CLI troubleshooting cheat sheet

This reference lists some important command line interface (CLI) commands that can be used for log gathering, analysis, and troubleshooting.

It provides a basic understanding of CLI usage for users with different skill levels. Exploring additional commands beyond the ones listed here to gain a comprehensive understanding of the CLI is recommended.

Enable/Disable debugging

Command	Description
`diagnose debug reset`	Stop all the prior debugs that were enabled and running in the foreground or background.
`diagnose debug enable`	Start printing debugs in the console.
`diagnose debug disable`	Stop printing debugs in the console. The debugs are still running in the background; use `diagnose debug reset` to completely stop them.
`diagnose debug duration 0`	Start debugging for infinite duration. By default, debug is set for 30 minutes.

System

Command	Description
`get system status`	Show system information.
`execute time`	Show current system time.
`get system performance status`	Show CPU and memory utilization.
`execute tac report`	Execute TAC report used to open a support ticket with Fortinet Support.
`diagnose sys top {s} {n} {i}`	Show a list of the first *n* processes every *s* seconds for *i* iterations. • *Shift +C*: Sort by highest CPU • *Shift + M*: Sort by highest memory
`diagnose debug crashlog read`	Show system and application crashes.
`diagnose sys process pidof <daemon>`	Show PID of the daemon that is running. The names of currently running daemons can be found using `diagnose sys top`. For example: `diagnose sys process pidof httpsd`
`diagnose sys kill 11 <pid>`	Kill the PID with signal 11.
`diagnose sys session stat`	Show session statistics.
`diagnose sys session exp-stat`	Show expectation session statistics.
`diagnose sys vd list`	Show virtual domain information and system statistics.
`diagnose sys cmdb info`	Show information about the latest configuration change performed by the daemon.
`execute factoryreset [keepvmlicense]`	Immediately reset to factory defaults and reboot. If keepvmlicense is specified (VM models only), the VM license is retained after reset.
`execute factoryreset-shutdown [keepvmlicense]`	Immediately reset to factory defaults and shutdown. If keepvmlicense is specified (VM models only), the VM license is retained after reset.
`execute factoryreset2 [keepvmlicense]`	Reset to factory default, except system settings, system interfaces, VDOMs, static routes, and virtual switches. If keepvmlicense is specified (VM models only), the VM license is retained after reset.
`diagnose debug config-error-log read`	Show errors in the configuration file.
`diagnose snmp ip frags`	Show fragmentation and reassembly information.

`diagnose sys process dump <PID>`
`diagnose sys process pstack <PID>`
`diagnose sys process trace <PID>`
	Show essential process related information for a particular process PID.

`diagnose sys mpstat {n}`	Show CPU usage every n seconds.
`diagnose hardware sysinfo memory`	Show system memory information.
`diagnose firewall packet distribution`	Show packet distribution statistics.
`execute reboot`	Reboot the device.

Hardware

Command	Description
`diagnose hardware sysinfo interrupts`	Show hardware interrupts statistics.
`diagnose hardware test suite all`	Execute a hardware diagnostic test, also known as an HQIP test.
`diagnose hardware deviceinfo disk`	Show disk information.
`diagnose sys flash list`	Show flash partitions.
`execute disk list`	Show available mounted disks.
`execute disk format <partition ref>`	Format the referenced partition.

`diagnose disktest device <device>`
`diagnose disktest block <block>`
`diagnose disktest size <mb>`
`diagnose disk test run`
	Execute a disk check to check if disk is faulty.
	• `<device>`: Device to test
	• `<block>`: Block size of each read/write operation.
	• `<mb>`: Test size limit for each cycle

`execute formatlogdisk`	Format the log disk.
`diagnose hardware sysinfo cpu`	Show CPU information.

`diagnose sys modem detect`
`diagnose debug application modemd -1`
`diagnose debug enable`
	Detect the modem and start real-time debugging of the modem daemon.

FortiGuard

Command	Description
`diagnose webfilter fortiguard statistics`	Show rating cache and daemon statistics.
`diagnose debug rating`	Show web filter rating server information.
`diagnose debug application update -1` `diagnose debug enable`	Start debugging for updated daemon to troubleshoot FortiGuard update issues.
`execute update-now`	Execute the FortiGuard update manually.
`diagnose autoupdate status` `diagnose autoupdate versions`	Show license information.

Session table

Command	Description
`diagnose sys session filter <filter>`	Set session table filters.
`diagnose sys session filter`	Show session filters, if set.

Command	Description
`diagnose sys session list`	Show session table after filtering.
`diagnose sys session clear`	Clear the session table for the specified filter.
`diagnose firewall iprope list`	Show FortiGate's internal firewall table.

Network diagnostics

Command	Description
`execute ping-options {options}` `execute ping <x.x.x.x>`	Ping IP address <x.x.x.x> using the specified options.
`execute ssh-options {options}` `execute ssh <x.x.x.x>`	SSH to IP address <x.x.x.x> using the specified options.
`execute traceroute-options {options}` `execute traceroute <x.x.x.x>`	Traceroute IP address <x.x.x.x> using the specified options.
`get system arp` `diagnose ip arp list`	Show ARP entries.
`diagnose netlink brctl list`	Show the names of all of the switches on the FortiGate.
`diagnose netlink brctl name host <switch-name>`	Show the switching table of the specified switch.
`get system interface` `get sys interface physical`	Show a summary of interface details, including IP address information.
`diagnose ip address list`	Show IP address information.
`diagnose hardware deviceinfo nic <interface>` `get hardware nic <interface>`	Show detailed interface information.
`get sys interface transceiver`	Show connected transceivers.

Packet sniffer

Command	Description
`diagnose sniffer packet <interface> <'filter'> <verbose> <count> <a|l>`	Execute the inbuilt packet sniffer, filtered on a particular interface with the specified filter. For more information, see Performing a sniffer trace or packet capture.

Debug flow

Command	Description
`diagnose debug reset`	Stop all the prior debugs that were enabled and running in the foreground or background.
`diagnose debug flow filter clear`	Clear any IPv4 debug flow filters.
`diagnose debug flow filter6 clear`	Clear any IPv6 debug flow filters.
`diagnose debug flow filter <filter>`	Set a filter for running IPv4 traffic debug flows.
`diagnose debug flow filter6 <filter>`	Set a filter for running IPv6 traffic debug flows.
`diagnose debug flow show function-name enable`	Show the function name of the code that the traffic accesses.
`diagnose debug flow show iprope enable`	Show which internal firewall policy that the traffic is going through.
`diagnose debug console timestamp enable`	Start printing timestamps on debugs.
`diagnose debug flow trace start <n>`	Show n lines of IPv4 debugs.
`diagnose debug flow trace start6 <n>`	Show n lines of IPv6 debugs.
`diagnose debug enable`	Start printing debugs in the console.

For more detailed debug flow filter information, see Technical Tip: Using filters to review traffic traversing the FortiGate.

UTM

Command	Description

`diagnose debug urlfilter <filter>`
`diagnose debug application urlfilter -1`
`diagnose debug enable`
	Start real-time debugging for web filter traffic.

`diagnose debug enable` `diagnose test application urlfilter`	List the web filter debug outputs.
`diagnose test application urlfilter <option>`	Show the web filter debug output for the specified option.
`diagnose debug application dnsproxy -1` `diagnose debug enable`	Start real-time debugging for DNS proxy. DNS proxy is responsible for DNS filter, DNS translation, DNS resolution etc.
`diagnose debug enable` `diagnose test application dnsproxy`	List the DNS proxy debug outputs.
`diagnose test application dnsproxy <option>`	Show the DNS proxy debug output for the specified option.

`diagnose ips filter set "host <x.x.x.x> and port <port>"`
`diagnose ips debug enable all`
`diagnose debug enable`
	Start IPS engine debugs for Application Control and IPS Security profile

`diagnose ips debug enable av`
`diagnose ips debug status show`
`diagnose sys scanunit debug all enable`
`diagnose sys scanunit debug level verbose`
`diagnose sys scanunit debug show`
`diagnose debug enable`
	Start real-time debugging for antivirus profile when antivirus profile is configured in flow mode.

`diagnose wad debug enable category scan`
`diagnose wad stream-scan av-test "debug enable"`
`diagnose wad stream-scan av-test "debug all:debug"`
`diagnose sys scanunit debug all enable`
`diagnose sys scanunit debug level verbose`
`diagnose sys scanunit debug show`
`diagnose debug enable`
	Start real time debugging for antivirus profile when antivirus profile is configured in proxy mode.

IPS engine

The IPS engine handles traffic related to flow-based processing.

Real-time debugs are CPU intensive tasks. Running real-time IPS engine debugs with proper filters can result in high CPU usage.

Command	Description
`diagnose test application ipsmonitor 1`	Show IPS engine information
`diagnose test application ipsmonitor 2`	Set the IPS engine enable/disable status.
`diagnose test application ipsmonitor 99`	Restart all IPS engines and monitor.
`diagnose test application ipsmonitor 97`	Start all IPS engines.
`diagnose test application ipsmonitor 98`	Stop all IPS engines.
`diagnose ips session list` `diagnose test application ipsmonitor 13`	Show the IPS sessions in each engine's memory space.

`diagnose ips filter set "host <x.x.x.x> and port <port>"`
`diagnose ips debug enable all`
`diagnose debug enable`
	Show IPS engine debugs for the traffic specified by the filter.

WAD

The WAD daemon handles proxy related processing.

Real-time debugs are CPU intensive tasks. Running real-time WAD debugs with proper filters can result in high CPU usage.

Command	Description
`diagnose test application wad 1000`	Show all WAD processes.
`diagnose test application wad 2`	Show total memory usage.
`diagnose test application wad 99`	Restart all WAD processes.

`diagnose wad debug display pid enable`
`diagnose wad filter <filter>`
`diagnose wad filter list`
`diagnose wad debug enable level <level>`
`diagnose wad debug enable category <category>`
`diagnose debug enable`
	Start real-time debugging of the traffic processed by WAD daemon.

`diagnose wad filter <filter>`	Set the filter for the WAD debugs.
`diagnose wad filter list`	Show all the filters that have been set for debugging.
`diagnose wad filter clear`	Clear the WAD filter settings.
`diagnose wad debug enable level <level>`	Set the verbosity level of the debugs.
`diagnose wad debug enable category <category>`	Set the traffic category.
`diagnose wad debug display pid enable`	Show the WAS worker PID in debugs that handle the session request.
`diagnose debug enable`	Start printing debugs in the console.

CPU profiling

Command	Description
`diagnose sys profile cpumask <cpu_id>`	Set the CPU core to profile.
`diagnose sys profile start`	Start CPU profiling and wait for one to two minutes to stop.
`diagnose sys profile stop`	Stop CPU profiling.
`diagnose sys profile module`	Show the applied kernel modules.
`diagnose sys profile show detail` `diagnose sys profile show order`	Show the CPU profiling result for the respective core.

Tree

Command	Description
`tree`	Show the entire command tree.
`tree execute`	Show the execute command tree.
`tree diagnose`	Show the diagnose command tree.

IPv4 and IPv6 routing

Command	Description
`get router info routing-table all`	Show routing table.
`get router info routing-table database` `get router info6 routing-table database`	Show IPv4 and IPv6 routing database information.

`diagnose ip route list`
`get router info kernel`
`diagnose ipv6 route list`
`get router info6 kernel`
	Show the IPv4 and IPv6 kernel routing table.

`get router info protocols` `get router info6 protocols`	Show routing protocol information for IPv4 and IPv6.
`execute router restart`	Restart the routing daemon
`get router info ospf status` `get router info6 ospf status`	Show OSPF status for IPv4 and IPv6.
`get router info ospf neighbor` `get router info6 ospf neighbor`	Show OSPF neighbors for IPv4 and IPv6.
`get router info ospf database brief`	Show OSPF database in brief.
`get router info bfd neighbor` `get router info6 bfd neighbor`	Show BFD neighbors for IPv4 and IPv6.

`diagnose test application bfd 1`
`diagnose test application bfd 2`
`diagnose test application bfd 3`
	Show BFD statistics.

`diagnose debug application bfdd <debug level>` `diagnose debug enable`	Start real-time BFD debugging .
`get router info bgp summary` `get router info6 bgp summary`	Show BGP summary for IPv4 and IPv6.

`get router info bgp neighbors`
`get router info6 bgp neighbors`
`get router info bgp neighbors <x.x.x.x> advertised-routes`
`get router info6 bgp neighbors <x:x::x:x/m> advertised-routes`
`get router info bgp neighbors <x.x.x.x> received-routes`
`get router info6 bgp neighbors <x:x::x:x/m> received-routes`
`get router info bgp neighbors <x.x.x.x> routes`
`get router info6 bgp neighbors <x:x::x:x/m> routes`
	Show BGP peer and the advertised and received routes from the BGP peer.
	• Substitute <x.x.x.x> with IPv4 address of the peer.
	• Substitute <x:x::x:x/m> with IPv6 address of the peer.

`diagnose ip router bgp all enable`
`diagnose ip router bgp level info`
`diagnose debug enable`
	Start real-time BGP debugging.

`execute router clear bgp {all | as <ASN> | ip x.x.x.x | ipv6 y:y:y:y:y:y:y:y}`	Execute a hard reset based on the specified parameters: • `all`: all BGP peers • `as <ASN>`: BGP peers specified by AS number • `ip x.x.x.x`: BGP peer specified by IPv4 address (x.x.x.x) • `ipv6 y:y:y:y:y:y:y:y`: BGP peer specified by IPv6 address (y:y:y:y:y:y:y:y)
`execute router clear bgp {all | ip x.x.x.x | ipv6 y:y:y:y:y:y:y:y} soft {in|out}`	Executea soft reset based on the specified parameter: • `all`: all BGP peers • `ip x.x.x.x`: BGP peer specified by IPv4 address (x.x.x.x) • `ipv6 y:y:y:y:y:y:y:y`: BGP peer specified by IPv6 address (y:y:y:y:y:y:y:y) • `in`: received BGP routes only • `out`: advertised BGP routes only A soft reset will occur in both directions if neither in nor out is specified.
`get router info ospf status` `get router info6 ospf status`	Show OSPF status for IPv4 and IPv6.
`get router info ospf interface` `get router info6 ospf interface`	Show OSPF running on interface for IPv4 and IPv6.
`get router info ospf neighbor all` `get router info6 ospf neighbor all`	Show OSFP neighbor information for IPv4 and IPv6.
`get router info ospf database brief` `get router info6 ospf database brief`	Show OSPF database in brief for IPv4 and IPv6.

`diagnose ip router ospf all enable`
`diagnose ip router ospf level info`
`diagnose debug enable`
	Start real-time OSPF debugging.

Multicast routing

Command	Description
`get router info multicast igmp interface`	Show IGMP statistics for an interface.
`get router info multicast igmp groups`	Show multicast groups subscribed to with IGMP.
`diagnose ip multicast get-igmp-limit`	Show maximum IGMP states.

`diagnose ip router igmp decode enable`
`diagnose ip router igmp level info`
`diagnose debug console timestamp enable`
`diagnose debug enable`
	Start real-time debugging of IGMP daemon.

`execute mrouter clear igmp-interface <interface>`	Clear all IGMP entries from one interface.
`execute mrouter clear igmp-group <group-address>`	Clear all IGMP entries for one or all groups.
`get router info multicast pim sparse-mode <interface>.`	Show sparse-mode interface information.
`get router info multicast pim sparse-mode <neighbor>`	Show sparse-mode neighbor information.
`get router info multicast pim sparse-mode rp-mapping`	Show RP to group mapping information.
`get router info multicast pim sparse-mode table`	Show sparse-mode routing table.

`diagnose ip router pim-sm events enable`
`diagnose ip router pim-sm all enable`
`diagnose ip router pim-sm level info`
`diagnose debug enable`
	Start real-time debugging of PIM sparse mode.

SD-WAN

Command	Description
`diagnose sys sdwan health-check status`	Show SD-WAN health check statistics.
`diagnose sys sdwan service4` `diagnose sys sdwan service6`	Show SD-WAN rules in control plane.
`diagnose sys sdwan member`	Show SD-WAN members.
`diagnose firewall proute list`	Show SDWAN rule and policy routes in the data plane.
`diagnose sys link-monitor status` `diagnose sys link-monitor interface <interface>`	Show link monitoring statistics.
`diagnose debug application link-monitor -1` `diagnose debug enable`	Start real-time link monitor debugging.

`diagnose test application lnkmtd 1`
`diagnose test application lnkmtd 2`
`diagnose test application lnkmtd 3`
	Show link monitoring statistics.

Authentication

Command	Description
`diagnose firewall auth filter <filter>`	Set the filter used to list entries.
`diagnose firewall auth list`	List filtered, authenticated IPv4 users.
`diagnose wad user list`	List current users authenticated by proxy (wad daemon).

`diagnose debug application fnbamd -1`
`diagnose debug application authd -1`
`diagnose debug enable`
	Start real-time debugging for remote and local authentication.

`diagnose test authserver <auth_protocol> <server_name> <user> <password>`	Test authentication directly from the CLI. Caution: The password is visible in clear text; be careful when capture this command to a log file.
`diagnose test authserver ldap <server_name> <user> <password>`	Test user authentication using an LDAP server. Caution: The password is visible in clear text; be careful when capture this command to a log file.
`diagnose test authserver radius <server_name> <auth_type> <user> <password>`	Test user authentication using a Radius server. Caution: The password is visible in clear text; be careful when capture this command to a log file.
`diagnose debug fsso-polling detail` `diagnose debug fsso-polling summary`	Show information about the polls from FortiGate to DC.
`diagnose debug fsso-polling user` `diagnose debug authd fsso list`	Show FSSO logged on users when Fortigate polls the DC.

`diagnose debug application fssod -1`
`diagnose debug application smbcd -1`
`diagnose debug enable`
	Start real-time debugging when the FortiGate is used for FSSO polling.

`diagnose debug fsso-polling refresh-user` `execute fsso refresh`	Refresh the current logged on FSSO users and refresh the list. Caution: This command can cause an outage, use it carefully.
`diagnose debug authd fsso server-status`	Show current status of connection between FortiGate and the collector agent.
`diagnose debug application authd 8256` `diagnose debug enable`	Start real-time debugging for the connection between FortiGate and the collector agent.
`diagnose debug authd fsso refresh-logons`	Resend the logged-on users list to FortiGate from the collector agent.
`diagnose debug application authd 8256` `diagnose debug enable`	Start real-time debugging for the connection between FortiGate and the collector agent.
`diagnose debug application samld -1` `diagnose debug enable`	Start real-time SAML debugging.

IPsec

Command	Description
`diagnose vpn ike gateway list`	Show IPsec phase 1 information.
`diagnose vpn tunnel list`	Show IPsec phase 2 information.
`get vpn ipsec tunnel summary` `get vpn ipsec tunnel details`	Show summary and detailed information about IPsec tunnels.
`diagnose vpn tunnel flush`	Flush all Phase2 tunnel SAs (Security Associations).
`diagnose vpn tunnel flush <name> [name]`	Flush one or more specific Phase2 tunnels by name.
`diagnose vpn ike gateway <clear | flush>`	Clear/flush IKE gateways (Phase1). Apply `diagnose vpn ike gateway filter` to filter on specific gateways.
`diagnose vpn ike gateway <clear | flush> name <name>`	Clear/flush a specific IKE gateway (Phase1) by name.
`diagnose vpn ike gateway filter`	Use various options to filter the IKE gateways.
`diagnose vpn ipsec status`	Show information about encryption counters.
`diagnose vpn ike log filter <filter>`	Set a filter for IKE daemon debugs.
`diagnose debug application ike -1` `diagnose debug enable`	Start real-time debugging of IKE daemon with the filter set.
`diagnose vpn ike restart`	Restart the IKE process.

`diagnose vpn ike counts`
`diagnose vpn ike routes`
`diagnose vpn ike errors`
`diagnose vpn ike stats`
`diagnose vpn ike status`
`diagnose vpn ike crypto`
	Show other information, such as IKE counts, routes, errors, and statistics.

SSL VPN

SSL VPN web mode has become Agentless VPN, and SSL VPN tunnel mode is no longer supported in 7.6.3 and later. Therefore, SSL VPN related debug commands may not work as expected.

Command	Description
`diagnose vpn ssl debug-filter list`	Show any filters that are set for SSL VPN debug.
`diagnose vpn ssl debug-filter clear`	Clear any filters that are set for SSL VPN daemon debug.
`diagnose vpn ssl debug-filter <filter>`	Set a filter for SSL VPN debugs.
`diagnose debug application sslvpn -1` `diagnose debug enable`	Start SSL VPN debugs for traffic that the filter is applied to.

`diagnose vpn ssl list`
`get vpn ssl monitor`
`execute vpn sslvpn list`
	Show the current SSL VPN sessions for both web and tunnel mode.

`diagnose vpn ssl statistics` `diagnose vpn ssl mux-stat`	Show the SSL VPN statistics.
`execute vpn sslvpn list`	Show all SSL VPN web and tunnel mode connections.
`execute vpn sslvpn del-tunnel`	Disconnect the users from tunnel mode SSL VPN connection.
`execute vpn sslvpn del-web`	Disconnect the users from web mode SSL VPN connection.

Managed FortiSwitches

The successful execution of commands for managed FortiSwitches requires that the feature is available on the FortiSwitch device itself. See the FortiSwitchOS Feature Matrix.

Enter `?` to view additional options or parameters required to obtain the required information in the `diagnose switch-controller switch-info` commands.

Command	Description
`diagnose switch-controller switch-info mac-table`	Show managed FortiSwitch MAC address list.
`diagnose switch-controller switch-info port-stats`	Show managed FortiSwitch port statistics.
`diagnose switch-controller switch-info trunk status`	Show managed FortiSwitch trunk information.
`diagnose switch-controller switch-info mclag`	Show MCLAG related information from FortiSwitch.
`diagnose switch-controller switch-info poe`	Show POE-related information.
`diagnose switch-controller switch-info lldp`	Show LLDP-related information.
`diagnose switch-controller switch-info port-properties`	Show managed FortiSwitch port properties.
`diagnose switch-controller switch-info acl-counters`	Show managed FortiSwitch port ACL counters information.
`diagnose switch-controller switch-info pdu-counters-list`	Show managed FortiSwitch pdu-counters information.
`diagnose switch-controller switch-info flapguard`	Show managed FortiSwitch flapguard information.
`diagnose switch-controller switch-info qos-stats`	Show managed FortiSwitch QoS statistics.
`diagnose switch-controller switch-info modules`	Show modules related information from FortiSwitch.
`diagnose switch-controller switch-info stp`	Show managed FortiSwitch STP instance status.
`diagnose switch-controller switch-info bpdu-guard-status`	Show managed FortiSwitch STP BPDU guard status.
`diagnose switch-controller switch-info igmp-snooping`	Show managed FortiSwitch IGMP snooping information.
`diagnose switch-controller switch-info loop-guard`	Show managed FortiSwitch loop-guard status.
`diagnose switch-controller switch-info dhcp-snooping`	Show managed FortiSwitch DHCP snooping interface list.
`diagnose switch-controller switch-info arp-inspection`	Show managed FortiSwitch ARP inspection interface list.
`diagnose switch-controller switch-info option82-mapping`	Show managed FortiSwitch DHCP option 82 mapping information.
`diagnose switch-controller switch-info 802.1X`	Show managed FortiSwitch port 802.1X status.
`diagnose switch-controller switch-info 802.1X-dacl`	Show managed FortiSwitch port 802.1X dynamic ACL status.
`diagnose switch-controller switch-info mac-limit-violations`	Show managed FortiSwitch violated MACs information.
`diagnose switch-controller switch-info flow-tracking`	Show managed FortiSwitch flow information.
`diagnose switch-controller switch-info mirror`	Show managed FortiSwitch mirror information.
`diagnose switch-controller switch-info ip-source-guard`	Show managed FortiSwitch source guard information in hardware.
`diagnose switch-controller switch-info rpvst`	Show managed FortiSwitch STP port information when inter-operating with rapid PVST network.
`execute switch-controller get-conn-status <FortiSwitch-SN>`	Show FortiSwitch connection status.
`execute switch-controller get-physical-conn standard <FortiSwitch-SN>`	Show FortiLink connectivity graph.
`execute switch-controller diagnose-connection <FortiSwitch-SN>`	Show FortiSwitch connection diagnostics.

Managed FortiAPs

Command	Description
`diagnose wireless-controller wlac -c wtp` `diagnose wireless-controller wlac -d wtp`	Show information about the FortiAP devices.
`diagnose wireless-controller wlac -c sta` `diagnose wireless-controller wlac -d sta`	Show information about the wireless clients connected to the FortiAP devices.
`diagnose wireless-controller wlac help`	Show a list of debug options available for the wireless controller.

`diagnose wireless-controller wlac sta_filter`
`diagnose wireless-controller wlac sta_filter clear`
`diagnose wireless-controller wlac sta_filter <aa:bb:cc:dd:ee:ff> 255`
`diagnose debug enable`
	Start real-time debugging of a wireless client/station that connects to the FortiAP.
	• `<aa:bb:cc:dd:ee:ff>`: MAC address of endpoint/station

`diagnose wireless-controller wlac -c vap`	Show virtual access point information, including its MAC address, BSSID, SSID, the interface name, and the IP address of the APs that are broadcasting it.

`diagnose wireless-controller wlac wtp_filter`
`diagnose wireless-controller wlac wtp_filter clear`
`diagnose wireless-controller wlac wtp_filter <FAP-SN> 0-<x.x.x.x>:5246 255`
`diagnose debug application cw_acd 0x7ff`
	Show the wireless termination point (WTP), or FortiAP, debugging on the wireless controller if FortiAP is failing to connect to FortiGate.
	• `<FAP-SN>`: FortiAP serial number
	• `<x.x.x.x>`: FortiAP IP address

High availability

Command	Description
`diagnose system ha status` `get system ha status`	Show HA status and information.
`execute ha manage <index> <username>`	Log into and manage a specific HA member.
`diagnose sys ha checksum cluster`	Show checksum information of all cluster members.
`diagnose sys ha checksum show <vdom>`	Show detailed checksum information for a VDOM.
`diagnose sys ha checksum recalculate`	Recalculate HA checksums.
`diagnose sys ha recalculate-extfile-signature`	Recalculate HA external files signatures.
`diagnose sys ha reset-uptime`	Reset the HA uptime. This is used to test failover.

`diagnose debug application hatalk -1`
`diagnose debug application hasync -1`
`diagnose debug application harelay -1`
`diagnose debug enable`
	Start real-time debugging of HA daemons.

`diagnose sys ha history read`	Show HA history.
`execute ha synchronize stop` `execute ha synchronize start`	Manually start and stop HA synchronization.

ZTNA

The WAD daemon handles proxy related processing.

The FortiClient NAC daemon (fcnacd) handles FortiGate to EMS connectivity.

Command	Description
`diagnose endpoint fctems test-connectivity <EMS>`	Verify FortiGate to FortiClient EMS connectivity.
`execute fctems verify <EMS>`	Verify the FortiClient EMS's certificate.
`diagnose test application fcnacd 2`	Dump the EMS connectivity information.
`diagnose debug app fcnacd -1` `diagnose debug enable`	Run real-time FortiClient NAC daemon debugs.
`diagnose endpoint ec-shm list <ip> <mac> <EMS_serial_number> <EMS_tenant_id>`	Show the endpoint record list. Optionally, add filters.
`diagnose endpoint lls-comm send ztna find-uid <uid> <EMS_serial_number> <EMS_tenant_id>`	Query endpoints by client UID, EMS serial number, and EMS tenant ID.
`diagnose endpoint lls-comm send ztna find-ip-vdom <ip> <vdom>`	Query endpoints by the client IP-VDOM pair.
`diagnose wad dev query-by uid <uid> <EMS_serial_number> <EMS_tenant_id>`	Query from WAD diagnose command by UID, EMS serial number, and EMS tenant ID.
`diagnose wad dev query-by ipv4 <ip>`	Query from WAD diagnose command by IP address.
`diagnose firewall dynamic list`	List EMS security posture tags and all dynamic IP and MAC addresses.
`diagnose test application fcnacd 7` `diagnose test application fcnacd 8`	Check the FortiClient NAC daemon ZTNA and route cache.
`diagnose wad worker policy list`	Display statistics associated with application gateway rules.

`diagnose wad debug enable category all`
`diagnose wad debug enable level verbose`
`diagnose debug enable`
	Run real-time WAD debugs.

`diagnose debug reset`	Reset debugs when completed

Logging

Command	Description
`diagnose log test`	Generate logs for testing.
`execute log filter <filter>`	Set log filters.
`execute log filter`	Show log filters.
`exec log display`	Show filtered logs.
`execute log delete`	Delete filtered logs.
`diagnose debug application miglogd -1` `diagnose debug enable`	Start real-time debugging of logging process miglogd.
`execute log fortianalyzer test-connectivity`	Test connectivity between FortiGate and FortiAnalyzer.

Traffic shaping

Command	Description
`diagnose firewall shaper traffic-shaper list`	Show configured traffic shapers.
`diagnose firewall shaper traffic-shaper stats list`	Show traffic shaper statistics.

SIP session helper

Command	Description
`diagnose sys sip status`	Show SIP status.
`diagnose sys sip mapping list`	Show SIP mapping list.
`diagnose sys sip dialog list`	Show SIP dialogue list.
`diagnose debug application sip -1` `diagnose debug enable`	Start real-time SIP debugging.

SIP ALG

Command	Description
`diagnose sys sip-proxy calls list`	Show list of active SIP proxy calls.
`diagnose sys sip-proxy stats`	Show SIP proxy statistics.
`diagnose sys sip-proxy session list`	Show SIP proxy session list.
`diagnose debug application sip -1` `diagnose debug enable`	Start real-time SIP debugging.