

# Useful CLI commands FortiOS

## Cheatsheets

- FortiOS 6.2 CheatSheet (<https://blog.boll.ch/cheatsheet-fortios-version-6-2/>)
- FortiOS 7.0 CheatSheet (<https://blog.boll.ch/cheatsheet-fortios-7-0/>)
- FortiOS 7.2 CheatSheet (<https://blog.boll.ch/cheatsheet-fortios-v7-2/>)

## CLI Commands

To start a transaction in CLI use ***execute config-transaction start.***

A workspace mode transaction times out in five minutes if there is no activity. When a transaction times out, all changes are discarded

Commit config changes with ***execute config-transaction commit.***  
Abort with ***execute config-transaction abort.***

## Generic Commands

### Default Device Information

<b>admin / no password</b>	Default login
<b>192.168.1.99</b>	Default IP on port1, internal or management port
<b>9600/8-N-1, hw flow control disabled</b>	Default serial console settings

### General system commands

<b>get system status</b>	General system information
<b>exec tac support</b>	Generates report for support
<b>tree</b>	List all commands
<b>&lt;command&gt; ? / tab</b>	Use ? or tab in CLI for help
<b>&lt;command&gt;   grep [filter]</b>	Grep commands to filter output

## Fortigate most used ports

<b>UDP/53, UDP/8888</b>	Fortiguard Queries
<b>TCP/389, UDP/389</b>	LDAP, PKI Authentication
<b>TCP/443</b>	Contract Validation, FortiToken, Firmware Updates
<b>TCP/443, TCP/8890</b>	AV and IPS Update
<b>UDP/500, ESP</b>	IPSEC VPN
<b>UDP/500, UDP/4500</b>	IPSEC VPN with NAT-Traversal
<b>TCP/514</b>	FortiManager, FortiAnalyzer
<b>TCP/1812, TCP/1813</b>	RADIUS Auth & Accounting
<b>UDP/5246, UDP/5247</b>	CAPWAP
<b>TCP/8001</b>	FSSO
<b>TCP/8013</b>	Compliance and Security Fabric
<b>ETH Layer 0x8890, 0x8891 and 0x8893</b>	HA Heartbeat For HA The virtual MAC address is determined based on following formula: 00-09-0f-09-<group-id_hex>-(<vcluster_integer> + <idx>)

## Network commands

### Interface information

<b>diag ip address list</b>	List of IP addresses on FortiGate interfaces
<b>diag firewall iplist list</b>	List of IP addresses on VIP and IP-Pools

## Security Fabric

<b>diag sys csf upstream / downstream</b>	List of up/downstream devices
<b>diag sys csf neighbor list</b>	MAC/IP list of connected FG devices
<b>diag automation test &lt;stich_name&gt;</b>	Test stitches in the CLI
<b>diag test appl csfd 1 ...</b>	Display security fabric statistics
<b>diag debug appl csfd -1</b>	Real-time debugger

## Switch Controller

<b>diag switch-controller switch-info mac-table</b>	Managed FortiSwitch MAC address list
<b>diag switch-controller switch-info port-stats</b>	Managed FortiSwitch port statistics
<b>diag switch-controller switch-info trunk</b>	Trunk information

<b>diag switch-controller switch-info mclag</b>	Dumps MCLAG releated information from FortiSwitch
<b>execute switch-controller get-conn-status</b>	Get FortiSwitch connection status
<b>execute switch-controller diagnose-connection</b>	Get FortiSwitch connection diagnostics

## SD-WAN

<b>diag sys virtual-wan-link member</b>	Provide interface details
<b>diag sys virtual-wan-link health-check &lt;name&gt;</b>	State of SLAs
<b>diag sys virtual-wan-link service &lt;rule-id&gt;</b>	SD-WAN rule state
<b>diag sys virtual-wan-link intf-sla-log &lt;intf-name&gt;</b>	Link Traffic History
<b>diag sys virtual-wan-link sla-log &lt;sla&gt; &lt;link_id&gt;</b>	SLA-Log on specific interface
<b>diag test application lnkmttd 1/2/3</b>	Statistics of link-monitor
<b>diag debug application link- monitor -1</b>	Real-time debugger of link-monitor

## Network Troubleshooting

<b>get hardware nic [port]</b>	Interface information
<b>get system arp</b> <b>get system arp   grep x.x.x.x</b> <b>diag ip arp list</b>	ARP table
<b>exec clear system arp table</b>	Clears ARP table
<b>exec ping x.x.x.x</b> <b>exec ping-options [option]</b>	Ping utility
<b>exec traceroute x.x.x.x</b> <b>exec traceroute-options [option]</b>	Traceroute utility
<b>exec telnet x.x.x.x [port]</b>	Telnet utility
<b>exec dhcp lease-list</b>	Show DHCP Leases
<b>diag traffictest server-intf</b> <b>diag traffictest client-intf</b> <b>diag traffictest port [port]</b> <b>diag traffictest run -c [public_iperf_server_ip]</b>	Iperf test directly run from FortiGate

## Transparent Mode

<b>diag netlink brctl</b>	Bridge MAC table
---------------------------	------------------

## Routing

### Routing troubleshooting

<b>get router info routing-table all</b>	Show routing table
--	--------------------

<b>get router info routing-table details x.x.x.x</b>	Show routing decision for specified destination-IP
<b>get router info routing-table database</b>	Routing table with inactive routes
<b>get router info kernel</b>	Forwarding information base
<b>diag firewall proute list</b>	List of policy-based routes
<b>diag ip rtcache list</b>	List of route cache
<b>exec router restart</b>	Restart of routing process
<b>diag sys link-monitor status/interface/launch</b>	Show link monitor status / per interface / for WAN LB

## BGP

<b>get router info bgp summary</b>	BGP summary of BGP status
<b>get router info bgp neighbors</b>	Information of BGP neighbors
<b>diag ip router bgp all enable</b> <b>diag ip router bgp level info</b>	Real-time debugging for BGP protocol
<b>exec router clear bgp all</b>	Restart of BGP session

## OSPF

<b>get router info ospf status</b>	OSPF status
<b>get router info ospf interface</b>	Information on OSPF interfaces
<b>get router info ospf neighbor</b>	Information on OSPF neighbors
<b>get router info ospf database brief / router lsa</b>	Summary / Details of all LSDB entries
<b>get router info ospf database self-originate</b>	Information on LSAs originating from FortiGate
<b>diag ip router ospf all enable</b> <b>diag ip router ospf level info</b>	Real-time debugging of OSPF protocol
<b>exec router clear ospf process</b>	Restart of OSPF session

## VPN

<b>diag debug appl ike 63</b>	Debugging of IKE negotiation
<b>diag vpn ike log filter</b>	Filter for IKE negotiation output
<b>diag vpn ike gateway list</b>	Phase 1 state
<b>diag vpn ike gateway flush</b>	Delete Phase 1
<b>diag vpn tunnel list</b>	Phase 2 state
<b>diag vpn tunnel flush</b>	Delete Phase 2

<b>get vpn ike gateway</b>	Detailed gateway information
<b>get vpn ipsec tunnel details</b>	Detailed tunnel statistics
<b>get vpn ipsec tunnel summary</b>	Detailed tunnel information
<b>diag vpn ipsec status</b>	Shows IPSEC crypto status
<b>show full vpn certificate local</b>	Export all keys and certs

Revision #18  
Created 20 May 2021 12:43:17  
Updated 13 March 2024 09:19:30 by Peter Baumann