CLI Reference Guide

FortiNDR 7.6.2

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO LIBRARY

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/training-certification

FORTINET TRAINING INSTITUTE

https://training.fortinet.com

FORTIGUARD LABS

https://www.fortiguard.com

END USER LICENSE AGREEMENT

https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdoc@fortinet.com

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-05-23	Initial release.
2025-06-24	Updated diagnose system disk-usage on page 71, execute raidrebuild status on page 91, execute raidrebuild start on page 91 and execute raidlevel on page 90.
2025-06-26	Updated execute demo on page 81.
2025-10-28	Updated execute factoryreset on page 83 and execute factoryreset disk on page 84

Introduction

You can access the FortiNDR CLI (Command Line Interface) using the FortiNDR 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 FortiNDR CLI is case-sensitive.

Configuration commands

The `config` commands configure your FortiNDR settings:

config log alertemail server

Syntax

Use this command to configure the Email server FortiNDR will use to send alert emails for events detected.

```
config log alertemail server
```

```
    set name < name >
    set openssl {enable|disable}
    set password <password>
    set port <port>
    set sendername <senderName>
    set username <username>
end
```

Variable	Description	Default
`name`	Name/IP of the mailing server.	`smtp.fortinet.com`
`openssl`	Enable/disable security connection for the email transaction.	`disable`
`password`	Password of the user in the mailing server.	
`port`	The port used to send email.	587
`sendername`	The email sender's name. This is different from `username`.	
`username`	Name of the user in the mailing server.	

config profile authentication radius

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

Syntax

```
config profile authentication radius
    edit <profile_name>
        set access-override {enable | disable}
        set auth-prot {auto | chap | mschap | mschap2 | pap}
        set message-authenticator-attribute {enable | disable}
        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
`access-override`	Enable or disable use of the `Fortinet-Access-Profile` attribute to override the admin profile.	`disable`
`auth-prot {auto | chap | mschap | mschap2 | pap}`	The authentication method for the RADIUS server.	`auto`
`message-authenticator-attribute`	Require the server to include the `Message-Authenticator` attribute in its response.	`enable`
`nas-ip <ip_addr>`	The NAS IP address and the Called Station ID. If you do not enter an IP address, FortiNDR uses the IP address that the FortiNDR 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. The standard port number for RADIUS is 1812.	`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 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. 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, FortiNDR uses the mail domain as the UPN. To use a UPN other than the mail domain, also configure upn-suffix <upns_str>.	`searchuser`
`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 FortiNDR 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=FortiNDR,dc=example,dc=com. This command is optional if your LDAP server does not require FortiNDR to authenticate when performing queries and you have enabled unauth-bind.	

Variable	Description	Default
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 FortiNDR 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 FortiNDR caches query results. After the time has elapsed, cached results expire and subsequent requests for that information requires FortiNDR 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. find: De-reference only when finding the base search object.	never
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, FortiNDR 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

Variable	Description	Default
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 FortiNDR 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 FortiNDR waits for query responses from the LDAP server.	10
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 FortiNDR 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 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}
      set vsa {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 FortiNDR 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
`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.	none

Variable	Description	Default
	Users with this permission set to none cannot log into the system. The default is none in the GUI.	
vsa {none | read | read-write}	Specify the account permission associated with this access profile. The read-write permission gives access to all the functions under Virtual Security Analyst. This includes Express Malware Analysis, Outbreak Search, Static Filter, NDR Muting, ML Configuration, Malware Big Picture and Device Enrichment.	

config system admin

Use this command to configure FortiNDR administrator accounts.

By default, FortiNDR 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 | ldap | 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 {Neutrino| Jade | Mariner | Graphite | Melongene | Onyx | Dark_Matter | Eclipse
| Cloud_App_Light | Cloud_App_Dark}
        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.	

Variable	Description	Default
auth-strategy {local | local-plus-radius | ldap | radius}	Select the local or remote type of authentication that the administrator can use.	local
name <name>	Name of user.	english
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 FortiNDR 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 {Neutrino| Jade | Mariner | Graphite | Melongene | Onyx | Dark_Matter | Eclipse | Cloud_App_Light | Cloud_App_Dark}	Theme of the GUI for this admin.	Neutrino
trust-hosts <host_ipv4mask>	Enter one to three IP addresses and netmasks from which the administrator can log into FortiNDR. 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 login page.

Syntax

```
config system appearance
    set login-page-theme {Neutrino| Jade | Mariner | Graphite | Melongene | Onyx | Dark_Matter |
Eclipse | Cloud_App_Light | Cloud_App_Dark}
end
```

Variable	Description	Default
login-page-theme {Neutrino| Jade | Mariner | Graphite | Melongene | Onyx | Dark_ Matter | Eclipse | Cloud_ App_Light | Cloud_App_Dark}	The theme of the setting page for this user.	Neutrino

config system automation-settings

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

Syntax

```
config system automation-settings
        edit <name_str>
                    set type {fgt-quarantine|fnac-quarantine| fsw-quarantine-via-
fortilink|generic-webhook}
                    set vdom <vdom_str>
                    set api-key <apikey_str>
                    set webhook-config <config_str>
                    set ip <ip_addr>
                    set port <port_int>
                    set status {enable | disable}
                    set source {fabric-device | sniffer}
                    set profile <enforcement_profile_name>
            end
```

Variable	Description	Default
name <string>	Automation Profile name	Fgt-quarantine
type {fgt-quarantine|fnac-quarantine|fsw-quarantine-via-fortilink|generic-webhook}	FortiNDR supports four types of automated quarantine: fgt-quarantine, fnac-quarantine, fsw-quarantine-via-fortilink and generic-webhook	root
vdom <vdom_str>	The VDOM of the FortiGate. Only applicable to fgt-quarantine and fsw-quarantine-via-fortilink.	
api-key <apikey_str>	API key of the device. Only applicable to fgt-quarantine, fsw-quarantine-via-fortilink and fnac-quarantine.	
webhook-config <config_str>	The webhook configuration to be used by FortiNDR enforcement. Only applicable to fgt-quarantine , fsw-quarantine-via-fortilink and generic-webhook. For fgt-quarantine or fsw-quarantine-via-fortilink: {"webhook_exec" :"ip_blocker", "webhook_undo": "ip_unblocker"} For generic-webhook: {"webhook_exec" :{"url":"https://host1[.]com:443/api/ip_blocker","method":"post","http_body":"{\"srcip\":\"%%srcip%%\"}","headers":{"content-type":"application/json"}}, "webhook_undo": {"url":"https://host1[.]com:443/api/ip_unblocker","method":"post","http_body":"{\"srcip\":\"%%srcip%%\"}","headers":{"content-type":"application/json"}} } To enter the JSON data through CLI, the JSON string must be formatted as one line and enclosed in single quotes (').	
ip <ip_addr>	IP address of the device. Only applicable to fgt-quarantine, fsw-quarantine-via-fortilink and fnac-quarantine.	
port <port_int>	Port number of the device. Only applicable for fgt-quarantine, fsw-quarantine-via-fortilink and fnac-quarantine.	443
Status {enable | disable}	Enable or disable the automation profile.	enable
source {fabric-device | sniffer}	Set the source of detection that applies to the current profile. Only applicable for fgt-quarantine fsw-quarantine-via-fortilink.	Fabric-device

Variable	Description	Default
`profile <enforcement_ profile_name>`	The enforcement profile to be used by the current automation setting.	`default`

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 FortiNDR 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.	
`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 FortiNDR.

FortiNDR 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 conserve-mode

Use this command can enable or disable FortiNDR conserve mode. Default is on.

Syntax

```
config system conserve-mode
    set status {enable | disable}
```

Variable	Description	Default
status {enable │ disable}	Enable or disable conserve mode.	enable

config system csf

Use this command to configure FortiNDR as a Security Fabric member.

Syntax

```
config system csf
    set configuration-sync {local | sync}
    set managment-ip <ip_str>
    set managment-port <port_int>
    set status {enable | disable}
    set upstream-ip <ip_str>
    set upstream-port <port_int>
```

Variable	Description	Default
configuration-sync {local | sync}	Configuration synchronization mode.	local
managment-ip <ip_str>	Management IP address of FortiNDR to join the Security Fabric.	
managment-port <port_int>	Management port number of the unit to join the Security Fabric. Set the value between 1-65535.	443
status {enable | disable}	Enable or disable Security Fabric configuration.	disable
upstream-ip <ip_str>	IP address of upstream FortiGate.	
upstream-port <port_int>	Upstream FortiGate port number.	8013

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
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 FortiNDR 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`
`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-profile

Use this command to configure the FortiNDR enforcement profile. FortiNDR system will use this to filter out anomaly detection events for executing enforcement.

Syntax

```
config system enforcement-profile
  edit <name_str>
    set allowlist <ipv4mask>
    set risk-level <int>
    set conf-level <int>
    set severity <int>
    set category {malware,botnet,encrypted-attack,network-attack,ioc,week-cipher, machine-
```

```
learning}
   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 FortiNDR. 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 FortiNDR. The valid range is `0.8` to `1.0`.	`0.8`

config system fortigate settings

Use this command to configure settings for FortiGate inline blocking. As of FortiOS 7.0.1, FortiGate can send files and get the verdict from FortiNDR directly via the HTTP/2 protocol after FortiNDR joins the Security Fabric.

Syntax

```
config system fortigate settings
   set timeout <timeout_int>
   set block-risk-level {low, medium, high, critical}
   set block-confidence-level {low, medium, high, critical}
end
```

Variable	Description	Default
`timeout <timeout_int>`	The maximum wait time for FortiNDR to send the verdict back to FortiGate. Timeout set to 0 means FortiNDR will not wait for the verdict and only use cache detection. Cache detection refers to the previous verdict or preload detections.	1
`Block-risk-level {low, medium, high, critical}`	FortiNDR will send block request to FortiGate when a malicious file is detected with a risk level and confidence level at or above the configured value.	medium
`Block-confidence-level {low, medium, high, critical}`	FortiNDR will send block request to FortiGate when a malicious file is detected with a risk level and confidence level at or above the configured value.	medium

config system fortiguard update

Use this command to configure how FortiNDR will retrieve the most recent Fortiguard Neural Networks engine and database updates.

Syntax

```
config system fortiguard update
    set scheduled-update-day <day_int>
    set scheduled-update-frequency {daily | every | weekly}
    set scheduled-update-status {enable | disable}
    set scheduled-update-time <time_str>
    set override-server-status {enable | disable }
    set override-include-default-servers {enable | disable }
    set override-server-main-port <port_num>
    set override-server-address-main <ovr_svr_1 ovr_svr_2 ...>
    set override-server-alt-port <port_num>
    set override-server-address-alt <ovr_svr_1 ovr_svr_2 ...>
    set anycast-status <enable/disable>
    set tunneling-status {enable | disable}
    set tunneling-address {web_proxy_address}
    set tunneling-port {web_proxy_port}
    set tunneling-username {proxy_user_name}
    set tunneling-password {proxy_user_password}
end
```

Variable	Description	Default
scheduled-update-day <day_int>	Enter the day of the week at which FortiNDR will request updates where the range is from 0-6 and 0 means Sunday and 6 means Saturday.	0
scheduled-update-frequency {every | daily | weekly}	Enter the frequency at which FortiNDR will request updates. You also need to configure scheduled-update-day <day_int> and scheduled-update-time <time_str>.	every
scheduled-update-status {enable | disable}	Enable to perform updates according to the configured schedule.	disable
scheduled-update-time <time_str>	Enter the time of the day at which FortiNDR will request updates, in the format hh:mm, where hh means update on every (1-23) hours, mm means starting on minutes (0-59), and 60 means random minutes.	01:60
override-server-status	When enabled, this will force the FDS update to point to the override server address(es).	disable
override-server-include-default-servers	In the case when the override servers cannot be reached, this will attempt to try to connect to the default servers as a fallback	enable

Variable	Description	Default
override-server-main-port	Port of the main override servers.	443
override-server-address-main	The address(es) of the override server(s) for the main FDS downloads (to override fai.fortinet.net). The override addresses can be an IP address or a hostname. Multiple override server addresses can be entered if each one is separated by a space. When using multiple override server addresses, the first one on the list will be attempted first, if it cannot be reached, then the updater will try the second address and so on.	0.0.0.0
override-server-alt-port	Port of the alternative override servers	443
override-server-address-alt	The address(es) of the override server(s) for the main FDS downloads (to override *globalupdate.fortinet.net* when anycast is enabled and to override *update.fortiguard.net* when anycast is disabled). The override addresses can be an IP address or a hostname. Multiple override server addresses can be entered if each one is separated by a space. When using multiple override server addresses, the first one on the list will be attempted first, if it cannot be reached, then the updater will try the second address and so on. Both the `override-server-address-main` and `override-server-address-alt` must be set at the same time.	0.0.0.0
anycast-status	When enabled, the alternative servers will use the anycast FDS server *globalupdate.fortinet.net* instead of unicast FDS server *update.fortiguard.net*.	enable
tunneling-status {enable | disable}	Turn proxying FDS communication on and off.	disable
tunneling-address <web_proxy_address>	Set IP (ipv4/ipv6) of web proxy server that FortiNDR will be using to communicate with FDS servers.	0.0.0.0
tunneling-port <web_proxy_port>	Set port of web proxy server that FortiNDR will be using to communicate with FDS servers.	0
tunneling-username <proxy_user_name>	Set user name of web proxy server that FortiNDR will be using to communicate with FDS servers.	
tunneling-password <proxy_user_password}>	Set user password of web proxy server that FortiNDR will be using to communicate with FDS servers	

config system global

Syntax

Use this command to configure the FortiNDR system-wide configuration.

```
config system global
   set hostname <str>
   set admin-idle-timeout <int>
end
```

Variable	Description	Default
`hostname <string>`	Host name of FortiNDR.	Varies by model
`Admin-idle-timeout`	The idle time-out for system administration in minutes.	45 minutes

config system ha

Use this command to configure FortiNDR to act as a member of a Hgh Availability (HA) cluster in order to increase availability.

```
config system ha
config interface
  edit <interface_name>
    set action-on-primary {ignore-vip | use-vip}
    set heartbeat-status {disable | primary | secondary}
    set peer-ip <ipv4mask>
    set port-monitor <enable | disable>
    set virtual-ip <ipv4mask>
set hb-base-port <hb-port_int>
set hb-lost-threshold <hb-threshold_int>
set mode {off | primary | secondary}
set password <password_str>
```

Variable	Description	Default
`<interface_name>`	Enter the interface name of which you want to apply HA configuration.	
`action-on-primary {ignore-vip | use-vip}`	Enable/disable virtual IP configured on this interface. • `ignore-vip`: Do not use the virtual ip configuration when HA mode is primary • `Use-vip`: Add the specified virtual IP address and netmask to the network interface when HA mode is	Ignore-vip

Variable	Description	Default
	primary. This option results in the network interface having two IP addresses: the actual and the virtual.	
heartbeat-status {disable | primary | secondary}	Specify if this interface will be used for HA heartbeat and synchronization. • `Disable`: Do not use this interface for HA heartbeat and synchronization. • `primary`: Select the primary network interface for heartbeat and synchronization traffic. This network interface must be connected directly or through a switch to the Primary heartbeat network interface of other member in the HA group. • `secondary`: Select the secondary network interface for heartbeat and synchronization traffic. The secondary heartbeat interface is the backup heartbeat link between the units in the HA group. If the primary heartbeat link is functioning, the secondary heartbeat link is only used for the HA heartbeat. Otherwise the secondary link is used for both the HA heartbeat and synchronization. In general, you should isolate the network interfaces that are used for heartbeat traffic from your overall network. Heartbeat and synchronization packets contain sensitive configuration information, are latency-sensitive, and can consume considerable network bandwidth.	disable
peer-ip <ipv4mask>	Enter the IP address of the matching heartbeat network interface of the other member of the HA group. If you are configuring the primary unit's primary heartbeat network interface, enter the IP address of the secondary unit's primary heartbeat network interface. For the secondary heartbeat network interface, enter the IP address of the other unit's secondary heartbeat network interface.	0.0.0.0
port-monitor <enable | disable>	Enable to monitor a network interface for failure. If the port fails, the primary unit will trigger a failover.	disable
virtual-ip <ipv4mask>	Enter the virtual IP address and netmask for this interface.	0.0.0.0/0
hb-base-port <hb-port_int>	Enter the first of four total TCP port numbers that will be used for: • The heartbeat signal	20000

Variable	Description	Default
	• Synchronization control • Data synchronization • Configuration synchronizatio	
hb-lost-threshold <hb-threshold_int>	Enter the total span of time, in seconds, for which the primary unit can be unresponsive before it triggers a failover and the secondary unit assumes the role of the primary unit. 💡 If the failure detection time is too short, the secondary unit may falsely detect a failure during periods of high load.	30
mode {off | primary | secondary}	Enter the HA operating mode or disable HA	off
password <password_str>	Enter a password for the HA group. The password must be the same on the primary and secondary FortiNDR unit(s). The password must be a least 1 character.	

config system ICAP server

Use this command to configure ICAP server settings.

Syntax

```
config system icap server
    set conf-level <confidence_level_int>
    set interface {port1 | port2}
    set enable {1 | 0}
    set rtavscan {1 | 0}
    set ssl-port <ssl_port_int>
    set ssl-support {1 | 0}
    set port <port_int>
    set timeout <timeout_int>
end
```

Variable	Description	Default
conf-level <confidence_level_int>	The confidence of detection. Value is between 0 and 100.	80
interface {port1 | port2}	Interface name.	Port1

Variable	Description	Default
enable {1 | 0}	Set to 1 to enable ICAP server. Set to 0 to disable the ICAP server.	
rtavscan {1|0}	Set to 1 to enable realtime FAI scan. Set to 0 to disable.	
timeout <timeout_int>	The maximum waiting time for realtime FAI scan.	10
ssl-port <ssl_port_int>	ICAP server SSL port number.	
ssl-support {1 | 0}	Set to 1 to enable SSL support. Set to 0 to disable it.	
port <port_int>	ICAP server port.	

config system interface

Use this command to configure allowed and denied administrative access protocols, up or down administrative status for the network interfaces of FortiNDR.

Syntax

```
config system interface
    edit <physical_interface_str>
        set allowaccess {ping https ssh telnet}
        set discover {enable | disable}
        set ip {ipv4mask}
        set mode {static | dhcp}
        set mtu <mtu_int>
        set sniffer {off | ndrd | snifferd}
        set speed {auto | 10full | 10half | 100full | 100half | 1000full}
        set status {down | up}
    end
```

Variable	Description	Default
<physical_interface_str>	Name of the physical network interface, such as port1.	
allowaccess {ping | https | ssh | telnet}	Add one or more protocols to the list of protocols that allow administrative access to FortiNDR through this network interface:	Varies by network interface.
	ping Allow ICMP ping responses from this network interface.	
	https Allow secure HTTP (HTTPS) access to the web-based manager and per-recipient quarantines.	

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.	
`discover {enable	disable}`	Allow discovery of the interface on this port.	
`ip <ipv4mask>`	IP address and netmask of the network interface.	
`set mtu <mtu_int>`	Sets the maximum packet or Ethernet frame size in bytes. The Maximum Transmission Unit (MTU) determines the largest size of packets or Ethernet frames that can be transmitted without fragmentation. Setting the correct MTU is crucial for optimal network performance and reliability. If the MTU is not aligned with the requirements of your network, packets may require fragmentation or defragmentation at network nodes, which can lead to performance issues and packet drops. The valid range is from 68 to 9702 bytes.	
`mode {static	dhcp}`	Interface mode.	`static`
`sniffer {off	ndrd	snifferd}`	Sniffer mode of the network interface. This option is only available on sniffer network interfaces.	`ndrd` `snifferd`
`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`

configure system ndr settings

Use this command to configure NDR- related features, such as enabling or disabling the databases for the IPS engine and managing pcap capturing.

Syntax

```
config system ndr setting
set ips-dbs { nids | apdb | isdb| otapp | none}
        set dump-pcap {enable | disable}
        set type {IOC | botnet | encrypted-attack  | network-attack  | weak-cipher}
        set external-path <external_path_str>
end
```

Multiple Options	Description	Default
`Ips-dbs { nids apdb isdb` `    otapp | none}`	Turn off or on nids, apdb, isdb or otapp database for IPS Engine. Use none to deselect all dbs for IPS Engine.	nids apdb
`dump-pcap {enable | disable}`	Select to enable conditional pcap capturing feature. • The number of anomaly session captures and packets that can be collected will depend on the device model. • This feature is not supported on VM models. • The maximum size of each capture file is 1 MB. • PCAP availability is commonly subject to latency.The tested FortiNDR-1000F max throughput when `pcap-dump` is enabled is 2Gbps for 1 hour.	disable

`type {IOC | botnet |`
`    encrypted-attack |`
`    network-attack | weak-`
`    cipher}`
	Select anomaly types events that will trigger pcap capturing.
	Multiple choices are supported.
		botnet encrypted-attack network-attack IOC

`External-path <external_path_` `    str>`	Enter the artifact storage profile name to enable pcap external storage. If there is no artifact storage profile specified, local disk storage will be enabled. For more information, see Artifact Storage.	

config system password-policy

Use this command to configure FortiNDR password policy.

Syntax

```
config system password-policy
    set status {enable | disable}
    set minimum-length        <minimum_int>
    set must-contain {upper-case-letter | lower-case-letter | number | non-alphanumeric}
    set allow-admin-empty-passwd      {enable | disable}
    set min-change-characters <min_change_char_int>
    set expire-status {enable | disable}
    set expire-day <expire_day_int>
end
```

Variable	Description	Default
`status {enable	disable}`	Select to enable the password policy.	Enable
`minimum-length <minimum_ int>`	Set the minimum acceptable length for passwords.	8
`must-contain < upper-case- letter	lower-case- letter	number	non-alphanumeric >`	Select any of the following special character types to require in a password. Each selected type must occur at least once in the password. <table><tr><td>`upper-case-letter`</td><td>A – Z</td></tr><tr><td>`lower-case-letter`</td><td>a- z</td></tr><tr><td>`number`</td><td>0, 1, 2, 3, 4, 5, 6, 7 8, 9</td></tr><tr><td>`non-alphanumeric`</td><td>Punctuation marks, @,#, ... %</td></tr></table>	upper-case-letter lower-case-letter number non-alphanumeric
`allow-admin-empty-passwd { enable	disable }`	Enable to allow the admin password to be empty.	Disable
`min-change-characters`	Minimum number of unique characters in new password which do not exist in old password (0 - 128, default = 0.)	0
`expire-status`	Enable or disable password expiration.	Disable
`expire-day`	Nmber of days after which passwords expire (1 - 999 days, default = 90)	90

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 snmp community

Use this command to configure simple network management protocol (SNMP) v1/2 settings. These commands apply only if the SNMP agent is enabled.

Syntax

```
config system snmp community
edit <index_int>
config host
edit <index_int>
set ip <address_ipv4>
set name <name_str>
set queryportv1 <port_int>
set queryportv2c <port_int>
set queryv1-status {enable | disable}
```

```
set queryv2c-status {enable | disable}
set status {enable | disable}
set trapevent {cpu | logdisk | datadisk | mem | system}
set trapportv1_local <port_int>
set trapportv1_remote <port_int>
set trapportv2c_local <port_int>
set trapportv2c_remote <port_int>
set trapv1_status {enable | disable}
set trapv2c_status {enable | disable}
end
```

config system snmp threshold

Use this command to configure the event types that trigger an SNMP trap.

Syntax

```
config system snmp threshold
    Set {cpu | logdisk | datadisk | mem } <trigger_int> <threshold_int> <sample_period_int> <sample_
        frequency_int>
end
```

Variable	Description		Default
{cpu | logdisk | datadisk | mem} <trigger_int> <threshold_int> <sample_period_int> <sample_frequency_int>	Specify the trap event, such as cpu or mem, then specify the following threshold values:		cpu: 80 3 600 30 mem: 80 3 600 30 logdisk: 90 1 7200 3600 Datadisk: 90 1 7200 3600
	trigger_int	You can enter either the percent of the resource in use or the number of times the trigger level must be reached before it is triggered. For example, using the default value, if the mailbox disk is 90% or more full, it will trigger.	
	threshold_int	Sets the number of triggers that will result in an SNMP trap. For example, if the CPU level exceeds the set trigger percentage once before returning to a lower level, and the threshold is set to more than one an SNMP trap will not be generated until that minimum number of triggers occurs during the sample period.	

Variable	Description		Default
	`sample_period_int`	Sets the time period in seconds during which the FortiMail unit SNMP agent counts the number of triggers that occurred. This value should not be less than the Sample Frequency value.	
	`sample_frequency_ int`	Sets the interval in seconds between measurements of the trap condition. You will not receive traps faster than this rate, depending on the selected sample period. This value should be less than the Sample Period value.	

config system snmp user

Use this command to configure SNMP v3 user settings. SNMP v3 adds more security by using authentication and privacy encryption.

Syntax

```
config system snmp user
edit <user_name>
set query-status {enable | disable}
set query-port <port_number>
set security-level {authnopriv | authpriv | noauthnopriv}
set auth-proto {sha1 | md5}
set aut-pwd <password>
set status {enable | disable}
set trap-status {enable | disable}
set trapevent {cpu | logdisk | datadisk | mem | system}
set trapport-local <port_number>
set trapport-remote <port_number>
config host
edit <host_no>
set ip <class_ip>
end
end
```

Variable	Description	Default
`<user_name>`	Enter a name to identify the SNMP user on FortiNDR.	
`query-status {enable	disable}`	Enable to allow SNMP v3 query from the SNMP managers. Also configure the query port as described below.	disable

Variable	Description	Default
`query-port <port_number>`	Specify the port number used to listen to queries from the SNMP manager.	161
`security-level {authnopriv	authpriv	noauthnopriv}`	Choose one of the three security levels for the communication between FortiNDR and the SNMP manager.	
	noauthnotpriv (no authentication, no privacy):	This option is similar to SNMP v1 and v2.	
	authnopriv (authentication, no privacy)	This option enables authentication only. The SNMP manager needs to supply a password that matches the password you specify on FortiNDR. You must also specify the authentication protocol (either SHA1 or MD5).	
	authpriv (authentication, privacy)	This option enables both authentication and encryption. You must specify the protocols and passwords. Both the protocols and passwords on the SNMP manager and FortiNDR must match.	
`auth-proto {sha1	md5}`	Specify the authentication protocol if you choose authentication for the security level. Otherwise, this option is not displayed.	
`aut-pwd <password>`	Specify the authentication password if you choose authentication for the security level. Otherwise, this option is not displayed.	
`status {enable	disable}`	Enable or disable the SNMP v3 user on FortiNDR.	`disable`
`trap-status {enable	disable}`	Enable to activate traps on FortiNDR.	`disable`
`trapevent {cpu	logdisk	datadisk	mem	system}`	Enter one or more of the following events that will generate a trap when the event occurs or when its threshold is reached	Cpu Logdisk datadisk mem system

Variable	Description	Default
`cpu`	CPU usage threshold.	
`logdisk`	Log disk space low threshold.	
`datadisk`	Data disk space low threshold.	
`mem`	Memory low threshold.	
`system`	System events, such as a change in the state of hardware, power failure and so on.	
`trapport-local <port_number>`	Enter the local port number for sending traps.	162
`trapport-remote <port_number>`	Enter the remote port number that listens to SNMP traps on the SNMP manager.	162
`<host_no>`	Enter an index number for the SNMP manager.	
`ip <class_ip>`	Enter the IP address of the SNMP manager.	

config system syslog fortianalyzer settings

Syntax

Use this command to configure a FortiAnalyzer remote server which will receive syslogs. FortiNDR system will send logs with specified type and severity (only for NDR type) to this remote server.

```
config system syslog fortianalyzer settings
    set ipaddr <ipv4mask>
    set port    <int>
    set status {enable, disable}
    set type    {event, malware, ndr, netflow}
    set ndr-severity {low, medium, high, critical}
    set protocol {syslog, oftps}
end
```

Variable	Description	Default
`ipaddr <ipv4mask>`	The IP address of the remote server. Only IPv4 is supported.	`0.0.0.0`
`port <int>`	The port number of the remote server for syslog services.	`514`

Variable	Description	Default
status {enable, disable}	Enable or disable sending logs to this remote server.	disable
type {event, malware, ndr, netflow}	FortiNDR supports three types of logs: event, malware, ndr and netflow. Multiple choices are supported.	event, malware, ndr
ndr-severity {low, medium, high, critical}	Filtering by severity is supported for sending ndr type log,. The supported multiple choices are low, medium, high and critical.	low, medium, high, critical
protocol {syslog, oftps}	The protocol for connecting to the remote server	oftps

config system syslog1 settings

Use this command to configure a general remote server which can receive syslogs. FortiNDR system will send logs with specified type and severity (only for ndr type) to this remote server.

Syntax

```
config system syslog1 settings
    set ipaddr <ipv4mask>
    set port   <int>
    set status {enable, disable}
    set type   {event, malware, ndr, netflow}
set ndr-severity {low, medium, high, critical}
set format {default, cef}
end
```

Variable	Description	Default
Name <string>	Profile name	
ipaddr <ipv4mask>	The IP address of the remote server. Only IPv4 is supported.	0.0.0.0
port <int>	The port number of the remote server for syslog services.	514
status {enable, disable}	Enable or disable sending logs to this remote server.	disable
type {event, malware, ndr, netflow}	FortiNDR supports three types of logs: event, malware, ndr and netflow. Multiple choices are supported.	event, malware, ndr

Variable	Description	Default
`ndr-severity {low, medium, high, critical}`	Filtering by severity is supported when sending `ndr` logs. The supported multiple choices are `low`, `medium`, `high` and `critical`.	`low, medium, high, critical`
`Format {default, cef}`	Log format: default is the syslog format, cef is the CEF (Common Event Format) format.	

config system syslog2 settings

Use this command to configure a general remote server which will receive syslogs. FortiNDR system will send logs with specified type and severity (only for `ndr` log types) to this remote server.

Syntax

```
config system syslog2 settings
    set ipaddr <ipv4mask>
    set port   <int>
    set status {enable, disable}
    set type   {event, malware, ndr, netflow}
set ndr-severity {low, medium, high, critical}
set format {default, cef}
end
```

Variable	Description	Default
`Name <string>`	Profile name	
`ipaddr <ipv4mask>`	The IP address of the remote server. Only IPv4 is supported.	`0.0.0.0`
`port <int>`	The port number of the remote server for syslog services.	`514`
`status {enable, disable}`	Enable or disable sending logs to this remote server.	`disable`
`type {event, malware, ndr, netflow}`	FortiNDR supports to three types of logs, including `event`, `malware` , `ndr` and `netflow`. Multiple choices are supported.	`event, malware, ndr`
`ndr-severity {low, medium, high, critical}`	Filtering by severity is supported when sending `ndr` logs. The supported multiple choices are `low`, `medium`, `high` and `critical`.	`low, medium, high, critical`
`Format {default, cef}`	Log format: default is the syslog format, cef is the CEF (Common Event Format) format.	

config system time manual

Use this command to manually configure the FortiNDR 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 FortiNDR 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 FortiNDR unit is located.	

config system time ntp

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

Accurate system time is required by many features of FortiNDR 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. FortiNDR 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 FortiNDR 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

The get command displays all settings, even if they are still in their default state.

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 profile ldap

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

Syntax

```
get profile ldap <ldap profile 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 FortiNDR administrator accounts.

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

For more information about the attributes, see Configuration commands on page 11.

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    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 00:45:24)
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 v1.5.2,build117,210903
Architecture: 64-bit
Serial-Number: FAI35FT319000026
BIOS version: 00010002
Log disk: Capacity 173 GB, Used 60 MB (0.04%), Free 173 GB
Data disk: Capacity 3313 GB, Used 25 GB (0.78%), Free 3287 GB
Remote disk: n/a
Memory: Capacity 375 GB, Used 25 GB (6.83%), Free 350 GB
Swap Memory: Capacity 31 GB, Used 0 MB (0.00%), Free 31 GB
Hostname: FAI35FT319000026
Strong-crypto: disabled
Distribution: International
Branch point: 117
Uptime: 3 days 16 hours 24 minutes
Last reboot: Fri Sep 03 19:29:00 MDT 2021
System time: Tue Sep 07 11:53:00 MDT 2021
Scenario AI DB: 1.076(2021-09-04 23:55)
Text AI Feature DB: 1.076(2021-09-04 23:56)
Text AI Group DB: 1.076(2021-09-04 23:56)
Text AI Learning Feature DB: 1.076(2021-09-04 23:56)
Binary Behavior DB: 1.082(2021-09-04 23:43)
Binary AI Feature DB: 1.082(2021-09-04 23:52)
Binary AI Group DB: 1.082(2021-09-04 23:52)
Binary AI Learning Feature DB: 1.082(2021-09-04 23:52)
Text AI Learning Engine: 1.004(2020-01-01 00:00)
Binary AI Engine: 1.053(2021-09-03 11:19)
Binary AI Learning Engine: 1.013(2021-09-03 11:19)
Scenario AI Engine: 1.001(2020-01-01 00:00)
Text AI Engine: 1.042(2020-01-01 00:00)
```

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 FortiNDR 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

The `diagnose` commands display diagnostic information that help you to troubleshoot problems.

diagnose autoupdate status

Show the status fo FDS updates.

Syntax

```
diagnose autoupdate status
```

Status	Description
FDN availability	Status of connection to FDN network.
Push update	Status of push updates.
Schedule update	Status of scheduled updates.
Web proxy tunneling for FDS updates	Status of FDS update through proxy.

diagnose debug

Use this command to displays the crash log for a specified date or for the past few days. If no date is provided, the current day's log is shown by default.

Syntax

```
diagnose debug application {cmdb_event | csfd | httpd | miglogd | sshd | updated | sdigestd |
ndrd} <debug_level>
diagnose debug cli <debug_level>
diagnose debug coredump {clear|delete|disable|enable|list|status|upload}
diagnose debug crashlog <days>|<yyyy-mm-dd>|<enter>
diagnose debug {enable | disable}
debug file {clear|disable|enable|info|show|upload}
```

```
diagnose debug kernel <debug_level>
diagnose debug process <process_name>
```

Variable	Description	Default
`debug_level`	A number from 0 to 8.	
`crash_log_date`	A date in the format of yyyy-mm-dd to filter the crash log by date.	
`process_name`	A specific process name. Available processes and explanations are as follows:	

`file_helper`	File processing daemon	
`event_flow`	Scenario Engine	
`moat_engine`	Text-based AI processing engine.	
`moat_learn`	Learning engine for text-based AI models.	
`pae2`	Binary AI Engine	
`pae_learn`	Binary AI learning Engine	
`sniffer`	Web packet sniffer	
`sys_mon`	System monitoring daemon	
`oftpd`	OFTP (Odette File Transfer Protocol) daemon.	
`sim_engine`	Similarity engine for comparing data patterns or content.	
`yyyy-mm-dd`	Date filter in yyyy-mm-dd format to display crash logs for a specific date.	
`days`	Integer (1–30) to display crash logs from the past specified number of days.	
`enter`	Press Enter without input to display the current day's crash log.	

Module/daemon	Description
`cmdb_event`	Monitor FortiNDR configuration change events.
`csfd`	Daemon responsible for Fortinet security fabric(csf) connection.
`httpd`	Daemon responsible for https service.
`ldapcached`	Daemon responsible for LDAP server querying service.

Module/daemon	Description
miglogd	Daemon responsible for system log generation.
ndrd	Daemon responsible for Network Detection and Response (NDR).
sdigestd	Daemon responsible for Network Share file scanning
sshd	Daemon responsible for SSH connections.
updated	Daemon responsible for FortiNDR license and ANN DB updates.

diagnose debug application

Use this CLI to view logs for various daemons based on system mode:

- *Sync daemon*: Available in Sensor and Center modes.
- *Control (ctrl) daemon*: Available in all modes.
- *PCAP capturing daemon*: Available in Sensor and Standalone modes.
- *Tag management daemon*: Available on 3600G models only.

If no variable is specified, the command displays real-time daemon logs by default.

Syntax

```
diagnose debug application {sync | ctrl}
diagnose debug application {sync|ctrl|pcapcleanerd|tgm}
diagnose debug application {sync|ctrl|pcapcleanerd|tgm} lines <number>
```

Variable	Description
sync	Daemon responsible for synchronizing data between center and sensor modes
ctrl	
lines <number>	Specify a positive integer to display that number of lines from the end (tail) of the selected daemon log. If the specified number exceeds the total number of lines in the log file, the entire file will be displayed.
<enter>	Press Enter without input to display the current day's crash log.

diagnose debug database error-log

Use this command to print out latest database error log.

Syntax

```
diagnose debug database error-log
```

diagnose debug icap

Use this command to display the most recent ICAP file event and related error messages from FortiNDR's ICAP Server.

Syntax

```
diagnose debug icap
```

Example

```
FortiNDR-VM # diagnose debug icap
System Time: 2024-05-06 11:09:37 PDT (Uptime: 10d 17h 29m)
2024-04-25 17:41:17,457 INFO main(1096) FNDR-ICAP is starting
2024-04-25 17:41:22,461 INFO main(1152) FNDR-ICAP configuration updated.
```

diagnose fds list

Use this command to show the current list of FDS server IPs and ports being used by FortiNDR. Be aware the current list of IPs can and will change without notice.

Syntax

```
diagnose fds list
```

diagnose hardware

Use this command to display FortiNDR 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 acceleratorinfo
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
diagnose hardware acceleratorinfo	Diagnose the accelerator status and information.	
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 hardware sensorinfo

Use this CLI to monitor and obtain information about the Power Supply, Temperature, and Fan sensors. This CLI is supported in FSA 3500F, 2500G and 2600G platforms.

Syntax

```
diagnose hardware sensorinfo {id | entity} <corresponding_data>
```

Variable	Description
Empty	Prints all the information about Power Supply, Temperature, and Fan sensors.
id <corresponding_data>	Allows you to get information about each sensor by its sensor ID.
entity <corresponding_data>	Each sensor is assigned a unique entity ID, grouping them accordingly. This arrangement allows for the provision of more detailed information based on these IDs.

diagnose kdb

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

Syntax

```
diagnose kdb
```

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 sniffer dump

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

Ensure the remote TFTP server has the *file create* permission.

Syntax

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

To dump files from FortiNDR with the CLI:

1. Specifiy the options and filters for file dumping with the following command:
   ```
   diagnose sniffer packet
   ```
   If traffic dumping is running in the background, you can stop or view the progress with the `stop` and `status` variables. For more information, see diagnose sniffer packet on page 63.

2. Get the PCAP's file name with the following command.
   ```
   diagnose sniffer file
   ```
   You will need the file name to delete all captured PCAP files. For more information, see diagnose sniffer file on page 62.

3. Transfer the previous dumped file to a TFTP server for further analysis.
   ```
   diagnose sniffer dump
   ```

Example:

```
FortiNDR-3500F # diagnose sniffer packet port1 "none" 1 20000 a chi.pcap 1 background
System Time: 2022-11-17 17:40:24 PST (Uptime: 14d 20h 22m)
interfaces=[port1]
filters=[none]
sniffer dump into chi.pcap (500M size limit)
last about 60 second
37 packets received by filter
0 packets dropped by kernel


FortiNDR-3500F # diagnose sniffer file display
System Time: 2022-11-17 17:40:40 PST (Uptime: 14d 20h 22m)
abc.pcap_2022-10-13-16-34-34.pcap 278 Thu Oct 13 16:34:34 2022
chi.pcap_2022-11-17-17-40-24.pcap 24 Thu Nov 17 17:40:24 2022
chi.pcap_2022-10-13-16-29-37.pcap 57208 Thu Oct 13 16:29:37 2022
chi.pcap_2022-10-13-16-27-06.pcap 98162098 Thu Oct 13 16:27:06 2022


FortiNDR-3500F # diagnose sniffer dump 172.19.235.204 chi.pcap_2022-11-17-17-40-24.pcap new.pcap
System Time: 2022-11-17 17:41:33 PST (Uptime: 14d 20h 23m)
Connect to tftp server 172.19.235.204 ...
Please wait...
#
Send sniffer file to tftp server OK.
```

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. 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.	1
count	Maximum number of packets to be recorded in this attempt.	-1
time format	Time format of the record. The options are:	relative

Variable	Description	Default
	a: Absolute UTC time in yyyy-mm-dd hh:mm:ss.ms format. `relative`: Relative to the start of sniffing in ss.ms format.	
`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 system csf global

Show a summary of all connected members in Security Fabric.

Syntax

```
diagnose system csf global
```

Example

```
{
    "path":"FGVM16TM00000000:FAI35FT000000000",
    "mgmt_ip_str":"",
    "mgmt_port":443,
    "sync_mode":1,
    "saml_role":"disable",
    "admin_port":443,
    "serial":"FAI35FT000000000",
    "host_name":"FAI35FT000000000",
    "firmware_version_major":1,
    "firmware_version_minor":5,
    "firmware_version_patch":0,
    "firmware_version_build":1,
    "device_type":"fortindr",
    "upstream_intf":"port1",
    "upstream_serial":"FGVM16TM00000000",
    "parent_serial":"FGVM16TM00000000",
    "parent_hostname":"FGVM",
    "upstream_status":"Authorized",
    "upstream_ip":-68480084,
    "upstream_ip_str":"172.19.1.1",
    "subtree_members":[
```

```
      ],
      "is_discovered":true,
      "ip_str":"172.19.1.2",
      "downstream_intf":"port2",
      "upstream_vdom":"root",
      "authorization_type":"certificate",
      "authorization_entry_name":"FAI35FT000000000",
      "idx":3
  }
```

diagnose system csf upstream

Show connected upstream FortiGates.

Syntax

```
diagnose system csf upstream
```

Example

```
System Time:  2021-04-11 01:01:01PDT (Uptime: 0d 1h 0m)
Upstream Information:
Serial Number:FGVM16TM00000000
IP:172.19.1.1
Connecting interface:port1
Connection status:Authorized
Saml setting not generated
```

diagnose system db

Use this command to diagnose and patch database if missing change has been detected. The process may take up to 10 mins.

Syntax

```
Diagnose system db
```

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 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 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 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-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 disk-usage

Use this command to check the disk usage of a specified system directory.

Syntax

```
diagnose system disk-usage {system-data|system-db|system-temp-data|system-inode}
```

diagnose system interface

This CLI is used to monitor the system interface status and get stats like PPS (packets per second) and drop rate. It will take the interface name and interval as inputs.

Syntax

```
diagnose system interface <Interface-name> <Interval>
```

Variable	Description	Default
`<Interface-name>`	Enter the name of available platform interface	
`<Interval>`	Seconds to sleep before reading from the interface. The default value is 1 second.	1

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 real-time system information, including CPU and memory usage, and running processes. By default, it refreshes every 5 seconds and shows the last 20 lines if no parameters are specified.

Syntax

```
diagnose system top <seconds> <lines> <iterations>
```

Variable	Description	Default
seconds	The interval between each refresh of the process list in seconds, range [1, 60] (default 5). For example, to refresh the process list every 5 seconds, type 5.	5
lines	The lines of the process list to display, range [1, 100] (default 20).	20
iterations	Specifies how many times to refresh and display the system information (1 to 1000). If not specified, the display runs continuously in real-time (default: unlimited).	unlimited

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 commands on page 76.
- <: 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*.

Example

This example refreshes the display of the top 19 most system-intensive processes every five seconds. The output indicates that FortiNDR 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
```

diagnose system top-fd

Use this command to display the top processes with the highest number of open file descriptors. If the detail option is used, it also shows detailed process information along with active file descriptor data. By default, the command displays the top 5 processes with the most open file descriptors.

Syntax

```
diagnose system top-fd detail <process-count> <fd-count>
```

Variable	Description	Default
process-count	Number of processes with the highest number of open file descriptors to display, range [1, 1000] (default 5).	5
fd-count	Number of file descriptors to include per process (default 50).	50

diagnose system vm

Use this command to diagnose the virtual machine state.

Syntax

```
Diagnose system vm
```

Example:

```
System Time:  2022-04-19 01:35:33 PDT (Uptime: 0d 8h 9m)

UUID:        420c1e91dbd40952f9c6e5a4b0500acb

File:        VM license file is valid.

Resources:   32 vcpus/32 allowed

Management IP: 0.0.0.0

Registered: 1 (True)

Status:      1 (Valid: Full License is in use.(Expire in 366 days 23 hours))
```

```
FDS code:   200

Warn count: 0

Copy count: 0

Received:   1720285758

Warning:    0

Recv:       202204190654

Dup:
```

Execute commands

The execute commands perform immediate operations on the FortiNDR unit.

execute api-key

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

> If you want to specify an API key instead of the key automatically generated by FortiNDR, the API key string must be 31 characters in length and contain only upper and lower case letters, and numbers.

Syntax

```
execute api-key <system-user-name> [user-specified-API-key]
```

execute backup config

Use this command to back up the configuration file.

Syntax

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

execute backup system-db ml-baseline

Use this command to backup FortiNDR Machine Learning (ML) baseline information in Standalone or Center mode.

Syntax

```
execute backup system-db ml-baseline {disk|scp|ftp|tftp} <filename-to-be-saved> <server>[:ftp port]
     <user-name> <password>
```

Variable	Description
disk	The local disk.
ftp	The FTP server.
scp	The SCP server.
tftp	The TFTP server.

execute backup system-db netflow-ml-baseline

Use this command to backup Netflow Machine Learning (ML) baseline info in Standalone or Center mode.

Syntax

```
execute backup system-db netflow-ml-baseline {disk|scp|ftp|tftp} <filename-to-be-saved> <server>
     [:ftp port] <user-name> <password>
```

Variable	Description
disk	The local disk.
ftp	The FTP server.
scp	The SCP server.
tftp	The TFTP server.

execute backup system-db network-share-config

Use this command to backup network share configurations in standalone or sensor mode.

Syntax

```
execute backup system-db network-share-config {disk|scp|ftp|tftp} <filename-to-be-saved> <server>
     [:ftp port] <user-name> <password>
```

Variable	Description
disk	The local disk.
ftp	The FTP server.
scp	The SCP server.
tftp	The TFTP server.

execute center-retention-setting

Use this CLI to set retention, Time to Live (TTL) for FortiNDR log tables. This is software theoretical limit for retention, for estimation of retention in different VM/physical models based on average AV and NDR throughput. This execute action is persistent after reboot/power-cycle.

For more information, see Planning deployment.

Syntax

```
execute center-retention-setting <'service name'> < retention days >
```

Variable	Description
'service name'	Select the retention setting for FortiNDR data. Available service names are: • Network Events • File Events • Sensor Monitor Data • Machine Learning Data Ensure the service name is enclosed in single quotes (').
retention days	Data retention in days. Valid range is from 1 – 730 days

execute cleanup

Use this command to remove all logs including all counts in the Dashboard, Malware Log, NDR log, and ML Discovery log but will keep the ML baseline and feedback.

Syntax

```
execute cleanup
```

execute cleanup ml

Use this command to clean up all FortiNDR ML Discovery logs. It also retrains the baseline but keeps user feedback.

Syntax

Center Mode

```
exec cleanup ml [sensor-group-id]
```

This CLI will clean up all related FortiNDR ML machine learning baselines if no `sensor-group-id` is specified.

Standalone Mode

```
execute cleanup ml
```

Variable	Description
`sensor-group-id`	Target sensor group ID (1-100).

execute cleanup netflow_ml

Use this command will clean up all Netflow ML Discovery logs. It also retains the baseline but keeps user feedback.

Syntax

Center Mode

```
exec cleanup netflow_ml [sensor-group-id]
```

This CLIO will clean up all related Netflow ML machine learning baselines if no `sensor-group-id` is specified.

Standalone Mode

```
execute cleanup netflow_ml
```

Variable	Description
sensor-group-id	Target sensor group ID (1-100).

exec cleanup ndr

This command removes logs including NDR related widgets on the Dashboard, NDR logs, and ML Discovery logs, but will keep the ML baseline and feedback.

> Due to some database changes, after upgrading from 7.0.0 to 7.0.1, users will need to run this command to clean up historical NDR log entries. This will clear all NDR, malware and system detection logs.

Syntax

```
execute cleanup (ndr)
```

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 db restore

Use this command to restore the database. This command will also clear the malware counters in the Dashboard.

Syntax

```
execute db restore
```

execute db sample_process_summary

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

Without *<from_date>* and *<to_date>*, the command will output from historical date until today.

Syntax

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

Example results

```
From Date    :12/31/1969
To Date      :03/06/2023
Sample detected                 :5
Distinct sample detected        :1
Sample processed                :5
Distinct sample processed       :1
Sample processing               :0
Distinct sample processing      :0
Distinct attacker IP            :1
Distinct victim IP              :1
```

execute demo

Use this command to enable or disable demo mode.

> Demo Mode is only available on FortiNDR VM.

> Please disable the ndrd daemon by running `exec ndrd off` before enabling demo mode.

Syntax

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

execute device

Use this command to add back a fabric device that has been removed before, or remove an existing fabric device from FortiNDR. This command is only available in Standalone and Sensor modes.

Syntax

```
execute device {add|remove} < Device type ID > <Serial> [VDOM]
```

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 detected-files

Use this command to export the detected files by FortiNDR 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>
```

> For the disk option to work, you have to insert a USB flash drive into the FortiNDR device. Please make sure the flash drive has enough storage.

execute export file-report

Use this command to export the FortiNDR 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 top-queries

Use this command to export the FortiNDR top queries as a zip file with password.

Syntax

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

execute factoryreset

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

The default RAID level depends on the number of disks:

- 2 disks: RAID 1
- 3 disks: RAID 5
- 4, 6, 8, or 12 disks: RAID 10**

Back up your configuration before using this command. This procedure resets all changes you have made to the FortiNDR 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 FortiNDR 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 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 FortiNDR 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 FortiNDR 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.

The default RAID level depends on the number of disks:

- 2 disks: RAID1
- 3 disks: RAID5
- 4, 6, 8, or 12 disks: RAID10

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

Syntax

```
execute factoryreset disk
```

exec filetype-prefilter sniffer

Use this command to set the file type to be processed in sniffer mode.

Syntax

```
execute filetype-prefilter sniffer [file-type-groups]
```

Variable	Description
`<enter>`	Click `Enter` to dump all file types.
`<filetype group>`	The following filetype groups are supported. : • `Executables` • `PDF_documents` • `Office_documents` • `Web_pages>` • `Compressed_archives` • `Flash_files` • `Android_files` • `Mac_files` • ` Linux_files` • `Others` If no file type group is specified all the file types will be processed.

File type group defintions

Executables	CLASS, JAR, AUTOITSCRIPT, E32IMAGE, GENSCRIPT, MSC, HLP, POWERSHELL, ISO, SIS, INF, SISX, EXE, VBS, BAT, UPX, FSG, ASPACK, PETITE, NSIS, AUTOIT, DLL, MSI, DOTNET, INNO, PYTHON
PDF_documents	PDF

`Office_documents`	VSDX, WORDBASIC, WORDML, ACCESS, XML, VBA, MSOFFICE, Hangul_Office, MSOFFICEX, OPENOFFICE, DOC, XLS, PPT, DOCX, XLSX, PPTX, RTF
`Web_pages`	PHP, HTML, JS ,IFRAME, HTA, CSS, LNK, WOFF
`Compressed_archives`	DAA, ZIP, TAR, GZIP, BZIP, BZIP2, RAR, LZH, LZW, ARJ, CAB, _7Z, XZ, EGG, KGB, Z, ACE, XAR
`Flash_files`	SWF
`Android_files`	DEX, APK
`Mac_files`	MACH_O, DMG
`Linux_files`	ELF, PERLSCRIPT, SHELLSCRIPT, CPIO, RPM
`Others`	ACTIVEMIME, MIME, BASE64, BINHEX ,UUE, HOSTS, FATMACH, TNEF, UNICODE, PYARCH, CHM, CRX, THMX, FLAC, XXE, OTF, EMF, GPGEML, REGISTRY, PFILE, CEF, PRC, JAD, COD, JPEG, GIF, TIFF, PNG, BMP, MPEG, MOV, MP3, WMA, WAV, AVI, RM, TOR, HIBUN, SLK

Example

```
execute filetype-prefilter sniffer Executables PDF_documents Office_documents
```

Only the file types in `Executables`,`PDF_documents` and `Office_documents` groups will be processed.

execute file-size-threshold

Use this command to change FortiNDR's maximum file size limit for different daemons. This command is only available in Standalone and Sensor modes. This execute action is persistent after reboot/power-cycle.

Syntax

```
execute file-size-threshold {FortiMail|FortiSandbox|ICAP|OFTP|inline-blocking|manual-upload|network-
      share|sniffer} <size_limit_1-10240MB>
```

Variable	Description
`FortiMail`	Files sent from FortiMail.
`FortiSandbox`	Files sent from FortiSandbox.
`ICAP`	Files sent from ICAP
`OFTP`	OFTP Devices
`inline-blocking`	Fabric Devices

Variable	Description
manual-upload	Manual uploaded files
network-share	Network share Scan
size_limit	1 to 10240MB (i.e. 10GB)
sniffer	Network Traffic Sniffer

execute formatdatadisk

Use this command to format the local hard disk that contains ML (Machine Learning), ANN (Artificial Neural Network) training data as well as NDR and malware detection history.

Formatting the disk will wipe and reset the database from scratch.

Syntax

```
execute formatdatadisk
```

execute formatlogdisk

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

> ⚠️ 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 learner

Use this command to enable or disable FortiNDR learners. This command is available in Standalone and Center modes only.

Syntax

```
execute learner {on|off}
```

execute netflow

Use this command to turn the Netflow listening feature on/off. If the listening feature turned off, FortiNDR will not consume any Netflow data. By default, this setting is enabled. This command is only available in Standalone and Sensor modes.

Syntax

```
execute netflow <on/off>
```

execute ndrd

Turn off NDRD to disable NDR engine in sniffer mode. This will result in no NDR detection/log (however AV/ANN malware file analysis can still run on FortiNDR). This command is only available in Standalone and Sensor modes.

Syntax

```
execute ndrd <on|off>
```

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 FortiNDR and 10.0.0.1.

execute raidlevel

Use this command to reset the RAID level, partition the disk, and optionally encrypt the disk if supported.

Executing this command will erase all existing data on the RAID array.

Syntax

```
execute raidlevel <raid-level-option> [encryption <security_key>]
```

Variable	Description	Default
`<raid-level-option>`	Enter a raid level, such as 1 or 10. Click Tab to show optional level values.	
`[encryption <security_ key>]`	Encrypt the disk and set the security key. Key value should be a combination of numbers, uppercase letters, lowercase letters, and selected special characters. Its length should be between 8 and 32. Selected special characters are ! # $ % * + , - . : = @ [ ] ^ - _ { } ~. **Note**: This option is only available in FNDR 1000F, FNDR 2500G and FNDR 3600G.	

Support in FortiNDR 1000F

For FortiNDR 1000F, use the CLI command `diagnose system raid-status-detail` to verify if it supports the encryption feature. In the CLI output, you need to see:

```
Enterprise Key Management:
==========================
Capability = Supported
```

If this is not present, please contact Fortinet to obtain a hardware key to enable this feature.

execute raidrebuild start

Use this command to enable RAID rebuilding.Rebuild UBad or UGood disks if detected. This command is supported in FNDR 1000F, FNDR 2500G and FNDR 3600G.

Syntax

```
execute raidrebuild start
```

execute raidrebuild status

Use this command to track RAID progress. This command is supported in FNDR 1000F, FNDR 2500G and FNDR 3600G.

Syntax

```
execute raidrebuild status
```

execute reboot force

Use this command to immediately reboot the system without syncing or unmounting your disks.

Syntax

```
execute reboot force
```

execute reboot

Use this command to restart FortiNDR.

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 FortiNDR 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 reset-ml-baseline-time

Use this command to set the FortiNDR (NDR And Netflow) Machine Learning (ML) baseline training time or to reset it to the default. The default training time is 604800 seconds (7 days). To reset all baseline training time back to the default, use the command without any options. This command is available in Standalone and Center modes only.

Syntax

Center Mode

```
exec reset-ml-baseline-time module-name [sensor-group-id] [new-training-time-in-seconds]
```

Standalone Mode

```
exec reset-ml-baseline-time module-name [new-training-time-in-seconds]
```

Option	Description
module-name	ndr or netflow
new-training-time-in [1]seconds	Enter a value between 120 - 2592000.
sensor-group-id	Target sensor group ID (1-100).

Examples

Set all baseline training time back to default for ndr:

```
exec reset-ml-baseline-time ndr
```

Set baseline training time for a sensor group to one day for netflow:

```
exec reset-ml-baseline-time netflow 55 86400
```

execute restore avdb

Use this command to restore, upgrade, or downgrade the anti-virus database.

Syntax

```
exec restore avdb [disk/tftp/ftp] filename
```

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 FortiNDR 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 FortiNDR 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 FortiNDR unit to its firmware/factory default configuration. For information on installing firmware via TFTP boot interrupt, see the FortiNDR 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 FortiNDR 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 FortiNDR 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 iotdb

Use this command to restore, upgrade, or downgrade the FortiNDR IOT database. This command replaces the existing IOT database.

Syntax

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

Variable	Description
`<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 restore ipsdb

Use this command to restore, upgrade, or downgrade the network attacks, botnet and JA3 encrypted attacks DB, these are packaged into one DB available from support website.

> This CLI is only available on FortiNDR hardware models.
> This CLI might take a long time to complete depending on the size of the database. We recommend using `execute snifferd on/off` and `exec ndrd on/off` to turn the daemons OFF to save memory before backing up.

Syntax

```
exec restore ipsdb [disk/tftp/ftp] filename
```

execute restore kdb

Use this command to restore, upgrade, or downgrade the FortiNDR 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 restore otsdb

Use this command to restore, upgrade, or downgrade the FortiNDR OT Threat and OT App database. This command replaces the existing OT databases.

> A SCADA/OT license is required to download the database from support.fortinet.com.

Syntax

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

Variable	Description
`<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 restore system-db ml-baseline

Use this command to restore FortiNDR Machine Learning (ML) baseline information in Standalone or Center mode.

Sytnax

```
execute restore system-db ml-baseline {disk|scp|ftp|tftp} <filename-to-be-saved> <server>[:ftp port]
      <user-name> <password>
```

Variable	Description
`disk`	The local disk.
`ftp`	The FTP server.
`scp`	The SCP server.
`tftp`	The TFTP server.

execute restore system-db network-share-config

Use this command to to restore network share configurations in standalone or sensor mode.

Sytnax

```
execute restore system-db network-share-config {disk|scp|ftp|tftp} <filename-to-be-saved> <server>
      [:ftp port] <user-name> <password>
```

Variable	Description
disk	The local disk.
ftp	The FTP server.
scp	The SCP server.
tftp	The TFTP server.

execute shutdown

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

⚠️ Power off the FortiNDR unit only after issuing this command. Unplugging or switching off the FortiNDR 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 snifferd

Turn off to disable sniffer as input for file analysis (AV and ANN) in FortiNDR.

> Manual submission, HTTP2 and OFTP will still work as file input sources.

Syntax

```
execute snifferd <on|off>
```

execute ssh

Use this command as the Linux `ssh` command.

Syntax

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

execute tac report

Use this command to generate log information used for debugging by running a list of CLI commands. This command runs a predefined set of CLI commands to collect debug logs.

Syntax

```
execute tac report
```

Runs a predefined set of CLI commands to collect debug logs.

Pre-defined CLI commands:

```
get system status
get system performance
show system interface
show full-configuration system dns
show full-configuration system global
diagnose hardware sysinfo
diagnose hardware sensorinfo
diagnose debug crashlog 7
diagnose debug database error-log
diagnose debug kernel display
diagnose fds list
```

```
diagnose kdb
diagnose query ioc
diagnose query wf
diagnose system top 5 25 1
diagnose system top-fd 10
diagnose system db
diagnose system disk-usage system-data
diagnose system disk-usage system-db
diagnose system disk-usage system-temp-data
diagnose debug application sync lines 10000
diagnose debug application tgm lines 10000
diagnose debug application pcapcleanerd lines 10000
diagnose debug application ctrl lines 10000
```

The TAC report may be too long and overflow the terminal buffer. To resolve this, run the CLI using PuTTY with the following settings:

1. Open PuTTY, without opening the session.
2. In the left-hand menu, go to *Window* and set *Lines of scrollback* to a larger value (e.g., 100000).
3. Go to *Session > Logging*:
   a. Select *All session output*.
   b. Specify a log file name and path (e.g., `C:\Users\...\Downloads\putty-log.txt`).
4. (Optional) To save these settings for future use:
   a. Go to *Session > Saved Sessions*.
   b. Enter a session name and click *Save*.
5. On the *Session* page:
   a. Enter the *Host Name (IP address)*.
   b. Click *Open* to start the session.

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 FortiNDR and another network device, and display information about the time required for network hops between FortiNDR 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 FortiNDR 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 traceroute 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 FortiNDR and example.com. However, FortiNDR cannot trace the route because the primary or secondary DNS server that FortiNDR 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 FortiNDR 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 FortiNDR 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]
```

FORTINET

www.fortinet.com