information
get system performance status	General performance info
exec tac report	Generates report for support

Firmware Update	
https://docs.fortinet.com/upgrade-tool/fortigate	Online Firmware Upgrade Path Tool Table
diag debug config-error-log read	Show config errors after firmware upgrades
diag fdsm image-list diag fdsm image-update-matrix	Download firmware image list and update-matrix

Process Information	
diag sys top [sec] [number] [iterations]	Process list Sort with P (CPU) / M (Memory) Control + C to stop command
diag debug crashlog read	Crash log

General Debugging Commands	
diag debug [enable/disable]	Enables/disables output for “diag debug” commands
diag debug cli 7	Shows WebUI changes in CLI
diag debug appl [appl] [level]	Realtime debugger for specific applications
diag test appl [appl] [test_level]	Status information for specific applications
diag deb console timestamp ena	Enables timestamp in console
diag debug reset	Reset all debug levels

HQIP Hardware Check	
diag hardware test suite all	Onboard hardware test
https://support.fortinet.com → Support → Downloads → Firmware Downloads > HQIP Images	Download HQIP images to scan hardware for possible faults

Session Troubleshooting

Firewall Session Troubleshooting	
diag sys session filter [filter]	Filter for session list
diag sys session list (expect)	Lists all (or expected) sessions
diag sys session clear	Clear all / filtered sessions
diag sys session stat	Session and memory statistics, drops, clashes

Packet Sniffer	
diag sniffer packet any / [if] ‘[filter]’ [verbose][count] [timestamp]	Packet sniffer. Use filters! Verbose levels 1-6 for different output
GUI: Network > Diagnostics > Packet Capture	Packet capture in WebUI.

Flow Trace	
diag debug flow filter [filter]	Use filters to narrow down trace results
diag deb flow trace start [count]	Debug command for traffic flow
diag debug flow show iprop en diag debug flow show fun en	Advanced flow output
GUI: Network > Diangostics > Debug Flow	Flow trace is also available in WebUI.

Network

Interface Information	
diag ip address list	List of IPs on FGT interfaces
diag firewall iplist list	List of IPs on VIP
diag firewall ippool list	List of IPs on IP pools
diag netlink interface list	List IF with MTU & device ID

Network Troubleshooting	
get hardware nic [interface]	Interface information
diag ip arp list / get system arp	ARP table
exec clear system arp table	Clears ARP table
exec ping x.x.x.x exec ping-options [option]	Ping utility
exec traceroute x.x.x.x exec traceroute-options [option]	Traceroute utility
exec telnet x.x.x.x [port] exec telnet-options [option]	Telnet utility

General Routing Troubleshooting	
get router info routing-table all	Routing table
get router info routing-table database	Routing table with inactive routes
get router info routing-table details x.x.x.x	Shows routing decision for specified destination-IP
get router info kernel	Forwarding information base
diag firewall proute list	List of policy-based routes
get router info protocols	Overview of dynamic routing protocol configuration
exec router restart	Restart of routing process
diag sys link-monitor status/interface/launch	Shows link monitor status / per interface / for WAN LLB

High Availability

HA General	
exec ha manage [index] [admin]	Jump to cluster member
get sys ha status	Information about HA status
diag sys ha history read	Details about past HA events
diag sys ha dump-by vcluster	Show cluster member uptime
diag sys ha reset-uptime	Reset cluster member uptime
diag debug appl hatalk -1 diag debug appl hasync -1	Debugging of HA-Talk/-Sync protocol
exec ha ignore-hardware-revision status / enable / disable	Set ignore status for different HW revisions
exec ha failover status	View failover status
exec ha failover set [cluster_id]	Triggers a HA failover on master device.

Cluster Synchronisation	
diag sys ha checksum cluster	Show config checksums of all cluster member
diag sys ha checksum recalculate	Recalculation of config checksums

UTM Services

FortiGuard Distribution Network (FDN)

*update.fortinet.net *guardservice.fortinet.net *update.fortiguard.net *service.fortiguard.net *securewf.fortiguard.net	URLs to access the FortiGuard Distribution Network (FDN)

Signature Update

diag autoupdate status	Summary of Fortiguard settings
diag autoupdate versions	Detailed versions of packages
diag test update info	Update & license information
diag debug appl update -1 exec update-now	Debugging for updating process with manual update

Antivirus

diag antivirus database-info	Antivirus database information

IPS

diag ips anomaly list	Lists statistics of DoS policies
diag ips packet status	IPS packet statistics
diag test appl ipsmonitor 2	Enable / disable IPS engine
diag test appl ipsmonitor 5	Toggle bypass status
diag test appl ipsmonitor 99	Restart all IPS processes

Web- & Email-Filter

diag debug rating	Webfilter/AS server information
diag webfilter fortiguard statistics list	Statistics of FortiGuard requests
diag webfilter fortiguard cache dump	List content of webfilter cache
diag test appl urlfilter 1	Lists webfilter test commands
diag debug urlfilter src-addr x.x.x.x diag debug appl urlfiter -1	Filter and realtime debugging for Webfiltering
diag emailfilter fortishield servers	Displays FortiShield server list
diag emailfilter fortishield stat list	Statistics of FortiShield requests

DNS-Filter

diag test appl dnsproxy 3	Shows server used for DNS-filter

Firewall Policy

Device Detection

exec update-src-vis	Update device detection DB
diag user device list / clear	Show / clear detected devices

Internet Service Database (ISDB)

diag internet-service-name list [internet-service-id]	Lists summary/details for specific Internet Service
diag internet-service info [vdom] / [proto] / [port]	Reverse ISDB lookup for specific IP, protocol or port
diag internet-service match [vdom] [ip] [netmask]	Reverse ISDB lookup for specific IP

FQDN

diag test application dnsproxy 6	Dump FQDN cache
diagnose firewall fqdn list-all	List all FQDN

Logging

diag log test	Generates dummy log messages
diag test app miglogd 6	Show log queue and fails

Traffic Shaper

diag firewall shaper traffic-shaper list / stats	Traffic shaper list / statistics
diag firewall shaper per-ip-shaper list / stats	Per IP traffic shaper list / statistics

SIP

diag sys sip status	SIP session helper status
diag sys sip-proxy stats list	SIP ALG status
diag sys sip-proxy calls list / clear	List/clear active SIP calls
diag debug appl sip -1	Realtime debugger for SIP

Authentication

Authentication

diag firewall auth filter …	Filter for authentication list
diag firewall auth list	List of authenticated user
diag test authserver [auth-protocol] [server] [user] [password]	Authentication test
diag debug appl authd -1	Debugging of local auth protocol
diag debug appl fnbamd -1	Debugging of remote auth prot.
diag debug appl saml -1	Debugging of SAML protocol
diag sys saml metadata	SAML metadata for admin-access

FortiToken

diag fortitoken info	Current FortiToken status
exec fortitoken activate [Forti-TokenSN]	Manual FortiToken activation
diag deb appl forticldd 255	FortiToken activation debugging
diag fortitoken debug enable	FortiToken debugging
exec fortitoken-mobile import 0000-0000-0000-0000-0000	Recover trial FortiToken (delete existing trial token before)

FSSO

diag debug authd fsso filter [filter]	Filter for FSSO user list
diag debug authd fsso list	List of FSSO authenticated user
diag debug authd fsso server-status	List of FSSO collector agents
get user adgrp	List of monitored groups
diag debug authd fsso refresh-logon / refresh-groups	Collector agents resend active user / group list to FGT
diag deb appl authd 8256	Debugging of authentication deamon
diag debug fsso-polling [option]	Info for clientless polling FSSO
diag debug appl fssod -1	Debugging of clientless polling FSSO

Explicit Proxy

diag wad user list / clear	List / clear of explicit proxy user
diag wad filter [filter] diag wad session list	Filtering / listing of web proxy sessions
diag test appl wad 0	List all different test level for “wad” (needs “diag deb ena”)

VPN

IPsec VPN (IKEv1 and IKEv2)	
diag debug appl ike 63	Debugging of IKE negotiation
diag vpn ike log filter [filter]	Filter for IKE negotiation output
diag vpn ike gateway list get vpn ike gateway	Detailed gateway/phase 1 information and state
diag vpn ike gateway flush name [name]	Delete phase 1
diag vpn tunnel list get vpn ipsec tunnel details	Detailed tunnel/phase 2 information and state
diag vpn tunnel flush [name]	Delete phase 2

Dynamic Routing

BGP	
get router info bgp summary	Summary of BGP status
get router info bgp neighbors	Information on BGP neighbors
get router info bgp neighbors x.x.x.x advertised-routes	Routes that the local FGT advertises to the neighbor
get router info bgp neighbors x.x.x.x route	Routes that a neighbor advertises to the local FGT
diag ip router bgp all enable diag ip router bgp level info	Real-time debugging of BGP protocol
exec router clear bgp [filter]	Restart of BGP session

OSPF	
get router info ospf status	OSPF status
get router info ospf interface	Information on OSPF interfaces
get router info ospf neighbor	Information on OSPF neighbors
get router info ospf database [filter]	Summary / details of LSDB entries
get router info ospf database self-originate	Information on LSAs originating from FGT
diag ip router ospf all enable diag ip router ospf level info	Real-time debugging of OSPF protocol
exec router clear ospf process	Restart of OSPF session

SD-WAN

SD-WAN	
diag sys sdwan member	Provide interface details
diag sys sdwan health-check status | filter [name/member]	State of SLAs
diag sys sdwan service [rule-id]	SD-WAN rule state
diag sys sdwan intf-sla-log [intf-name]	Link traffic history
diag sys sdwan sla-log [sla] [link_id]	SLA-Log on specific interface
diag test appl lnkmtd 0/1/2	Statistics of link-monitor
diag debug appl link-mon -1	Debugger of link-monitor

Security Fabric

Security Fabric, Automation Stitches, Security Rating	
diag sys csf upstream / downstream	List of up/downstream devices
diag sys csf neighbor list	MAC/IPs of connected FGTs
diag test appl csfd 1	Display security fabric statistics
diag debug appl csfd -1	Debugger for Security Fabric

Security Fabric, Automation Stitches, Security Rating (cont.)	
diag automation test [stitch_name]	Test stitches in the CLI
diag deb appl autod -1	Debugging automation stitches
diag report-runner trigger security-rating-reports	Manually run security rating reports

Wireless, Switch, FortiExtender

Access Point (CLI commands on Access Point)	
cfg –a ADDR_MODE	Set DHCP or static IP address mode on FortiAP
cfg –a AP_IPADDR	Set static IP on FortiAP
cfg –a AP_NETMASK	Set subnet mask on FortiAP
cfg –a IPGW	Set gateway on FortiAP
cfg –a AC_IPADDR_1	Specify IP of Wireless Controller on FortiAP
cfg –s / -c	List / Save config on FortiAP
cfg -x	Reset to factory default

Wireless Controller	
exec wireless-controller restart-acd	Restart wireless controller daemon
exec wireless-controller reset-wtp	Restart FortiAPs
diag wireless-controller wlac -c ap-rogue	List rogue APs
exec wireless-controller spectral-scan [wtp-id] [radio-id] [on | off] [duration] [channel] [report-interval]	Start or stop spectrum analysis
diag wireless-controller wlac -c rf-sa [wtp-id] [radio-id] [channel] get wireless-controller spectral-info [wtp-id] [radio-id]	Show spectrum analysis results

Switch Controller	
diag switch-controller switch-info mac-table	Managed FortiSwitch MAC address list
diag switch-controller switch-info port-stats	Managed FortiSwitch port statistics
diag switch-controller switch-info trunk	Trunk information
diag switch-controller switch-info mclag	Dumps MCLAG related information from FortiSwitch
exec switch-controller get-conn-status	Get FortiSwitch connection status
exec switch-controller diagnose-connection [switch]	Get FortiSwitch connection diagnostics

FortiExtender	
get extender sys-info [ext-sn]	Check the FortiExtender status
get extender modem-status [ext-sn] [modem-id]	Get the detailed modem status of the FortiExtender
diag debug appl extenderd -1	FortiExtender debugging
exec extender reset-fortiextender	Restart managed FortiExtender
exec extender restart-fortiextender-daemon	Restart FortiExtender daemon

Modem	
diag sys modem detect	Detect attached modem
diag debug appl modemd 3	Debugger for modem commands

Cheat Sheet – Other

System

Default Device Information	
admin / no password	Default login
192.168.1.99	Default IP (port1/internal/mgmt)
9600/8-N-1 / flow control disabled	Default serial console settings

General Config Commands	
config, get, show, set, unset, append, unselect	Configuration commands
tree	Lists all possible commands
[command] ? or tab	Use ? or tab in CLI for help
[command] | grep [pattern]	Grep command to filter outputs
show [full] | grep -f [pattern]	Grep command to filter config
print tablesize	Used and max values on FGT

Factory Reset	
exec factoryreset	Reset whole configuration
exec factoryreset-shutdown	Reset config and shutdown
exec factoryreset2	Reset but retaining admin, interfaces and static routing
exec factoryreset keepvmlicense	Reset but retaining VM license

VDOMs	
sudo diag / exec / show / get	Sudo-command to access global / VDOM settings directly

Transparent Mode	
diag netlink brctl name list diag netlink brctl name host	Bridge MAC table

Certificates	
exe vpn certificate local generate [certificate-use]	Regenerate default certificates Chose correct certificate usage

Console Logging (>300E/400F/900G)	
diag deb comlog enable/disable	Enable/disable console logging
diag deb comlog read/clear	Read/clear console logging
diag deb comlog info	Display console logging settings

Integrated Iperf Utility	
diag traffictest server-intf diag traffictest client-intf diag traffictest port [port] diag traffictest run -c [public_iperf_server_ip]	Iperf test run directly from FGT

Hardware

Hardware Information	
get hardware status	General HW status
diag hardware sysinfo cpu	CPU information
diag hardware sysinfo memory	Memory size, utilization
diag hardware sysinfo shm	Shared Memory size, utilization
diag hardware sysinfo conserve	Conserve Mode details
get hardware nic [interface]	Physical interface information
get system interface physical / transceiver	Signal information for copper or SFP/SFP+ interfaces

Disk Operation	
diag sys logdisk usage	Logdisk usage information
diag hardware deviceinfo disk	List disks with partitions
exec disk scan [ref_int]	Run disk check and fix

Disk Operation (cont.)	
exec disk format [ref_int]	Format the specified partitions or disks and reboots the system
exec formatlogdisk	Formatting the log disk, reboot included

Hardware Acceleration	
config firewall policy > edit [id[set auto-asic-offload disable	Disable session offloading per firewall policy
config vpn ipsec phase1-int > set npu-offload disable	Disable VPN offloading per phase 1

General Information

Fortinet Links	
docs.fortinet.com	Documentation, Release Notes
community.fortinet.com	Knowledge Base, User Forum
www.fortiguard.com	FortiGuard Website
support.fortinet.com	Support Site (Login required)
fndn.fortinet.net	Fortinet Developer Network
blog.boll.ch	Boll Blog

FortiGate most used ports	
TCP/443, TCP/UDP/53/8888	FortiGuard Queries
TCP/443	Contract Validation, FortiToken, Firmware Updates
TCP/443, TCP/8890	AV and IPS Update
UDP/500, ESP (IP#50) UDP/500, UDP/4500	IPSEC VPN (default) IPSEC VPN with NAT-Traversal
TCP/514	FortiManager, FortiAnalyzer
TCP/1812 TCP/1813	RADIUS Authentication RADIUS Accounting
TCP/389, UDP/389 TCP/636, UDP/636	LDAP, PKI Authentication LDAPS
UDP/5246, UDP/5247	CAPWAP
TCP/8000, TCP/8001	FSSO
TCP/8013, UDP/8014	FortiTelemetry
TCP/703, UDP/703	HA synchronisation
ETH 0x8890, 0x8891, 0x8893	HA heartbeat / sync

FortiClient EMS

ZTNA Troubleshooting and Debugging (on FortiGate)	
diag endpoint fctems test connectivity [EMS name]	Verify FortiGate to FortiClient EMS connectivity
diag test app fcnacd 2	EMS connectivity information
diag debug app fcnacd -1	Debugger for FortiClient NAC
diag endpoint ec-shm list	Show endpoint record list, filter by the endpoint IP address.
diag wad dev query-by ipv4 [ip]	Query from WAD diagnose command IP address
diag firewall dynamic list	List EMS ZTNA tags and all dynamic IP and MAC addresses
execute fctems verify [EMS name]	Verify FortiClient EMS certificate

Something missing?

Please contact us for comments, corrections or ideas
regarding our cheat sheet at support@boll.ch