FortiAI - CLI Reference Guide

Version 1.3.1

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

August 14, 2020
FortiAI 1.3.1 CLI Reference Guide
55-131-639184-20200814

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-14	Initial release.

Introduction

You can access the FortiAI CLI (Command Line Interface) using the FortiAI console or using an SSH or TELNET client. These services must be enabled on the port1 interface.

CLI commands are intended to be used for initial device configuration and troubleshooting. Some commands are specific to hardware or VM devices. Use `?` with the command for information on how to use the command.

The FortiAI CLI is case-sensitive.

Configuration commands

config profile ldap

Use this command to configure LDAP profiles which can query LDAP servers for authentication.

Before using an LDAP profile, verify each LDAP query and connectivity with your LDAP server.

Each LDAP profile contains queries that retrieve configuration data from an LDAP server, such as user groups.

Syntax

```
config profile ldap
    edit <profile_name>
        set auth-bind-dn {cnid | none | searchuser | upn}
        set authstate {enable | disable}
        set base-dn <basedn_str>
        set bind-dn <binddn_str>
        set bind-password <bindpw_str>
        set cache-state {enable | disable}
        set cache-ttl <ttl_int>
        set cnid-name <cnid_str>
        set dereferencing {never | always | search | find}
        set fallback-port <port_int>
        set fallback-server {<fqdn_str> | <server_ipv4>}
        set port <port_int>
        set query <query_str>
        set scope {base | one | sub}
        set secure {none | ssl}
        set server <name_str>
        set timeout <timeout_int>
        set unauth-bind {enable | disable}
        set upn-suffix <upns_str>
        set version {ver2 | ver3}
    end
```

Variable	Description	Default
`<profile_name>`	Name of the LDAP profile.	
`auth-bind-dn {cnid | none | searchuser | upn}`	`none`: Do not define a user authentication query. `cnid`: Name of the user objects' common name attribute, such as `cn` or `uid`. `searchuser`: Form the user's bind DN (distinguished name) by using the DN retrieved for that user.	`searchuser`

Variable	Description	Default
	upn: Form the user’s bind DN by prepending the user name portion of the email address ($u) to the user principal name (UPN such as example.com). By default, FortiAI uses the mail domain as the UPN. To use a UPN other than the mail domain, also configure upn-suffix <upns_str>.	
authstate {enable | disable}	Enable to perform user authentication queries.	disable
base-dn <basedn_str>	The DN of the part of the LDAP directory tree where FortiAI searches for user objects, such as ou=People,dc=example,dc=com. User objects must be child nodes of this location.	
bind-dn <binddn_str>	The bind DN of an LDAP user account with permissions to query the basedn, such as cn=FortiAI,dc=example,dc=com. This command is optional if your LDAP server does not require FortiAI to authenticate when performing queries and you have enabled unauth-bind.	
bind-password <bindpw_str>	The password of bind-dn.	
cache-state {enable | disable}	Enable to cache LDAP query results. Caching LDAP queries can reduce LDAP network traffic when there are frequent queries for information that does not change. However, caching might cause a delay from the time you update LDAP directory information and when FortiAI begins using that new information. If you enable this option but queries are not cached, check the TTL value. A TTL value of 0 effectively disables caching.	disable
cache-ttl <ttl_int>	The amount of time, in minutes, that FortiAI caches query results. After the time has elapsed, cached results expire and subsequent requests for that information requires FortiAI to query the LDAP server and refresh the cache. The default TTL value is 1440 minutes (one day). The maximum is 10080 minutes (one week). A value of 0 effectively disables caching.	1440
cnid-name <cnid_str>	Name of the user objects’ common name attribute, such as cn or uid.	
dereferencing {never | always | search | find}	Method of de-referencing attributes whose values are references. never: Do not de-reference. always: Always de-reference. search: De-reference only when searching.	never

Variable	Description	Default
	find: De-reference only when finding the base search object.	
fallback-port <port_int>	If you have configured a backup LDAP server that listens on a nonstandard port, enter the TCP port number. The standard port for LDAP is 389. The standard port for SSL-secured LDAP is 636. If secure is set to ssl, FortiAI uses SSL-secured LDAP to connect to the server.	389
fallback-server {<fqdn_str> | <server_ipv4>}	The FQDN or IP address of the backup LDAP server. If there is no fallback server, enter an empty string ('').	
port <port_int>	If you have configured a backup LDAP server that listens on a nonstandard port, enter the TCP port number. The standard port for LDAP is 389. The standard port for SSL-secured LDAP is 636.	389
query <query_str>	An LDAP query filter, enclosed in single quotes ('), that selects a set of user objects from the LDAP directory. The query filter string filters the result set based on attributes common to all user objects and excludes non-user objects. For example, if user objects in your directory have two characteristics, the objectClass and mail attributes, use the query filter: (& (objectClass=inetOrgPerson) (mail=$m)) where $m is the FortiAI variable for a user's email address. This command applies to user defined schema only. For details on query syntax, see any standard LDAP query filter reference manual.	(& (objectClass= inetOrgPerson) (mail=$m))
scope {base | one | sub}	The level of depth to query: base: Query the basedn level. one: Query only one level below the basedn in the LDAP directory tree. sub: Query recursively all levels below the basedn in the LDAP directory tree.	sub
secure {none | ssl}	Whether to connect to LDAP servers using an encrypted connection: none: Use a non-secure connection. ssl: Use an SSL-secured (LDAPS) connection.	none
server <name_str>	The FQDN or IP address of the LDAP server.	
timeout <timeout_int>	The maximum length of time in seconds that FortiAI waits for query responses from the LDAP server.	10

Variable	Description	Default
unauth-bind {enable | disable}	Enable to perform queries in this profile without supplying a bind DN and password for the directory search. Many LDAP servers require LDAP queries to be authenticated using a bind DN and password. If your LDAP server does not require FortiAI to authenticate before performing queries, you might enable this option. If this option is disabled, you must configure bind-dn and bind-password.	disable
upn-suffix <upns_str>	If you want to use a UPN other than the mail domain, enter that UPN. This is useful if users authenticate with a domain other than the mail server's principal domain name.	
version {ver2 | ver3}	The protocol version used to communicate with the LDAP server.	ver3

config profile authentication radius

Use this command to configure FortiAI to connect to an external RADIUS server to authenticate FortiAI Users.

Syntax

```
config profile authentication radius
    edit <profile_name>
        set auth-prot {auto | chap | mschap | mschap2 | pap}
        set nas-ip <ip_addr>
        set port <port_int>
        set secret <password_str>
        set send-domain {enable | disable}
        set server {<fqdn_str> | <host_ipv4>}
    end
```

Variable	Description	Default
server {<fqdn_str> | <host_ipv4>}	The IP address or FQDN of the POP3 server.	
auth-prot {auto | chap | mschap | mschap2 | pap}	The authentication method for the RADIUS server.	auto
nas-ip <ip_addr>	The NAS IP address and the Called Station ID. If you do not enter an IP address, FortiAI uses the IP address that the FortiAI interface uses to communicate with the RADIUS server. For information about RADIUS attribute 31, see Microsoft Vendor-specific RADIUS Attributes.	0.0.0.0
port <port_int>	If the RADIUS server listens on a nonstandard port number, enter the port number of the RADIUS server.	1812

Variable	Description	Default
	The standard port number for RADIUS is 1812.	
`secret <password_str>`	The password of the RADIUS server.	
`send-domain {enable | disable}`	Enable if the RADIUS server requires both the user name and the domain when authenticating.	
`server {<fqdn_str> | <host_ipv4>}`	The IP address or FQDN of the RADIUS server.	

config system accprofile

Use this command to configure access profiles. This command governs which areas of the web-based manager and CLI that administrators can access and whether they have permission to change the configuration or other items in each area.

Everyone is treated as an administrator. Set up non-administrators with a custom non-administrator `accprofile`.

The GUI *Admin Profiles* is the `accprofile`. Only the default *SuperAdminProfile* can modify *Admin Profiles* and `accprofile`. Only administrators with the default *SuperAdminProfile* can reboot or shut down the system.

Syntax

```
config system accprofile
    edit <profile_name>
        set system-access {none | read | read-write}
        set system-config {none | read | read-write}
        set system-maintenance {none | read | read-write}
        set system-status {none | read | read-write}
    end
```

Variable	Description	Default
`<profile_name>`	Name of the access profile.	
`system-access {none | read | read-write}`	Specify the account permission associated with this access profile. The `read-write` permission gives access to settings critical to FortiAI network accessibility, including GUI console, network, administrator, admin profiles, certificates, and RADIUS/LDAP authentication.	`none`
`system-config {none | read | read-write}`	Specify the account permission associated with this access profile. The `read-write` permission gives access to modify other system settings such as system time settings, system FortiGuard update, and Security Fabric settings.	`none`

Variable	Description	Default
`system-maintenance {none | read | read-write}`	Specify the account permission associated with this access profile. The `read-write` permission gives access to system maintenance settings such as back up system configuration, restore configuration, and restore firmware.	`none`
`system-status {none | read | read-write}`	Specify the account permission associated with this access profile. The `read-write` permission gives access to the system to check its status. Users with this permission set to `none` cannot log into the system. The default is `none` in the GUI.	`none`

config system admin

Use this command to configure FortiAI administrator accounts.

By default, FortiAI units have a single administrator account named admin. For more granular control over administrative access, you can create additional administrator accounts with more restricted permissions such as being able to configure a specific domain.

Syntax

```
config system admin
    edit <name_str>
        set access-profile <profile_name>
        set auth-strategy {local | local-plus-radius | pki | radius}
        set name <name>
        set password <password_str>
        set radius-permission-check {enable | disable}
        set radius-subtype-id <subtype_int>]
        set radius-vendor-id <vendor_int>
        set sshkey <key_str>
        set status {enable | disable}
        set theme {Blue | Green | Mariner | Red}
        set trust-hosts <host_ipv4mask>
    end
```

Variable	Description	Default
`<name_str>`	Name of the administrator account.	
`access-profile <profile_name>`	Name of an access profile that determines which functional areas the administrator account may view or affect.	
`auth-strategy {local | local-plus-radius | pki | radius}`	Select the local or remote type of authentication that the administrator can use.	`local`
`name <name>`	Name of user.	`english`

Variable	Description	Default
`password <password_str>`	If `auth-strategy` is local or `local-plus-radius`, enter the password for the administrator account. Do not use an administrator password shorter than six characters. For better security, use a longer password with a complex combination of characters and numbers. Change the password regularly. A weak password might compromise the security of your FortiAI unit.	
`radius-permission-check {enable | disable}`	If `auth-strategy` is local or `local-plus-radius`, enable this option to query the RADIUS server for the permissions attribute.	`disable`
`radius-subtype-id <subtype_int>]`	If `auth-strategy` is local or `local-plus-radius`, and `radius-permission-check` is enabled, enter the RADIUS subtype identifier.	`0`
`radius-vendor-id <vendor_int>`	If `auth-strategy` is local or `local-plus-radius`, and `radius-permission-check` is enabled, enter the RADIUS vendor identifier.	`0`
`sshkey <key_str>`	Enter the SSH key string inside single straight quote marks ('). When connecting from an SSH client that presents this key, administrators do not need to enter the account name and password to log in to the CLI.	
`status`	Enable or disable admin users.	
`theme {Blue | Green | Mariner | Red}`	Theme of the GUI for this admin.	`Green`
`trust-hosts <host_ipv4mask>`	Enter one to three IP addresses and netmasks from which the administrator can log into FortiAI. Separate each pair of IP address and netmask with a comma (,). To allow the administrator to authenticate from any IP address, enter `0.0.0.0/0.0.0.0`.	`0.0.0.0/0.0.0.0`

config system appearance

Use this command to customize the appearance of the web-based manager.

Syntax

```
config system appearance
    set login-page-theme {Blue | Green | Red}
end
```

Variable	Description	Default
`login-page-theme {Blue | Green | Red}`	The theme of the setting page for this user.	`Green`

config system automation-settings

Use this command to configure the automation profiles used by the FortiAI enforcement feature.

For information on FortiAI enforcement, see the FortiAI Administration Guide in the Fortinet Document Library.

Syntax

```
config system automation-settings
    edit <name_str>
        set vdom <vdom_str>
        set api-key <apikey_str>
        set webhook-config <config_str>
        set ip <ip_addr>
        set port <port_int>
        set enabled {enable | disable}
        set source {fabric-device | sniffer}
    end
```

Variable	Description	Default
`<name_str>`	Name of the automation profile.	
`vdom <vdom_str>`	VDOM of the FortiGate.	`root`
`api-key <apikey_str>`	API key of the FortiGate.	

`webhook-config <config_str>`	The FortiGate webhook configuration to be used by FortiAI enforcement.
	For example, to utilize the Ban IP enforcement action, provide the FortiGate webhook name for executing Ban IP, webhook name for undoing the execution, and the Ban IP action number (1) as JSON data.
	`{`
	`    "action" : 1,`
	`    "webhook_exec" : "ip_blocker",`
	`    "webhook_undo" : "ip_unblocker"`
	`}`
	To enter the JSON data through CLI, the JSON string must be formatted as one line and enclosed in single quotes ('). Using the above example, enter the JSON string as follows:
	`'{"action" : 1,"webhook_exec" : "ip_blocker","webhook_undo" : "ip_unblocker"}'`	

`ip <ip_addr>`	IP address of the FortiGate.	

Variable	Description	Default
`port <port_int>`	Port number of the FortiGate.	`443`
`enabled {enable | disable}`	Enable or disable the automation profile.	`enable`
`source {fabric-device | sniffer}`	Set the source of detection that applies to the current profile.	`fabric-device`

config system certificate ca

Use this command to import certificates for certificate authorities (CA).

Certificate authorities validate and sign other certificates to indicate to third parties that those certificates can be trusted.

CA certificates are required by connections that use transport layer security (TLS).

Syntax

```
config system certificate ca
    edit <name_str>
        set certificate <cert_str>
    end
```

Variable	Description	Default
`<name_str>`	The name of this certificate.	
`certificate <cert_str>`	Enter or paste the certificate in PEM format to import it.	

config system certificate crl

Use this command to import certificate revocation lists.

To ensure that FortiAI validates only certificates that have not been revoked, periodically upload a current certificate revocation list from certificate authorities (CA) or use the online certificate status protocol (OCSP) to query the certificate status.

Syntax

```
config system certificate crl
    edit <name_str>
        set crl <cert_str>
    end
```

Variable	Description	Default
`<name_str>`	The name of this certificate revocation list.	

Variable	Description	Default
crl <cert_str>	Enter or paste the certificate in PEM format to import it.	

config system certificate local

Use this command to import signed certificates and certificate requests to install them for local use by FortiAI.

FortiAI requires a local server certificate that it can present when clients request secure connections.

When using this command to import a local certificate, you must follow the order of the commands described below. This is because privatekey needs the password to decrypt the private key and certificate needs a matched private key file.

Syntax

```
config system certificate local
    edit <name_str>
        set password
        set private-key
        set certificate <cert_str>
        set csr <csr_str>
        set comments <comment_str>
    end
```

Variable	Description	Default
<name_str>	The name of the certificate to be imported.	
password	The password of the certificate.	
private-key	The private key of the certificate.	
certificate <cert_str>	Enter or paste the certificate in PEM format to import it.	
csr <csr_str>	Enter or paste the certificate signing request in PEM format to import it.	
comments <comment_str>	Comments for this certificate.	

config system certificate remote

Use this command to import the certificates of the online certificate status protocol (OCSP) servers of your certificate authority (CA).

OCSP lets you revoke or validate certificates by query rather than by importing certificate revocation lists (CRL).

If you enable OCSP for PKI users, remote certificates are required.

Syntax

```
config system certificate remote
    edit <name_str>
        set certificate <cert_str>
    end
```

Variable	Description	Default
`<name_str>`	The name of the certificate to be imported.	
`certificate <cert_str>`	Enter or paste the certificate in PEM format to import it.	

config system dhcp server

Use this command to configure the DHCP server object.

Syntax

```
config system dhcp server
    edit <serverName>
        config exclude-range
            edit <id of IP address>
        config ip-range
            edit <id of IP address>
        config reserved-address
            edit <id of IP address>
        set auto-configuration {enable | disable}
        set conflicted-ip-timeout <int>
        set default-gateway <IP Address>
        set dns-service {default | specify}
        set domain <domain name>
        set enable {enable | disable}
        set htype {normal | other}
        set interface <interface name>
        set lease-time <lease time in seconds>
        set netmask <netmask_ip>
    end
```

Variable	Description	Default
`edit <serverName>`	The server name of this DHCP server.	
`config exclude-range`	DHCP excluded IP range.	
`config ip-range`	DHCP IP address range.	
`config reserved-address`	DHCP reserved IP address.	
`auto-configuration {enable | disable}`	Enable or disable auto configuration.	`enable`
`conflicted-ip-timeout <int>`	IP address conflict timeout in seconds.	`1800`

Variable	Description	Default
`default-gateway <IP Address>`	Default gateway IP address.	`192.168.2.99`
`dns-service {default | specify}`	DNS server options.	`default`
`domain <domain name>`	Domain name of the DHCP server.	
`enable {enable | disable}`	Enable or disable this DHCP server.	`enable`
`htype {normal | other}`	Device/port name.	
`interface <interface name>`	Interface name.	
`lease-time <lease time in seconds>`	Lease time in seconds.	`604800`
`netmask <netmask_ip>`	Netmask of this DHCP server.	`255.255.255.0`

config system dns

Use this command to configure the IP addresses of the primary and secondary DNS servers that FortiAI queries to resolve domain names into IP addresses.

Syntax

```
config system dns
    set cache {enable | disable}
    set cache-min-ttl <time_in_sec>
    set primary <dns_ipv4>
    set private_ip_query {enable | disable}
    set protected-domain-dns-servers <class_ip>
    set protected-domain-dns-state {enable | disable}
    set secondary <dns_ipv4>
    set truncate-handling {disable | tcp-retry}
end
```

Variable	Description	Default
`cache {enable | disable}`	Enable to cache DNS query results to improve performance. If memory is low, disable to free up more memory.	`enable`
`cache-min-ttl <time_in_sec>`	Minimum TTL for cached DNS records in seconds.	
`primary <dns_ipv4>`	IP address of the primary DNS server.	`0.0.0.0`
`private_ip_query {enable | disable}`	Enable to perform reverse DNS lookups on private network IP addresses, as defined in RFC 1918. The DNS server must have PTR records for your private network's IP addresses. Not having records for those IP addresses might increase DNS query time and cause query results to show *Host not found*.	`disable`

Variable	Description	Default
`protected-domain-dns-servers <class_ip>`	IP addresses of DNS servers for protected domains.	
`protected-domain-dns-state {enable | disable}`	Enable or disable using DNS servers for protected domains.	
`secondary <dns_ipv4>`	IP address of the secondary DNS serve.	`0.0.0.0`
`truncate-handling {disable | tcp-retry}`	Action for truncated UDP.	

config system enforcement-settings

Use this command to configure the FortiAI enforcement settings. Enforcement settings are policies for the FortiAI system to filter out malicious detection records for executing enforcement.

Syntax

```
config system enforcement-settings
    set allowlist <allowlist_ipv4mask>
    set risk-level <risk_lvl_int>
    set conf-level <conf_lvl_float>
end
```

Variable	Description	Default
`allowlist <allowlist_ipv4mask>`	The IP addresses and netmasks in the allowlist (white list) are excluded from enforcement consideration. Separate each pair of IP address and netmask with a comma (,).	
`risk-level <risk_lvl_int>`	Malicious detected records with the entered risk level and above are considered when executing enforcement by FortiAI. Valid values are `2` (medium risk), `3` (high risk), or `4` (critical risk).	`4`
`conf-level <conf_lvl_float>`	Malicious detected records with the entered confidence level and above are considered when executing enforcement by FortiAI. The valid range is `0.8` to `1.0`.	`0.8`

config system interface

Use this command to configure allowed and denied administrative access protocols, maximum transportation unit (MTU) size, and up or down administrative status for the network interfaces of FortiAI.

Proxy and built-in MTA behaviors are configured separately based on whether the protocol connection is incoming or outgoing. Because a network connection considers the network layer rather than the application layer when deciding whether to intercept a connection, the concept of incoming and outgoing connections is determined by IP addresses of connecting clients and servers.

Syntax

```
config system interface
    edit <physical_interface_str>, <logical_interface_str>, or loopback
        set allowaccess {ping http https snmp ssh telnet}
        set discover {enable | disable}
        set ip <ipv4mask>
        set ip6 <ipv6mask>
        set mode {static | dhcp}
        set mtu <mtu_int>
        set speed {auto | 10full | 10half | 100full | 100half | 1000full}
        set status {down | up}
        set type {vlan | redundant}
    end
```

If `type` is `vlan`:

```
{set redundant-link-monitor {mii-link | arp-link} }
{set redundant-member <member_interface_ str>}
```

If `type` is `redundant`:

```
{set vlanid <int>}
```

Variable	Description	Default
`<physical_interface_ str>`	Name of the physical network interface, such as port1.	
`<logical_interface_str>`	Name of the VLAN or redundant interface. Then set the interface type.	
`loopback`	A loopback interface is a logical interface that is always up (no physical link dependency) and the attached subnet is always present in the routing table. The FortiAI loopback IP address does not depend on a specific external port so it is possible to access it through several physical or VLAN interfaces. The loopback interface is useful when you use a layer 2 load balancer in front of several FortiAI units. In this case, you can set the FortiAI loopback interface IP address to be the same as the load balancer IP address so that FortiAI can pick up the traffic forwarded to it from the load balancer. In this version, you can only add one loopback interface.	
`allowaccess {ping | http | https | snmp | ssh | telnet}`	Add one or more protocols to the list of protocols that allow administrative access to FortiAI through this network interface: `ping`: Allow ICMP ping responses from this network interface. `http`: Allow HTTP access to the web-based manager and per-recipient quarantines. `https`: Allow secure HTTP (HTTPS) access to the web-based manager and per-recipient quarantines. `snmp`: Allow SNMP v2 access.	Varies by network interface.

Variable	Description	Default
	`ssh`: Allow SSH access to the CLI. `telnet`: Allow Telnet access to the CLI. ⚠ HTTP and Telnet connections are not secure and can be intercepted by a third party. To reduce risk, enable this option only on network interfaces connected directly to your management computer. To control SMTP access, configure access control rules and session profiles.	
`discover {enable | disable}`	Allow discovery of the interface on this port.	
`ip <ipv4mask>`	IP address and netmask of the network interface. If FortiAI is in transparent mode, IP address and netmask might display bridging. This means that the network interface is acting as a layer 2 bridge. If high availability (HA) is also enabled, IP address and netmask might display bridged (isolated) when the operating mode is worker (slave) and therefore the network interface is disconnected from the network, or bridging (waiting for recovery) when the operating mode is failed and the network interface is disconnected from the network until failover completes and restores connectivity.	
`ip6 <ipv6mask>`	The IPv6 address and netmask of the network interface. If FortiAI is in transparent mode, IP address and netmask might display bridging. This means that the network interface is acting as a layer 2 bridge. If high availability (HA) is also enabled, IP address and netmask might display bridged (isolated) when the operating mode is worker (slave) and therefore the network interface is disconnected from the network, or bridging (waiting for recovery) whe the operating mode is failed and the network interface is disconnected from the network until failover completes and restores connectivity.	
`mode {static | dhcp}`	Interface mode. DHCP mode applies only if FortiAI is operating in gateway mode or server mode.	`static`
`mtu <mtu_int>`	The maximum packet or Ethernet frame size from 576 to 1500 bytes. If network devices between FortiAI and its destinations require smaller or larger units of traffic, additional processing mgiht be required at each node to fragment or defragment the units which lowers network performance. Adjust the MTU size to match your network traffic to improve network performance.	`1500`

Variable	Description	Default
`type {vlan | redundant}`	`vlan`: A virtual LAN subinterface is a virtual interface on a physical interface. This subinterface allows routing of VLAN tagged packets using that physical interface but it is separate from other traffic on the physical interface. VLANs use ID tags to logically separate devices on a network into smaller broadcast domains. These smaller domains forward packets only to devices that are part of that VLAN domain. This reduces traffic and increases network security. An example of using VLANs is a company’s accounting department where computers are located at both main and branch offices. Accounting computers need to communicate with each other frequently and require increased security. VLANs allow accounting network traffic to be sent only to accounting computers and to connect accounting computers in different locations as if they were on the same physical subnet. After setting `type`, also configure redundant-link-monitor `{mii-link | arp-link}` and redundant-member `<member_ interface_ str>`. `redundant`: On the FortiAI unit, you can combine two or more physical interfaces to provide link redundancy. This allows you to connect to multiple switches to ensure connectivity in case one physical interface fails. In a redundant interface, traffic only goes over one interface at any time. This differs from an aggregated interface where traffic goes over all interfaces for increased bandwidth. This difference means redundant interfaces can have a more robust configuration with fewer possible points of failure. This is important in a fully-meshed HA configuration. After setting `type`, also configure `vlanid <int>`.	
`speed {auto | 10full | 10half | 100full | 100half | 1000full}`	Speed of the network interface. Some network interfaces might not support all speeds.	`auto`
`status {down | up}`	`up` enables the network interface to send and receive traffic. `down` disables the network interface.	`up`

config system route

Use this command to configure static routes.

Syntax

```
config system route
    edit <route_int>
        set destination <destination_ipv4mask>
        set gateway <gateway_ipv4>
        set interface <interface name>
    end
```

Variable	Description	Default
`<route_int>`	Index number of the route in the routing table.	
`destination <destination_ipv4mask>`	Destination IP address and netmask of traffic that is subject to this route, separated by a space. To indicate all traffic regardless of IP address and netmask, enter `0.0.0.0 0.0.0.0`.	`0.0.0.0 0.0.0.0`
`gateway <gateway_ipv4>`	IP address of the gateway router.	`0.0.0.0`
`set interface <interface name>`	Network interface associated with this route.	

config system time manual

Use this command to manually configure the FortiAI system time.

Accurate system time is required by many features such as log messages and SSL-secured connections.

This command applies only if NTP is disabled. Alternatively, you can configure FortiAI to synchronize its system time with an NTP server.

Syntax

```
config system time manual
    set daylight-saving-time {disable | enable}
    set zone <zone_int>
end
```

Variable	Description	Default
`daylight-saving-time {disable | enable}`	Enable to automatically adjust the system time for daylight-saving time (DST).	`enable`
`zone <zone_int>`	The number which indicates the time zone where the FortiAI unit is located.	

config system time ntp

Use this command to configure FortiAI to synchronize its system time with a network time protocol (NTP) server.

Accurate system time is required by many features of FortiAI such as log messages and SSL-secured connections.

Syntax

```
config system time ntp
    set ntpserver {<address_ipv4> | <fqdn_str>}
    set ntpsync {enable | disable}
    set syncinterval <interval_int>
end
```

Variable	Description	Default
ntpserver {<address_ipv4> | <fqdn_str>}	IP address or FQDN of an NTP server. You can add a maximum of ten NTP servers. FortiAI uses the first NTP server based on the selection mechanism of the NTP protocol. To locate a public NTP server, visit http://www.ntp.org/.	pool.ntp.org
ntpsync {enable | disable}	Enable to synchronize FortiAI with an NTP server instead of manually configuring the system time.	enable
syncinterval <interval_int>	The interval in minutes between synchronizations of the system time with the NTP server. The valid range is 1 to 1440.	

Get commands

get profile ldap

Use this command to get the details of LDAP authentication setting.

Syntax

```
get profile ldap <ldap profile name>
```

get profile authentication radius

Use this command to get the details of RADIUS authentication setting.

Syntax

```
get profile authentication radius <RADIUS auth server name>
```

get system accprofile

Use this command to get the number of accprofile of the current system.

Syntax

```
get system accprofile
```

get system admin

Use this command to get information about FortiAI administrator accounts.

By default, FortiAI has a single administrator account: admin.

For more information about the attributes, see config system admin on page 12.

Syntax

```
get system admin <userName>
```

Example

When user name is not presented:

```
== [ admin ]
status: enable     trusted-hosts: 0.0.0.0/0 ::/0     auth-strategy: local
     access-profile: SuperAdminProfile     user-profile:
```

When user name is presented:

```
username            : admin
name                :
wildcard            : disable
status              : enable
trusted-hosts       : 0.0.0.0/0 ::/0
auth-strategy       : local
msg-methods         :
password            : *
radius-permission-check: disable
radius-vendor-id    : 0
radius-subtype-id   : 0
access-profile      : SuperAdminProfile
user-profile        :
theme               : Green
sshkey              :
assist-user         :
assist-password     : *
assist-access       : alexa ifttt
```

get system admin-list

Use this command to get the list of users that has accessed this server.

Syntax

```
get system admin-list
```

Example

```
[0] login-name: adminror at 'admin-list'. (-284)
access-profile: SuperAdminProfile
login-method: CONSOLEmin-list
login-time: Thu Nov 21 11:12:17 2019
timeout-time: Thu Nov 21 11:57:17 2019
process-ID: 10217
client-address:
```

get system appearance

Syntax

```
get system appearance
```

Example

```
Last Update Time    : 2019-11-20 17:34:10
```

get system automation-settings

Syntax

```
get system automation-settings <profile-name>
```

Example

When profile name is not presented:

```
 name    Automation settings name
 fgt1
```

When a specified profile name is presented

```
name              : fgt1
vdom              : root
api-key           : *
webhook-config    : "{\"action\" : 1,\"webhook_exec\" : \"ip_blocker\", \"webhook_undo\" :
\"ip_unblocker\"}"
ip                : 172.19.235.251
port              : 443
enabled           : enable
source            : fabric-device
```

get system dhcp server

Syntax

```
get system dhcp server
```

get system dns

Syntax

```
get system dns
```

Example

```
Last Update Time             : 2019-11-20 18:12:41
primary                      : 208.91.112.53
secondary                    : 208.91.112.52
private-ip-query             : disable
cache                        : enable
truncate-handling            : tcp-retry
protected-domain-dns-state   : disable
protected-domain-dns-servers:
cache-min-ttl                : 300
```

get system enforcement-settings

Syntax

```
get system enforcement-settings
```

Example

```
Last Update Time     : 2020-07-31 10:00:00
allowlist            : 192.16.1.222/32
risk-level           : 4
conf-level           : 0.800000
```

get system interface

Syntax

```
get system interface <interface-name>
```

Example

When interface name is not presented:

```
== [ port1 ] (2019-11-05 05:22:30)
type: physical    redundant-master: 0    ip: 172.19.122.250/24    ip6: ::/0    status: up
     allowaccess: https ping ssh     discover: enable
```

When a specific interface name is presented:

```
name                 : port1
type                 : physical
mode                 : static
redundant-master     :
ip                   : 172.19.122.250/24
ip6                  : ::/0
mtu                  : 1500
speed                : auto
status               : up
mac-addr             : 00:0c:29:09:5a:55
```

```
allowaccess         : https ping ssh
discover            : enable
```

get system performance

Syntax

```
get system performance
```

Example

```
CPU usage:     0% used, 100% idle
Memory usage: 60% used
System Load:   18
Uptime:        1 days  21 hours  14 minutes
```

get system raid-status

Get information about RAID.

Syntax

```
get system raid-status
```

get system raid-status-detail

Get information about RAID including the available commands and detailed information of virtual and physical disks.

Syntax

```
get system raid-status-detail
```

get system route

Syntax

```
get system route <route number>
```

Example

Without specifying a route number:

```
== [ 1 ] (2019-11-21 09:45:24)
     destination: 0.0.0.0/0    gateway: 172.19.122.1    interface: port1
```

With specifying a route number:

```
<No.>               : 1
destination         : 0.0.0.0/0
gateway             : 172.19.122.1
interface           : port1
```

get system status

Syntax

```
get system status
```

Example

```
Version:            FortiAI-3500F v1.30,build46,200605 (1.30.0 Beta) (Debug)
Architecture:       64-bit
Serial-Number:      FAI35FT000000000
BIOS version:       00010002
Log disk:           Capacity 43 MB, Used 1 MB (2.57%), Free 42 MB
Data disk:          Capacity 3517 GB, Used 117 GB (3.35%), Free 3399 GB
Remote disk:        n/a
Hostname:           FAI35FT319000030
Strong-crypto:      disabled
Distribution:       International
Branch point:       1
Uptime:             0 days  21 hours  9 minutes
Last reboot:        Fri Jun 05 14:45:12 PDT 2020
System time:        Sat Jun 06 11:54:35 PDT 2020
```

get system time manual

Syntax

```
get system time manual
```

Example

```
Last Update Time    :
daylight-saving-time: enable
zone                : 4
```

get system time ntp

Syntax

```
get system time ntp
```

Example

```
Last Update Time    :
ntpsync             : enable
ntpserver           : ntp1.fortiguard.com ntp2.fortiguard.com
syncinterval        : 60
```

Show and show full-configuration commands

Show commands display the FortiAI configuration that is changed from the default setting. Unlike get commands, show commands do not display settings that remain in their default state.

For example, you might show the current DNS settings:

```
show system dns
   config system dns
      set primary 172.16.1.10
   end
```

If the command does not display the secondary DNS server settings, that indicates that it has not been configured or has reverted to its default value.

Show full-configuration commands display the full configuration including default settings. While similar to get commands, show full-configuration output uses configuration file syntax.

For example, you might show the current DNS settings, including settings that remain at their default values (in bold below):

```
show full-configuration system dns
   config system dns
      set primary 172.16.1.10
      set secondary 172.16.1.11
      set private-ip-query disable
      set cache enable
   end
```

Depending on whether you specify an object, the show command displays either the configuration that you have just entered but not yet saved or the configuration as it currently exists on disk.

For example, immediately after configuring the secondary DNS server setting but before saving it, show displays two outputs (differences in bold):

```
config system dns
   set secondary 192.168.1.10
   show
      config system dns
      set primary 172.16.1.10
      set secondary 192.168.1.10
   end
   show system dns
      config system dns
      set primary 172.16.1.10
   end
```

The first output indicates the value that you have configured but not yet saved; the second output indicates the value that was last saved to disk.

If you have entered settings but cannot remember how they differ from the existing configuration, the two different forms of show, with and without the object name, can be a useful reminder.

Diagnose commands

diagnose hardware

Use this command to display FortiAI device status and information, read data from an I/O port, list information on PCI buses and connected devices, set PCI configuration space data, and list system hardware information.

Syntax

```
diagnose hardware deviceinfo {nic | nic-detail}
diagnose hardware ioport {byte | word | long} <correspond_data>
diagnose hardware pciconfig {bus| id | option} <correspond data>
diagnose hardware setpci pciconfig <device> <register> <data> option <option>
diagnose hardware sysinfo {cpu | interrupts | iomem | ioports | memory | mtrr | slab |
      stream | df}
```

Variable	Description	Default
`deviceinfo {nic	nic-detail}`	Diagnose the list device status and information.	
`ioport {byte	word	long} <correspond_data>`	Diagnose the process of reading data from an I/O port.	
`pciconfig {bus	id	option} <correspond data>`	Diagnose the list information on PCI buses and connected devices.	
`setpci pciconfig <device> <register> <data> option <option>`	Diagnose the process of setting PCI configuration space data.	`ios`
`sysinfo {cpu	interrupts	iomem	ioports	memory	mtrr	slab	stream	df}`	Diagnose the list system hardware information.	

diagnose kdb

Use this command to diagnose ANN DB (KDB) and display version.

Syntax

```
diagnose kdb
```

diagnose sniffer dump

Use this comand to dump the data flow records of the network port to a specific TFTP server.

Ensure the remote TFTP files are created.

Syntax

```
diagnose sniffer dump <tftp IP>  <local sniffer file name> <remote tftp server file name>
```

diagnose sniffer file

Use this command to manage the tcpdump recorded by the `sniffer packet` command.

Syntax

```
diagnose sniffer file {display|clear}
```

diagnose sniffer packet

Use this comand to diagnose the sniffer database by dumping and checking data flow records of the network port.

Ensure the remote TFTP files are created.

Syntax

```
diagnose sniffer packet <interface>  <filter> <verbose> <count> <time format> <file name>
     <ttl> {background|NULL}
diagnose sniffer packet {stop|status}
```

Variable	Description	Default
`interface | 'stop' | 'status'`	If an interface is specified, the tcpdump starts a process recording the data flow of that port. Use `stop` to stop a process that is working in the background. Use `status` to check the files that have been generated so far.	`any`
`filter`	For example, to print UDP 1812 traffic between `forti1` and either `forti2` or `forti3`, use `udp and port 1812 and host forti1 and \( forti2 or forti3 \).`	`none`
`verbose`	Set the verbosity of the record. The options are: `1`: Print header of packets. `2`: Print header and data from the IP address of packets.	`1`

Variable	Description	Default
	3: Print header and data from the Ethernet of packets (if available). 4: Print header of packets with interface name. 5: Print header and data from IP address of packets with interface name. 6: Print header and data from Ethernet of packets (if available) with INTF name.	
count	Maximum number of packets to be recorded in this attempt.	-1
time format	Time format of the record. The options are: a: Absolute UTC time in yyyy-mm-dd hh:mm:ss.ms format. relative: Relative to the start of sniffing in ss.ms format.	relative
file name	File name of the record for this recording attempt.	
ttl	Maximum time allowed for this record attempt to run (in minutes).	
{background}	Optional variable to specify if this recording attempt executes in the backend or displays on the console.	NULL

diagnose session list

Use this command to diagnose the active session lists.

Syntax

```
diagnose session list
```

Example

```
System Time:  2019-11-21 13:51:48 PST (Uptime: 1d 22h 36m)
Protocol  Remote IP Remote     Port     Local IP    Local Port   Expire(s)
tcp        72.19.122.220       57575  172.19.122.250    5432       22
tcp        172.19.122.220      52413  172.19.122.250     22        320
```

diagnose system disk info

Disk hardware status information.

Syntax

```
diagnose system disk info
```

Example

```
System Time:  2020-06-06 11:57:01 PDT (Uptime: 0d 21h 11m)
Disk 0:
Device Model:     SSDSC2KB038T8R
Serial Number:    PHYF915502NZ3P8EGN
LU WWN Device Id: 5 5cd2e4 150d5a715
Add. Product Id:  DELL(tm)
Firmware Version: XCV1DL63
User Capacity:    3,840,755,982,336 bytes [3.84 TB]
Sector Sizes:     512 bytes logical, 4096 bytes physical
Rotation Rate:    Solid State Device
Form Factor:      2.5 inches
Device is:        Not in smartctl database [for details use: -P showall]
ATA Version is:   ACS-3 (unknown minor revision code: 0x006d)
SATA Version is:  SATA >3.1, 6.0 Gb/s (current: 6.0 Gb/s)
Local Time is:    Sat Jun  6 11:57:01 2020 PDT
SMART support is: Available - device has SMART capability.
SMART support is: Enabled

Disk 1:
Device Model:     SSDSC2KB038T8R
Serial Number:    PHYF915502R93P8EGN
LU WWN Device Id: 5 5cd2e4 150d5a75d
Add. Product Id:  DELL(tm)
Firmware Version: XCV1DL63
User Capacity:    3,840,755,982,336 bytes [3.84 TB]
Sector Sizes:     512 bytes logical, 4096 bytes physical
Rotation Rate:    Solid State Device
Form Factor:      2.5 inches
Device is:        Not in smartctl database [for details use: -P showall]
ATA Version is:   ACS-3 (unknown minor revision code: 0x006d)
SATA Version is:  SATA >3.1, 6.0 Gb/s (current: 6.0 Gb/s)
Local Time is:    Sat Jun  6 11:57:01 2020 PDT
SMART support is: Available - device has SMART capability.
SMART support is: Enabled
```

diagnose system disk summary

Summary of smartctl details.

Syntax

```
diagnose system disk summary
```

Example

```
System Time:  2020-06-06 11:58:52 PDT (Uptime: 0d 21h 13m)
Smartctl Results
             Overall       Realloc Pending Seek
Device       Health        Sectors Sectors Count   Last Run Test
--------------------------------------------------------------------------
```

```
/dev/sda     PASSED        0       0       0       extended,completed without error
/dev/sda     PASSED        0       0       0       extended,completed without error
/dev/sdb     NOT-SUPPORTED
```

diagnose system disk health

Health information of this disk.

Syntax

```
diagnose system disk health
```

Example

```
System Time:  2019-11-21 18:24:26 GMT (Uptime: 0d 0h 0m)
smartctl 6.3 2014-07-26 r3976 [x86_64-linux-4.9.60-3500F] (local build)
Copyright (C) 2002-14, Bruce Allen, Christian Franke, www.smartmontools.org

/dev/sda [megaraid_disk_00] [SAT]: Device open changed type from 'megaraid,0' to 'sat+-
megaraid,0'
=== START OF READ SMART DATA SECTION ===
SMART Status not supported: ATA return descriptor not supported by controller firmware
SMART overall-health self-assessment test result: PASSED
Warning: This result is based on an Attribute check.

smartctl 6.3 2014-07-26 r3976 [x86_64-linux-4.9.60-3500F] (local build)
Copyright (C) 2002-14, Bruce Allen, Christian Franke, www.smartmontools.org

/dev/sda [megaraid_disk_01] [SAT]: Device open changed type from 'megaraid,1' to 'sat+-
megaraid,1'
=== START OF READ SMART DATA SECTION ===
SMART Status not supported: ATA return descriptor not supported by controller firmware
SMART overall-health self-assessment test result: PASSED
Warning: This result is based on an Attribute check.

smartctl 6.3 2014-07-26 r3976 [x86_64-linux-4.9.60-3500F] (local build)
Copyright (C) 2002-14, Bruce Allen, Christian Franke, www.smartmontools.org

/dev/sdb: Unknown USB bridge [0x196d:0x0201 (0x1120)]
Please specify device type with the -d option.

Use smartctl -h to get a usage summary
```

diagnose system disk attributes

Information about the attributes of this disk.

Syntax

```
diagnose system disk attributes
```

Example

```
diagnose system disk attributes

System Time:  2019-11-21 17:59:00 GMT (Uptime: 0d 0h 1m)
smartctl 6.3 2014-07-26 r3976 [x86_64-linux-4.9.60-3500F] (local build)
Copyright (C) 2002-14, Bruce Allen, Christian Franke, www.smartmontools.org

/dev/sda [megaraid_disk_00] [SAT]: Device open changed type from 'megaraid,0' to 'sat+-
megaraid,0'

=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 1
Vendor Specific SMART Attributes with Thresholds:
ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_
VALUE

  1 Raw_Read_Error_Rate     0x000e   130   130   039    Old_age   Always       -
15079102
  5 Reallocated_Sector_Ct   0x0033   100   100   001    Pre-fail  Always       -       0
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       5
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -       24
 13 Read_Soft_Error_Rate    0x001e   083   080   000    Old_age   Always       -
1095231739582
170 Unknown_Attribute       0x0033   100   100   010    Pre-fail  Always       -       0
174 Unknown_Attribute       0x0032   100   100   000    Old_age   Always       -       24
179 Used_Rsvd_Blk_Cnt_Tot   0x0033   100   100   010    Pre-fail  Always       -       0
180 Unused_Rsvd_Blk_Cnt_Tot 0x0032   100   100   000    Old_age   Always       -       25540
181 Program_Fail_Cnt_Total  0x003a   100   100   000    Old_age   Always       -       0
182 Erase_Fail_Count_Total  0x003a   100   100   000    Old_age   Always       -       0
184 End-to-End_Error        0x0032   100   100   000    Old_age   Always       -       0
194 Temperature_Celsius     0x0022   100   100   000    Old_age   Always       -       18
195 Hardware_ECC_Recovered  0x0032   100   100   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   100   100   000    Old_age   Always       -       0
201 Unknown_SSD_Attribute   0x0033   100   100   010    Pre-fail  Always       -
     120275667391
202 Unknown_SSD_Attribute   0x0027   100   100   000    Pre-fail  Always       -       0
225 Unknown_SSD_Attribute   0x0032   100   100   000    Old_age   Always       -       15898
226 Unknown_SSD_Attribute   0x0032   100   100   000    Old_age   Always       -       0
227 Unknown_SSD_Attribute   0x0032   100   100   000    Old_age   Always       -       99
228 Power-off_Retract_Count 0x0032   100   100   000    Old_age   Always       -       77
232 Available_Reservd_Space 0x0033   100   100   010    Pre-fail  Always       -       0
233 Media_Wearout_Indicator 0x0032   100   100   000    Old_age   Always       -       15898
234 Unknown_Attribute       0x0032   100   100   000    Old_age   Always       -       0
241 Total_LBAs_Written      0x0032   100   100   000    Old_age   Always       -       15898
242 Total_LBAs_Read         0x0032   100   100   000    Old_age   Always       -       132126
245 Unknown_Attribute       0x0032   100   100   000    Old_age   Always       -       100

smartctl 6.3 2014-07-26 r3976 [x86_64-linux-4.9.60-3500F] (local build)
Copyright (C) 2002-14, Bruce Allen, Christian Franke, www.smartmontools.org

/dev/sda [megaraid_disk_01] [SAT]: Device open changed type from 'megaraid,1' to 'sat+-
megaraid,1'
```

```
=== START OF READ SMART DATA SECTION ===
SMART Attributes Data Structure revision number: 1
Vendor Specific SMART Attributes with Thresholds:

ID# ATTRIBUTE_NAME          FLAG     VALUE WORST THRESH TYPE      UPDATED  WHEN_FAILED RAW_
VALUE
  1 Raw_Read_Error_Rate     0x000e   130   130   039    Old_age   Always       -
11512623
  5 Reallocated_Sector_Ct   0x0033   100   100   001    Pre-fail  Always       -       0
  9 Power_On_Hours          0x0032   100   100   000    Old_age   Always       -       5
 12 Power_Cycle_Count       0x0032   100   100   000    Old_age   Always       -       24
 13 Read_Soft_Error_Rate    0x001e   079   077   000    Old_age   Always       -
2332178754351
170 Unknown_Attribute       0x0033   100   100   010    Pre-fail  Always       -       0
174 Unknown_Attribute       0x0032   100   100   000    Old_age   Always       -       24
179 Used_Rsvd_Blk_Cnt_Tot   0x0033   100   100   010    Pre-fail  Always       -       0
180 Unused_Rsvd_Blk_Cnt_Tot 0x0032   100   100   000    Old_age   Always       -       25538
181 Program_Fail_Cnt_Total  0x003a   100   100   000    Old_age   Always       -       0
182 Erase_Fail_Count_Total  0x003a   100   100   000    Old_age   Always       -       0
184 End-to-End_Error        0x0032   100   100   000    Old_age   Always       -       0
194 Temperature_Celsius     0x0022   100   100   000    Old_age   Always       -       18
195 Hardware_ECC_Recovered  0x0032   100   100   000    Old_age   Always       -       0
197 Current_Pending_Sector  0x0012   100   100   000    Old_age   Always       -       0
198 Offline_Uncorrectable   0x0010   100   100   000    Old_age   Offline      -       0
199 UDMA_CRC_Error_Count    0x003e   100   100   000    Old_age   Always       -       0
201 Unknown_SSD_Attribute   0x0033   100   100   010    Pre-fail  Always       -
120275601610
202 Unknown_SSD_Attribute   0x0027   100   100   000    Pre-fail  Always       -       0
225 Unknown_SSD_Attribute   0x0032   100   100   000    Old_age   Always       -       15931
226 Unknown_SSD_Attribute   0x0032   100   100   000    Old_age   Always       -       0
227 Unknown_SSD_Attribute   0x0032   100   100   000    Old_age   Always       -       100
228 Power-off_Retract_Count 0x0032   100   100   000    Old_age   Always       -       77
232 Available_Reservd_Space 0x0033   100   100   010    Pre-fail  Always       -       0
233 Media_Wearout_Indicator 0x0032   100   100   000    Old_age   Always       -       15931
234 Unknown_Attribute       0x0032   100   100   000    Old_age   Always       -       0
241 Total_LBAs_Written      0x0032   100   100   000    Old_age   Always       -       15931
242 Total_LBAs_Read         0x0032   100   100   000    Old_age   Always       -       132056
245 Unknown_Attribute       0x0032   100   100   000    Old_age   Always       -       100

smartctl 6.3 2014-07-26 r3976 [x86_64-linux-4.9.60-3500F] (local build)
Copyright (C) 2002-14, Bruce Allen, Christian Franke, www.smartmontools.org

/dev/sdb: Unknown USB bridge [0x196d:0x0201 (0x1120)]

Please specify device type with the -d option.
Use smartctl -h to get a usage summary
```

diagnose system disk-details

Syntax

```
diagnose system disk-details
```

Example

```
System Time:  2019-11-21 14:01:55 PST (Uptime: 1d 22h 47m)
for type for-var-physical
+device-name=sdb
|   is-enc=0
|   is-dma=1
|   is-usb=0
|     size=26843545600   (opt=0,min=512,alg=0,phy=512,log=512,grn=1048576)
+-----part-name=sdb1
|             size=26835157504
|             start=1048576(aligned)
|       is-mounted=0
|          fs-type=LVM2
```

diagnose system ntp-status

Use this command to print the NTP sync status.

Syntax

```
diagnose system ntp-status
```

Example

```
System Time:  2019-11-21 14:03:11 PST (Uptime: 1d 22h 48m)
remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
*LOCAL(0)        .LOCL.          10 l   20   64  377    0.000    0.000   0.000
208.91.113.70    172.16.101.30    2 u  259 1024    0    0.913    0.005   0.000
208.91.114.23    .FTNT.           1 u   6h 1024    0    1.335    0.404   0.000
```

diagnose system top

Use this command to display:

- Up time (run time).
- Current total processor and memory usage.
- Current free memory.
- The most resource-intensive system processes and daemons showing their memory (RAM) and processor (CPU) usage.

The first two lines of the display indicate the up time, and the processor and memory usage. Processor and memory usages on the second line have abbreviated labels shown below in bold.

Run Time: 0 days, 21 hours and 3 minutes

0**U**, 4**S**, 95**I**; 1035792**T**, 646920**F**

Letter	Description
U	User CPU usage (%)
S	System CPU usage (%)
I	Idle CPU usage (%)
T	Total memory (KB)
F	Free memory (KB)

The remaining lines contain the process list, which has the following columns:

Column 1 is the process name, such as SSHD.

Column 2 is the process ID (PID) number, such as 731.

Column 3 is the status:

- S: Sleeping (idle)
- R: Running
- Z: Zombie (crashed)
  You might be able to restart a zombie process without rebooting. See execute reload on page 55.
- <: High priority
- N: Low priority

Column 4 is CPU usage (%).

Column 5 is memory usage (%).

When the command is running, you can sort the process list. The default sort order is by CPU usage.

- Shift + P: Sort by CPU usage.
- Shift + M: Sort by memory usage.

Process list output displays in your CLI window until you stop it by pressing *q* or *Ctrl* + *C*.

Syntax

```
diagnose system top <refresh_int>
```

Variable	Description	Default
`<refresh_int>`	The interval between each refresh of the process list in seconds. For example, to refresh the process list every 5 seconds, type 5.	

Example

This example refreshes the display of the top 19 most system-intensive processes every five seconds. The output indicates that FortiAI is mostly idle except for some processor resources used by a connection to the web UI (`admin.fe`) and to the CLI.

```
diagnose system top 5
Run Time: 0 days, 21 hours and 3 minutes
0U, 4S, 95I; 1035792T, 646920F
admin.fe 987 S 6.0 0.0
admin.fe 979 S 1.4 0.0
cli 984 R 0.2 0.0
miglogd 755 S 0.2 0.0
dbmanager 731 S 0.0 0.0
mailfilter 767 S 0.0 0.0
httpd 972 S 0.0 0.0
smtpd 793 S 0.0 0.0
smtpd 796 S 0.0 0.0
dbdaemon 766 S 0.0 0.0
smtpd 829 S 0.0 0.0
smtpd 830 S 0.0 0.0
smtpd 831 S 0.0 0.0
smtpd 828 S 0.0 0.0
smtpproxy 780 S 0.0 0.0
spamreport 790 S 0.0 0.0
fmlmonitor 799 S 0.0 0.0
cmdbsvr 745 S 0.0 0.0
netd 756 S 0.0 0.0
```

Execute commands

execute date

Use this command to set the system date.

Syntax

```
execute date <date_str>
```

Variable	Description	Default
`<date_str>`	The system date in mm/dd/yyyy format.	

execute demo

Use this command to enable or disable demo mode.

Syntax

```
execute demo {on|off}
```

execute expandspooldisk

Use this command to expand `/var/spool` disk without losing pre-existing data; This disk is mainly used for storing training data and detection history.

Syntax

```
execute expandspooldisk
```

execute export

Use this command to export the FortiAI detection history as a .csv file.

Syntax

```
execute export file-report {disk|scp|ftp|tftp} <filenmame-to-be-saved> <server>[:ftp port]
     <user-name> <password>
```

execute export db-files

Use this command to export the detected file report in raw format.

Syntax

```
execute export db-files {disk|scp|ftp|tftp} <filenmame-to-be-saved> <server>[:ftp port] <user-
     name> <password>
```

CSV columns

Column name	Description
fileid	The UUID of this file in FortiAI.
filesize	The size of this file.
ftypeid	The UUID of the filetype of this file in FortiAI.
entrydate	The time this file get recorded in FortiAI.
sip	The source IP address.
sport	The source port.
dip	The destination IP address.
dport	The destination port.
mal_bit	Whether the file contains malware. 0 means clean.
conf	A number (0,1) which indicates the confidence of detection.
vname	The virus name.
pbit	The bit to indicate whether this file has been processed by FortiAI engine.
md5	The MD5 hash of this file.
sha512	The SHA512 hash of this file.
url	The URL of this file.
tfc	Feature count.
tmfc	Malicious feature count.
tptime	Processing time.
findate	The time that this file is processed by FortiAI.
det_type_id	The ID of malware detected in this file.
det_sub_type_id	The sub-ID of malware detected in this file.
tlmfc	Malicious feature learned.
tlcfc	Clean feature learned.

Column name	Description
det_type_id_grp	TA JSON object consist of multiple pairs of {DET_TYPE_ID:COUNT}.
det_sub_type_id_grp	A JSON object consist of multiple pairs of {DET_SUB_TYPE_ID:COUNT}.
isfgt	The host that contains this file.
eng_ver	The version of engine that process this file.
kdb_ver	The version of kdb that process this file.
ioc_list	A JSON object consisting of multiple pairs of {IOC_TYPE_ID:COUNT}.

Filetype ID map

ID	Filetype
1	PE
2	PDF
3	MSOFFICE
4	DEX
5	HTML
6	ELF
7	VBS
8	VBA
9	JS

Detection type map

ID	Detection type
1	Downloader
2	Redirector
3	Dropper
4	Ransomware
5	Worm
6	PWS
7	Rootkit
8	Banking Trojan
9	Infostealer

ID	Detection type
10	Exploit
11	Clicker
12	Virus
13	Application
14	Multi
15	CoinMiner
16	DoS
17	BackDoor
18	WebShell
19	SEP
20	Proxy
21	Trojan
22	Phishing
23	Fileless
24	Wiper
25	Industroyer

IOC type map

ID	Description
1	Contains either script statements or link to an external script file through other attributes.
2	Contains a form made up of different types of input elements such as text fields, checkboxes, buttons, and usually a link the form data is sent to.
3	Contains a inline frame element.
4	Contains a defined window within a frameset in HTML4.
5	Contains an incomplete iframe definition.
6	Contains an URL attribute.
7	Contains an href attribute.
8	Contains hex encoded content.
9	Contains a function that converts a Unicode number into a character.
10	Contains a function that converts a Unicode number into a character twice.
11	Contains JavaScript code snippets which attempts to decode an encoded string.

ID	Description
12	Contains a src attribute.
13	Contains URI.
14	Contains JavaScripts.
15	Contains multiple streams.
16	Contains a hex encoded text in a stream.
17	Contains VBA scirpts in the office file.
18	Contains base64 encoded text.
19	Contains VBA scirpts in the office file.
20	Contains URLs in the office file.
21	Contains VBA scirpts in the office file.
22	Contains VBA scirpts in the office file.
23	Contains abnormal commands in the VBA script.
24	Contains a PE file in the office file.
25	Contains abnormal commands in the office OLE stream.
26	Contains abnormal commands in the VBA script.
27	Contains abnormal commands in the VBA script.
28	Contains two layers of base64 encoding.
29	Contains a compressed data encoded with base64.
30	Contains URLs in a compressed base64 encoded content.
31	Contains URLs in the VBA script.
32	Contains URLs in the context that is decoded by a function which converts a Unicode number into a character twice.
33	Contains abnormal commands.
34	Contains abnormal URLs in an href attribute.
35	Contains URLs in the action attribute of a form.
36	Contains abnormal URLs in the action attribute of a form.
37	Contains URLs in the URL attribute.
38	Contains abnormal URLs in the URL attribute.
39	Contains the packed content.
40	Contains abnormal style elements in the context that is decoded by a function which converts a Unicode number into a character.

ID	Description
41	Contains URLs in a hex encoded content.
42	Contains abnormal URLs in a hex encoded content.
43	Contains URLs in the packed content.
44	Contains abnormal URLs in the packed content.
45	Contains abnormal URLs in the context that is decoded by a function which converts a Unicode number into a character twice.
46	Contains URLs.
47	Contains abnormal URLs.
48	Contains abnormal commands in the VBA script.
49	Contains abnormal URLs in a src attribute.
50	Contains URLs in the VBA script.
51	Contains URIs in a compressed stream.
52	Contains URLs in a compressed stream.
53	Contains abnormal URLs in a compressed stream.
54	Contains URLs in the context that is decoded by a function which converts a Unicode number into a character.
55	Contains abnormal URLs in the context that is decoded by a function which converts a Unicode number into a character.
56	Contains URLs in the script.
57	Contains abnormal URLs in the script.
58	Contains VBA encoding.
59	Contains URLs in the VBA encoding.
60	Contains abnormal URLs in the VBA encoding.
61	Contains abnormal commands in the VBA encoding.
62	Contains abnormal commands in URL encoding.
63	Contains the BlackHole Exploit Kit.
64	Contains URLs in the XML content.
65	Contains abnormal URLs in the XML content.
66	Contains abnormal commands in the context that is decoded by a function which converts a Unicode number into a character.
67	Contains URL encoding.
68	Contains abnormal URL encoding.

ID	Description
69	Contains URLs in the base64 encoded content.
70	Contains abnormal URLs in a base64 encoded content.
71	Contains abnormal URLs in the VBA script.
72	Contains URLs in the file content.
73	Contains abnormal URLs in the file content.
74	Contains abnormal URLs in the VBA script.
75	Contains abnormal commands in the VBA script.
76	Contains escaped Unicode.
77	Contains abnormal URLs in the office file.
78	Contains URLs in a inline frame element.
79	Contains abnormal URLs in a inline frame element.
80	Contains URLs in a defined window within a frameset.
81	Contains abnormal URLs in a defined window within a frameset.
82	Contains URLs in an incomplete iframe definition.
83	Contains abnormal URLs in an incomplete iframe definition.
84	Contains phishing content.
85	Contains context that encrypted with RC4.
86	Contains URLs in the RC4 context.
87	Contains abnormal URLs in the RC4 encrypted content.
88	Contains the context that has reversed order.
89	Contains URLs in a reversed content.
90	Contains abnormal URLs in a reversed content.
91	Contains QakBot characteristics.
92	Contains QakBot executable download URLs.
93	Contains QakBot executable download URLs.
94	Contains a PE file.
95	Contains a PE file in the office file.
96	Contains a PE file in a base64 encoded content.
97	Contains abnormal URLs in a compressed base64 encoded content.
98	Contains a packed content.

ID	Description
99	Contains abnormal codes in a compressed stream.
100	Contains a hidden iframe.

execute export detected-files

Use this command to export the detected files by FortiAI as a zip file with password. The password of the zip file is *infected*.

Syntax

```
execute export detected-files {disk|scp|ftp|tftp} <filenmame-to-be-saved> <server>[:ftp port]
     <user-name> <password>
```

execute api-key

Use this command to generate API key for a system user.

Syntax

```
execute api-key <system-user-name>
```

execute db restore

Use this command to restore the database.

Syntax

```
execute db restore
```

execute db sample_process_summary

Use this command to get the processing status of FortiAI within a specific time period.

Syntax

```
execute db sample_process_summary <from_date> <to_date>
```

Example of results

```
Sample accepted                :192
Distinct sample accepted       :88
Sample processed               :192
Distinct sample accepted       :88
Sample detected                :192
infected host count            :1
distinct infected remote IP    :10
distinct infected host IP      :5
```

execute factoryreset config

Use this command to reset the configuration only.

Back up your configuration before using this command. This command makes major changes to your configuration. If you are downgrading the firmware, this procedure resets all changes you have made to the FortiAI configuration file and reverts the system to the default values for that firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiAI Administration Guide in the Fortinet Document Library.

Syntax

```
execute factoryreset config
```

execute factoryreset disk

Use this command to reset the RAID level and partition the disk to default settings. This command does not reset the configuration such as IP configuration.

Back up all data on the disks before using this command. This command deletes all files on the disk.

Syntax

```
execute factoryreset disk
```

execute factoryreset

Use this command to reset FortiAI to its default settings for the currently installed firmware version. If you have not upgraded or downgraded the firmware, this restores factory default settings.

Back up your configuration before using this command. This procedure resets all changes you have made to the FortiAI configuration file and reverts the system to the default values for the firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiAI Administration Guide in the Fortinet Document Library.

Syntax

```
execute factoryreset
```

Example

```
execute factoryreset
```

The CLI displays the following:

```
This operation will change all settings to
factory default! Do you want to continue? (y/n)
```

If you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
System is resetting to factory default...
```

execute formatdatadisk

Use this command to format the local hard disk that contains training data as well as detection history.

Format the disk regularly to improve performance.

Syntax

```
execute formatdatadisk
```

execute formatlogdisk

Use this command to reformat the local hard disk that contains log data. This command also reboots the unit.

Format the disk regularly to improve performance.

Back up all data on the disks before using this command. This command deletes all files on the disk.

Syntax

```
execute formatlogdisk
```

Example

```
execute formatlogdisk
```

The CLI displays the following:

```
This operation will erase all data on the log disk!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following and logs you out of the CLI:

```
Formatting disk, Please wait a few seconds!
```

execute partitiondisk

Use this command to adjust the size ratio of the hard disk partitions for log and training data.

⚠ Back up all data on the disks before using this command. This command deletes all files on the disk.

Syntax

```
execute partitiondisk <percentage_str>
```

Variable	Description	Default
`partitiondisk <percentage_str>`	Enter an integer between 1 and 95 to create a partition of that percentage of the total hard disk space for the log disk. The remaining space is for the data disk.	5

execute ping

Use this command to perform an ICMP ECHO request (a ping) to a host by specifying its FQDN or IP address.

Syntax

```
execute ping {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
`ping {<fqdn_str> | <host_ipv4>}`	IP address or FQDN of the host.	

Example 1

```
execute ping 172.16.1.10
```

The CLI displays the following:

```
PING 172.16.1.10 (172.16.1.10): 56 data bytes
64 bytes from 172.16.1.10: icmp_seq=0 ttl=128 time=0.5 ms
64 bytes from 172.16.1.10: icmp_seq=1 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=2 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=3 ttl=128 time=0.2 ms
64 bytes from 172.16.1.10: icmp_seq=4 ttl=128 time=0.2 ms
--- 172.16.1.10 ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.2/0.2/0.5 ms
```

The results of the ping indicate that a route exists between FortiWeb and 172.16.1.10. It also indicates that during the sample period, there was no packet loss and the average response time was 0.2 milliseconds (ms).

Example 2

```
execute ping 10.0.0.1
```

The CLI displays the following:

```
PING 10.0.0.1 (10.0.0.1): 56 data bytes
```

After several seconds with no output, the administrator stops the ping by pressing *Ctrl* + *C*. The CLI displays the following:

```
--- 10.0.0.1 ping statistics ---
5 packets transmitted, 0 packets received, 100% packet loss
```

The results of the ping indicate that the host might be down or there is no route between FortiAI and 10.0.0.1.

execute raidlevel

Use this command to reset the RAID level and partition the disk.

Syntax

```
execute raidlevel <raid-level-option>
```

execute reboot

Use this command to restart FortiAI.

Syntax

```
execute reboot
```

Example

```
execute reboot
```

The CLI displays the following:

```
This operation will reboot the system !
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is rebooting...
```

If you are connected to the CLI through a local console, the CLI displays messages during the reboot.

If you are connected to the CLI through the network, the CLI does not display any notifications during the reboot since the connection is terminated.

execute reload

If you set your console to batch mode, use this command to flush the current configuration from system memory and reload the configuration from a previously saved configuration file.

You can also use this command to reload individual daemons that have crashed, in this syntax:

```
execute reload [{httpd | ...}]
```

where `[{httpd | ...}]` is the name of the daemon you want to restart.

For example, if HTTP and HTTPS access are enabled but you cannot get a connection response on the GUI, although you can still connect via SSH and ping. So you know that FortiAI has not crashed entirely. If you do not want to reboot as this would interrupt SMTP, you can try to restart the HTTP daemon only.

```
execute reload httpd
Restart httpd?
Do you want to continue? (y/n)y

Reloading httpd....done
```

This command does not check if the daemon actually exists. If the command does not execute in a few seconds, it is possible that the daemon might not exist.

Syntax

```
execute reload [<daemon_name>]
```

execute restore config

Use this command to restore a primary configuration file from a TFTP server.

Back up your configuration before using this command. This command makes major changes to your configuration. If you are downgrading the firmware, this procedure resets all changes you have made to the FortiAI configuration file and reverts the system to the default values for that firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiAI Administration Guide in the Fortinet Document Library.

Unlike installing firmware via TFTP during a boot interrupt, installing firmware using this command will attempt to preserve settings and files, and not necessarily restore the FortiAI unit to its firmware/factory default configuration. For information on installing firmware via TFTP boot interrupt, see the FortiAI Administration Guide.

Syntax

```
execute restore config {disk <filename> | ftp <file name> <server_ipv4> | scp <file name>
     <server_ipv4> | tftp  <file name> <server_ipv4>}
```

Variable	Description	Default
`<filename_str>`	Name of the configuration file you want to restore from the TFTP server.	
`<server_ipv4>`	IP address of the TFTP server where the configuration file is stored.	
`management-station {normal | template}`	If you want to restore a configuration file or apply a template stored in FortiManager, enter the management-station and then enter either: `normal`: Restore a configuration revision number. `template`: Apply a template revision number.	
`<revision_int>`	If you want to restore a configuration file or apply a template stored in FortiManager, enter the revision number of the configuration file or template.	

Example 1

This example restores configuration file revision 2 which is stored in FortiManager.

```
execute restore config management-station normal 2
```

The CLI displays the following:

```
This operation will overwrite the current settings!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
Connect to FortiManager ...
Please wait...
```

Example 2

This example restores a configuration file from a TFTP server at 172.16.1.5.

```
execute restore config tftp fml.cfg 172.16.1.5
```

The CLI displays the following:

```
This operation will overwrite the current settings!
(The current admin password will be preserved.)
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following, then terminates the SSH connection and reboots with the restored configuration:

```
Connect to tftp server 172.16.1.5 ...
Please wait...

Get config file from tftp server OK.
File check OK.
```

execute restore image

Use this command to restore a firmware file from a TFTP server or a FortiManager unit.

⚠ Back up your configuration before using this command. This command makes major changes to your configuration. If you are downgrading the firmware, this procedure resets all changes you have made to the FortiAI configuration file and reverts the system to the default values for that firmware version, including factory default settings for the IP addresses of network interfaces. For information on creating a backup, see the FortiAI Administration Guide in the Fortinet Document Library.

Syntax

```
execute restore image {disk <filename> | ftp <file name> <server_ipv4> | scp <file name>
     <server_ipv4> | tftp <file name> <server_ipv4>}
```

Variable	Description	Default
`<filename_str>`	Name of the firmware file on the TFTP server.	
`<server_ipv4>`	IP address of the TFTP server where the firmware file is stored.	

Example

This example restores firmware file FAI_3500F-v12-build0047-FORTINET.out, which is stored on the TFTP server 192.168.1.20.

```
execute restore image tftp FAI_3500F-v12-build0047-FORTINET.out 192.168.1.20
```

The CLI displays the following:

```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
Connect to tftp server 192.168.1.20 ...
Please wait...
########################
Get image from tftp server OK.
Check image OK.
execute restore image {disk <filename> | ftp <file name> <server_ipv4> | scp <file name>
     <server_ipv4> | tftp <file name> <server_ipv4>}
```

execute restore kdb

Use this command to restore, upgrade, or downgrade the FortiAI ANN database. This command replaces the existing ANN database.

Syntax

```
execute restore kdb {disk <filename> | ftp <file name> <server_ipv4> | scp <file name>
     <server_ipv4> | tftp <file name> <server_ipv4>}
```

Variable	Description	Default
`<filename_str>`	Name of the firmware file on the TFTP server.	
`<server_ipv4>`	IP address of the TFTP server where the firmware file is stored.	

execute shutdown

Use this command to prepare the FortiAI unit to be powered down by halting the software, clearing all buffers, and writing all cached data to disk.

Power off the FortiAI unit only after issuing this command. Unplugging or switching off the FortiAI unit without issuing this command could result in data loss.

Syntax

```
execute shutdown
```

Example

```
execute shutdown
```

The CLI displays the following:

```
This operation will halt the system
(power-cycle needed to restart)!Do you want to continue? (y/n)
```

After you enter `y` (yes), the CLI displays the following:

```
System is shutting down...(power-cycle needed to restart)
```

If you are connected to the CLI through a local console, the CLI displays a message when the shutdown is complete.

If you are connected to the CLI through the network, the CLI does not display any notifications and the connection times out.

execute ssh

Use this command as the Linux `ssh` command.

Syntax

```
execute ssh <user@host>
```

execute telnettest

Use this command to test Telnet connectivity to a host.

Syntax

```
execute telnettest {<fqdn_str> | <host_ipv4>}[:<port_int>]
```

Variable	Description	Default
`{<fqdn_str> | <host_ipv4>}`	IP address or FQDN of the Telnet server.	
`[:<port_int>]`	If the Telnet server listens on a port number other than port 23, enter a colon (:) followed by the port number.	`:23`

Example

This example tests the connection to an Telnet server at 192.168.1.10 on port 2323.

```
execute telnettest 192.168.1.10:2323
```

The CLI displays the following:

```
(using 192.168.1.20 to connect)
Remote Output(hex):
FF FD 18 FF FD 20 FF FD
23 FF FD 27
Connection Status:
Connecting to remote host succeeded.
```

execute traceroute

Use this command to use ICMP to test the connection between FortiAI and another network device, and display information about the time required for network hops between FortiAI and that device.

Syntax

```
execute traceroute {<fqdn_str> | <host_ipv4>}
```

Variable	Description	Default
`traceroute {<fqdn_str> | <host_ipv4>}`	IP address or FQDN of the host.	

Example 1

This example tests connectivity between FortiAI and http://docs.fortinet.com. In this example, the trace times out after the first hop indicating a possible connectivity problem at that point in the network.

```
execute traceoute docs.fortinet.com
traceroute to docs.fortinet.com (65.39.139.196), 30 hops max, 38 byte packets
1  172.16.1.200 (172.16.1.200) 0.324 ms 0.427 ms 0.360 ms
2  * * *
```

Example 2

This example tests the availability of a network route to the server example.com.

```
execute traceroute example.com
```

The CLI displays the following:

```
traceroute to example.com (192.168.1.10), 32 hops max, 72 byte packets
1 172.16.1.2  0 ms 0 ms 0 ms
2  10.10.10.1  <static.isp.example.net> 2 ms 1 ms 2 ms
3  10.20.20.1   1 ms  5 ms  1 ms
4  10.10.10.2  <core.isp.example.net> 171 ms 186 ms 14 ms
5  10.30.30.1  <isp2.example.net> 10 ms 11 ms 10 ms
6  10.40.40.1  73 ms 74 ms 75 ms
7 192.168.1.1  79 ms 77 ms 79 ms
8 192.168.1.2 73 ms 73 ms 79 ms
9 192.168.1.10 73 ms 73 ms 79 ms
10 192.168.1.10 73 ms 73 ms 79 ms
```

Example 3

This example attempts to test connectivity between FortiAI and example.com. However, FortiAI cannot trace the route because the primary or secondary DNS server that FortiAI is configured to query cannot resolve the FQDN example.com into an IP address, and so it does not know to which IP address it should connect. As a result, an error message displays.

```
execute traceroute example.com
traceroute: unknown host example.com
Command fail. Return code 1
```

To resolve the error in order to perform connectivity testing, the administrator would first configure FortiAI with the IP addresses of DNS servers that are able to resolve the FQDN example.com.

execute update

Use this command to manually request updates or delete the downloaded cache files for updates to the FortiAI ANN database and engine from FDS (FortiGuard Distribution Servers).

Syntax

```
execute update {now|clean-up}
```

execute vm license

In VM only, use this command to install license.

Syntax

```
execute vm license {disk|scp|ftp|tftp} <filenmame> <server>[:ftp port]
```