FortiOS - REST API Reference

VERSION 5.2.14

FORTINET DOCUMENT LIBRARY

https://docs.fortinet.com

FORTINET VIDEO GUIDE

https://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM

https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE

https://training.fortinet.com

FORTIGUARD CENTER

https://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

July 18, 2019

FortiOS 5.2.14 REST API Reference

01-5214-270937-20190718

TABLE OF CONTENTS

Change Log

Date	Change Description
2019-07-18	Updated for version 5.2.14.

Introduction

This document provides the REST API information supported in FortiOS 5.2.14. This document covers a reference of the REST API supported by the FortiOS GUI.

FortiOS 5.2.14 supports the following REST APIs:

- CMDB API
  - Retrieve object meta data (default, schema)
  - Retrieve object/table (with filter, format, start, count, other flags)
  - Create object
  - Modify object
  - Delete object
  - Clone object
  - Move object
- Monitor API
  - Retrieve/Reset endpoint stats (with filter, start, count)
  - Perform endpoint operations
  - Upgrade/Downgrade firmware
  - Restart/Shutdown FGT

Authentication

All requests to FortiOS REST APIs require:

- Valid authentication cookie
- Valid CSRF token for write requests (HTTP POST/PUT/DELETE)
- Appropriate admin profile permission to access the requested resource

Authentication Cookie

Authentication cookie (APSCOOKIE) is provided by the API after a successful login request. All subsequent requests must include this cookie to be authorized by the API. Any request without the cookie or with mismatched cookie will be denied access to the API.

CSRF Tokens

Cross-Site Request Forgery (CSRF) Tokens are alphanumeric values that are passed back-and-forth between client and server to ensure that a user's form submission does not originate from an offsite document.

The CSRF token is available in the session `ccsrftoken` cookie, which must be included in the request header under `X-CSRFTOKEN`.

Read request (`HTTP GET`) does not require CSRF token.

Admin profile permission

Each endpoint requires specific group permission defined in `Access Group` of the endpoint summary table. Request to the endpoint will be checked against this access group to ensure the admin has proper permission to access the resource. Make sure the administrative account you login with has the permissions required to perform the intended actions.

Admin with read-only permission to the resource can only send read requests (`HTTP GET`) to the resource. Admin with write permission to the resource can send read/write requests (`HTTP GET/POST/PUT/DELETE`) to the resource. Admin with no permission to the resource cannot access the resource.

Request with insufficient profile permission will return 403 error.

Setting Up an Authenticated Session

To setup an authenticated session, make a POST request to the login request handler with your username and password. The POST names for these fields are `username` and `secretkey`, respectively.

Login URL	/logincheck
Body data Username	username
Body data Password	secretkey

Logging out of an Authenticated Session

Authenticated sessions remain active until either explicitly logged out, or the session has been inactive for the number of minutes defined in the `admin timeout` setting under `config system global`. If you do not log out of a session when you are finished using the API, it will occupy one of the connection slots on the FortiGate, and may result in denied logins later on.

To log out, a POST request to the /logout URL will remove the current session.

Logout URL	/logout
Body data	none needed

Supported HTTP methods

FortiOS Rest APIs support the following HTTP methods:

HTTP Method	Description
GET	Retrieve a resource or collection of resources.
POST	Create a resource or execute actions.
PUT	Update a resource.
DELETE	Delete a resource or collection of resources.

For any action other than GET, a CSRF token must be provided to the API. If the request is submitted using HTTP POST, the HTTP method can also be overridden using the `X-HTTP-Method-Override` HTTP header.

Response codes

FortiOS APIs use well-defined HTTP status codes to indicate query results to the API.

The following table shows how some of the HTTP status codes are used in the context of FortiOS APIs:

HTTP Response Code	Description
200 - OK	Request returns successful.
400 - Bad Request	Request cannot be processed by the API.
403 - Forbidden	Request is missing CSRF token or administrator is missing access profile permissions.
404 - Resource Not Found	Unable to find the specified resource.
405 - Method Not Allowed	Specified HTTP method is not allowed for this resource.
413 - Request Entity Too Large	Request cannot be processed due to large entity.
424 - Failed Dependency	Fail dependency can be duplicate resource, invalid attribute value.
500 - Internal Server Error	Internal error when processing the request.

Debugging

Verbose debug output can be enabled in the FortiGate CLI with the following commands:

```
diagnose debug enable
diagnose debug application httpsd -1
```

This will produce the following output when the REST API for IPv4 policy statistics is queried:

```
[httpsd 228 - 1418751787] http_config.c[558] ap_invoke_handler -- new request
    (handler='api_monitor_v2-handler', uri='/api/v2/monitor/firewall/policy',
    method='GET')
[httpsd 228 - 1418751787] http_config.c[562] ap_invoke_handler -- User-Agent: Mozilla/5.0
    (Macintosh; Intel Mac OS X 10_10_1) AppleWebKit/537.36 (KHTML, like Gecko)
    Chrome/39.0.2171.71 Safari/537.36
[httpsd 228 - 1418751787] http_config.c[565] ap_invoke_handler -- Source:
    192.168.1.100:56256 Destination: 192.168.1.99:443
[httpsd 228 - 1418751787] api_monitor.c[1427] api_monitor_v2_handler -- received api_
    monitor_v2_request from '192.168.1.100'
[httpsd 228 - 1418751787] aps_access.c[3652] aps_chk_rolebased_perm -- truncated URI
    (/api/v2/monitor/firewall/policy) to (/api/v2/monitor) for permission check
[httpsd 228 - 1418751787] api_monitor.c[1265] handle_req_v2_vdom -- attempting to change
    from vdom "root" to vdom "root"
[httpsd 228 - 1418751787] api_monitor.c[1280] handle_req_v2_vdom -- new API request
    (action='select',path='firewall',name='policy',vdom='root',user='admin')
[httpsd 228 - 1418751787] api_monitor.c[1286] handle_req_v2_vdom -- returning to original
    vdom "root"
[httpsd 228 - 1418751787] http_config.c[581] ap_invoke_handler -- request completed
    (handler='api_monitor_v2-handler' result==0)
```

This debug will also include all requests to/from the FortiOS web interface, in addition to REST API requests.

CMDB API

CMDB API is used to retrieve and modify CLI configurations. For example, create/edit/delete firewall policy.

URL path

All CMDB requests start with `/api/v2/cmdb/`. Below is the format of CMDB URL path.

```
/api/v2/cmdb/<path>/<name>/<mkey>(optional)/
```

CMDB URL path follows CLI commands syntax with an exception of vdom configuration.

CLI Command	path	name	mkey	URL
configure vdom	system	vdom		/api/v2/cmdb/system/vdom/
configure vdom, edit vdom1	system	vdom	vdom1	/api/v2/cmdb/system/vdom/vdom1/
configure firewall policy	firewall	policy		/api/v2/cmdb/firewall/policy/
configure firewall policy, edit 1	firewall	policy	1	/api/v2/cmdb/firewall/policy/1/
configure firewall schedule recurring	firewall.schedule	recurring		/api/v2/cmdb/firewall.schedule/recurring/

For operations on the entire table, mkey is not needed. For instance, add new entry, get all entries, purge table.

For operations on a specific resource, mkey is required. For example, edit/delete/clone/move a firewall policy.

URL Parameters

In addition to the URL path, user can specify URL parameters which are appended to the URL path.

Generic Parameters

The following URL parameters are generic to all CMDB requests.

URL parameter	Example	Description
vdom=root	GET /api/v2/cmdb/firewall/address/?vdom=root	Return result/apply changes on the specified vdom. If vdom parameter is not provided, use current vdom instead. If admin does not have access to the vdom, return permission error.
global=1	GET /api/v2/cmdb/firewall/address/?global=1	Return a list of results/apply changes on all provisioned vdoms. The request is only applicable to vdoms that the admin has access to.

Specific Parameters

Each CMDB method may require extra URL parameters which are unique to the method. Those extra parameters are documented in the `Extra Parameters` section of each CMDB method.

Below are some examples.

URL parameter	Example	Description
action=schema	GET /api/v2/cmdb/firewall/policy/?action=schema	Return schema of the resource table
action=default	GET /api/v2/cmdb/firewall/policy/?action=default	Return default attributes of the resource
action=move	PUT /api/v2/cmdb/firewall/policy/1/?action=move&after=2	Move policy 1 to after policy 2
action=clone	POST /api/v2/cmdb/firewall/address/address1/?action=clone&nkey=address1_clone	Clone 'address1' to 'address1_clone'

URL parameter	Example	Description
skip=1	GET /api/v2/cmdb/firewall/policy/?skip=1	Return a list of all firewall policy but only show relevant attributes
skip=1	GET /api/v2/cmdb/firewall/policy/1/?skip=1	Return firewall policy 1 but only show relevant attributes
format=policyid|action	GET /api/v2/cmdb/firewall/policy/?format=policyid|action	Return a list of all firewall policy, however, only show policyid and action for each policy
format=policyid|action	GET /api/v2/cmdb/firewall/policy/1?format=policyid|action	Return firewall policy 1, however, only show policyid and action
start=0&count=10	GET /api/v2/cmdb/firewall/address/?start=0&count=10	Return the first 10 firewall addresses
key=type&pattern=fqdn	GET /api/v2/cmdb/firewall/address/?key=type&pattern=fqdn	Return all addresses with type fqdn

Body data

Beside URL parameters, some POST/PUT requests also require body data, which must be included in the HTTP body. For example, to create/edit firewall address object, user needs to specify the new/edit data.

GET/DELETE requests do not accept body data.

Request	Body data	Description
POST /api/v2/cmdb/firewall/address?vdom=root	{'name':"address1", 'type': "ipmask", 'subnet': "1.1.1.0 255.255.255.0"}	create new firewall address with the specified data
PUT /api/v2/cmdb/firewall/address/address1?vdom=root	{'subnet': "2.2.2.0 255.255.255.0"}	edit firewall address with the specified data

List of Methods

Type	HTTP Method	Action	Summary
collection	GET		Select all entries in a CLI table.
resource	GET	default	Return the CLI default values for this object type.
resource	GET	schema	Return the CLI schema for this object type.
collection	DELETE		Delete all objects in this table.
collection	POST		Create an object in this table.
resource	GET		Select a specific entry from a CLI table.
resource	PUT		Update this specific resource.
resource	PUT	move	Move this specific resource.
resource	POST	clone	Clone this specific resource.
resource	DELETE		Delete this specific resource.

collection

GET

Summary	Select all entries in a CLI table.
HTTP Method	GET
ETag Caching	Enabled
Response Type	array

Extra parameters

Name	Type	Summary	Required
datasource	int	Enable to include datasource information for each linked object.	No
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	No
with_meta	int	Enable to include meta information about each object (type id, references, etc).	No
skip	int	Enable to call CLI skip operator to hide skipped properties.	No
format	string	List of property names to include in results, separated by | (i.e. policyid|srcintf).	No
key	string	If present, objects will be filtered on property with this name.	No
pattern	string	If present, objects will be filtered on property with this value.	No

resource

GET: default

Summary	Return the CLI default values for this object type.
HTTP Method	GET
ETag Caching	Enabled
Response Type	object

GET: schema

Summary	Return the CLI schema for this object type.
HTTP Method	GET
ETag Caching	Enabled
Response Type	object

collection

DELETE

Summary	Delete all objects in this table.
HTTP Method	DELETE

POST

Summary	Create an object in this table.
HTTP Method	POST

resource

GET

Summary	Select a specific entry from a CLI table.
HTTP Method	GET
ETag Caching	Enabled
Response Type	array

Extra parameters

Name	Type	Summary	Required
datasource	int	Enable to include datasource information for each linked object.	No

Name	Type	Summary	Required
with_meta	int	Enable to include meta information about each object (type id, references, etc).	No
skip	int	Enable to call CLI skip operator to hide skipped properties.	No
format	string	List of property names to include in results, separated by | (i.e. policyid|srcintf).	No

PUT

Summary	Update this specific resource.
HTTP Method	PUT

PUT: move

Summary	Move this specific resource.
HTTP Method	PUT

Extra parameters

Name	Type	Summary	Required
before	string	The ID of the resource that this resource will be moved before.	No
after	string	The ID of the resource that this resource will be moved after.	No

POST: clone

Summary	Clone this specific resource.
HTTP Method	POST

Extra parameters

Name	Type	Summary	Required
nkey	string	The ID for the new resouce to be created.	No

DELETE

Summary	Delete this specific resource.
HTTP Method	DELETE

Examples

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/firewall/address	?action=schema		Retrieve firewall address object's schema
GET	/api/v2/cmdb/firewall/address	?action=default		Retrieve firewall address object's default
GET	/api/v2/cmdb/firewall/address	?vdom=root		Retrieve all IPv4 firewall addresses, vdom root
GET	/api/v2/cmdb/firewall/address	?vdom=root&start=0&count=10&skip=1		Retrieve the first 10 firewall addresses, skip inapplicable attributes, vdom root
GET	/api/v2/cmdb/firewall/address	?vdom=root&format=name|type		Retrieve all firewall addresses but only show name and type, vdom root
GET	/api/v2/cmdb/firewall/address	?vdom=root&key=type&pattern=fqdn		Retrieve all fqdn firewall addresses, vdom root

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/firewall/address/address1	?action=select&vdom=root		Retrieve only firewall address 'address1', vdom root
POST	/api/v2/cmdb/firewall/address	?vdom=root	{"name":"address1"}	Create firewall address 'address1', vdom root
PUT	/api/v2/cmdb/firewall/address/address1	?vdom=root	{"name":"address2"}	Rename 'address1' to 'address2', vdom root
PUT	/api/v2/cmdb/firewall/address/address1	?vdom=root	{"comment":"test comment"}	Edit 'address1' to update comment 'test comment', vdom root
POST	/api/v2/cmdb/firewall/address/address1	?vdom=root&action=clone&nkey=address1_clone		Clone 'address1' to 'address1_clone', vdom root
PUT	/api/v2/cmdb/firewall/policy/1	?vdom=root&action=move&after=2		Move policy 1 to after policy 2, vdom root
DELETE	/api/v2/cmdb/firewall/address/address1	?vdom=root		Delete firewall address 'address1', vdom root

Method	URL	URL Parameters	Body Data	Description
DELETE	/api/v2/cmdb/firewall/address	?vdom=root		Purge all firewall addresses, vdom root
POST	/api/v2/cmdb/application/list	?vdom=root	{"name":"profile 1"}	Create application list profile1, vdom root
PUT	/api/v2/cmdb/application/list/profile1	?vdom=root	{"entries": [{"id":1},{"id":2}]}	Edit profile1 to create child table 'entries' with 1 and 2, vdom root
PUT	/api/v2/cmdb/application/list/profile1	?vdom=root	{"entries": [{"id":1,"application":[{"id":31236},{"id":31237}]}]}	Edit profile1 to add child object '1' which has child table 'applications', vdom root
GET	/api/v2/cmdb/vpn.ssl/settings	?action=select		Retrieve vpn ssl settings object
GET	/api/v2/cmdb/firewall/address	?global=1		Retrieve all IPv4 firewall addresses, all accessible vdoms

Method	URL	URL Parameters	Body Data	Description
POST	/api/v2/cmdb/firewall/address	?global=1	{"name":"address1"}	Create firewall address 'address1' for all accessible vdoms
DELETE	/api/v2/cmdb/firewall/address/address1	?global=1		Delete firewall address 'address1' for all accessible vdoms

Monitor API

Monitor API is used to perform specific actions on endpoint resources. For example, retrieve/close firewall sessions, restart/shutdown FortiGate.

URL path

All Monitor API requests start with `/api/v2/monitor/`. Below is the format of Monitor URL path.

```
/api/v2/monitor/<uri>/
```

Each Monitor endpoint has a specific URI, which are provided by the URI field of each endpoint.

URI	Full URL	Description
/firewall/policy/	GET /api/v2/monitor/firewall/policy/	List traffic statistics for all IPv4 policies, implicit select action
/firewall/policy/reset	POST /api/v2/monitor/firewall/policy/reset	Reset traffic statistics for all IPv4 policies

URL parameters

In addition to the URL path, user can specify URL parameters which are appended to the URL path.

Generic parameters

The following URL parameters are generic to all Monitor requests.

URL parameter	Example	Description
vdom=root	GET /api/v2/monitor/firewall/policy/?vdom=root	Return result/apply changes on the specified vdom. If vdom parameter is not provided, use current vdom instead. If admin does not have access to the vdom, return permission error.
global=1	GET /api/v2/monitor/firewall/policy/?global=1	Return a list of results/apply changes on all provisioned vdoms. The request is only applicable to vdoms that the admin has access to.

Specific parameters

Each Monitor endpoint may require extra URL parameters which are unique to the endpoint. Those extra parameters are documented in the "Extra Parameters" section of each endpoint.

Below are some examples.

URL parameter	Example	Description
count=-1	GET /api/v2/monitor/firewall/session?count=10	Return all ipv4 firewall sessions
ip_version=ipv6&count=10	GET /api/v2/monitor/firewall/session?ip_version=ipv6&count=10	Return the first 10 ipv6 firewall sessions

Body data

Beside URL parameters, some POST requests also require body data, which must be included in the HTTP body. The extra body data are documented in "Extra Parameters" section of each endpoint.

GET requests do not accept body data.

Below are some examples.

Request	Body Data	Description
POST /api/v2/monitor/firewall/session/close?vdom=root	{'pro': "udp", 'saddr': "192.168.100.110", 'daddr': "96.45.33.73", 'sport': 55933, 'dport': 8888}	Close the specific ipv4 firewall sessions

List of Methods

URI	HTTP Method	Summary
firewall/health/select/	GET	List configured load balance server health monitors.
firewall/local-in/select/	GET	List implicit and explicit local-in firewall policies.
firewall/policy/select/	GET	List traffic statistics for all IPv4 policies.
firewall/policy/reset/	POST	Reset traffic statistics for all IPv4 policies.
firewall/policy/clear_counters/	POST	Reset traffic statistics for one or more IPv4 policies by policy ID.

URI	HTTP Method	Summary
firewall/policy6/select/	GET	List traffic statistics for all IPv6 policies.
firewall/policy6/reset/	POST	Reset traffic statistics for all IPv6 policies.
firewall/policy6/clear_counters/	POST	Reset traffic statistics for one or more IPv6 policies by policy ID.
firewall/session/select/	GET	List all active firewall sessions (optionally filtered).
firewall/session/clear_all/	POST	Immediately clear all active IPv4 and IPv6 sessions.
firewall/session/close/	POST	
firewall/session-top/select/	GET	List of top sessions by specified grouping criteria.
firewall/shaper/select/	GET	List of statistics for configured firewall shapers.
firewall/shaper/reset/	POST	Reset statistics for all configured traffic shapers.
firewall/load-balance/select/	GET	List all firewall load balance servers.
firewall/anomaly/select/	GET	List active IPv4 DoS anomaly meters.
firewall/anomaly6/select/	GET	List active IPv6 DoS anomaly meters.
fortiview/statistics/select/	GET	Retrieve drill-down and summary data for FortiView (both realtime and historical).
fortiview/sandbox-file-details/select/	GET	Retrieve FortiSandbox analysis details for a specific file checksum.
log/stats/select/	GET	Return number of logs sent by category per day for a specific log device.
log/stats/reset/	POST	Reset logging statistics for all log devices.
router/ipv4/select/	GET	List all active IPv4 routing table entries.
router/ipv6/select/	GET	List all active IPv6 routing table entries.
router/statistics/select/	GET	Retrieve routing table statistics, including number of matched routes.
system/dashboard/reboot/	POST	Immediately reboot this device.
system/dashboard/shutdown/	POST	Immediately shutdown this device.

URI	HTTP Method	Summary
system/resource/select/	GET	Retrieve system resource information, including CPU and memory usage.
system/dhcp/select/	GET	Return a list of all DHCP leases, grouped by interface.
system/dhcp/revoke/	POST	Revoke a list of IPv4 leases.
system/firmware/select/	GET	Retrieve a list of firmware images available to use for upgrade on this device.
system/firmware/upgrade/	POST	
system/fsck/start/	POST	Reboot the device and immediately start file system check utility.
system/modem/select/	GET	Retrieve statistics for internal/external configured modem.
system/modem/reset/	POST	Reset statistics for internal/external configured modem.
system/modem/connect/	POST	Trigger a connect for the configured modem.
system/modem/disconnect/	POST	Trigger a disconnect for the configured modem.
system/3g-modem/select/	GET	List all 3G modems available via FortiGuard.
system/sniffer/select/	GET	Return a list of all configured packet captures.
system/sniffer/restart/	POST	Restart specified packet capture.
system/sniffer/start/	POST	Start specified packet capture.
system/sniffer/stop/	POST	Stop specified packet capture.
system/fsw/select/	GET	Retrieve statistics for configured FortiSwitches
system/fsw/update/	POST	
system/interface/select/	GET	Retrieve statistics for all system interfaces.
system/debug/select/	GET	Log debug messages to the console (if enabled).
system/vdom-resource/select/	GET	Retrieve VDOM resource information, including CPU and memory usage.
extender-controller/extender/select/	GET	Retrieve statistics for specific configured FortiExtender units.

URI	HTTP Method	Summary
extender-controller/extender/reset/	POST	
user/firewall/select/	GET	List authenticated firewall users.
user/firewall/deauth/	POST	Deauthenticate all firewall users.
user/banned/select/	GET	Return a list of all banned users by IP.
user/banned/clear_users/	POST	Immediately clear a list of specific banned users by IP.
user/banned/add_users/	POST	Immediately add one or more users to the banned list.
user/banned/clear_all/	POST	Immediately clear all banned users.
user/fortitoken/activate/	POST	Activate a set of FortiTokens by serial number.
user/fortitoken/refresh/	POST	Refresh a set of FortiTokens by serial number.
user/fortitoken/provision/	POST	Provision a set of FortiTokens by serial number.
utm/av/select/	GET	Retrieve AntiVirus statistics.
utm/av/reset/	POST	Reset AntiVirus statistics.
utm/web/select/	GET	Retrieve WebFilter statistics.
utm/web/reset/	POST	Reset WebFilter statistics.
utm/web-cat/select/	GET	Retrieve WebFilter category statistics.
utm/web-cat/reset/	POST	Reset WebFilter category statistics.
utm/email/select/	GET	Retrieve Email Filter statistics.
utm/email/reset/	POST	Reset Email Filter statistics.
utm/dlp/select/	GET	Retrieve DLP statistics.
utm/dlp/reset/	POST	Reset DLP statistics.
utm/rating-lookup/select/	GET	Lookup FortiGuard rating for a specific URL.
utm/app/select/	GET	Retrieve application control statistics.
utm/app/reset/	POST	Reset application control statistics.

URI	HTTP Method	Summary
utm/app-lookup/select/	GET	Query remote FortiFlow database to resolve hosts to application control entries.
webfilter/override/select/	GET	List all administrative and user initiated webfilter overrides.
webfilter/override/delete/	POST	
visibility/device-type-dist/select/	GET	Retrieve a breakdown of detected devices by type.
visibility/device-os-dist/select/	GET	Retrieve a breakdown of detected devices by operating system.
visibility/device-list/select/	GET	Retrieve a list of detected devices.
vpn/ipsec/select/	GET	Return an array of active IPsec VPNs.
vpn/ipsec/tunnel_up/	POST	Bring up a specific IPsec VPN tunnel.
vpn/ipsec/tunnel_down/	POST	Bring down a specific IPsec VPN tunnel.
vpn/ipsec/tunnel_reset_stats/	POST	Reset statistics for a specific IPsec VPN tunnel.
vpn/auto-ipsec/select/	GET	Retrieve a list of all auto-IPsec tunnels.
vpn/auto-ipsec/accept/	POST	
vpn/auto-ipsec/reject/	POST	
vpn/ssl/select/	GET	Retrieve a list of all SSL-VPN sessions and sub-sessions.
vpn/ssl/clean_tunnel/	POST	
vpn/ssl/delete/	POST	
wanopt/peer_stats/select/	GET	Retrieve a list of WAN opt peer statistics.
wanopt/peer_stats/reset/	POST	Reset WAN opt peer statistics.
webcache/stats/select/	GET	Retrieve webcache statistics.
webcache/stats/reset/	POST	Reset all webcache statistics.
wifi/client/select/	GET	Retrieve a list of connected WiFi clients.
wifi/managed_ap/select/	GET	Retrieve a list of managed FortiAPs.

URI	HTTP Method	Summary
wifi/managed_ap/set_status/	POST	
wifi/ap_status/select/	GET	Retrieve statistics for all managed FortiAPs.
wifi/interfering_ap/select/	GET	Retrieve a list of interferring APs for one FortiAP radio.
wifi/euclid/select/	GET	Retrieve presence analytics statistics.
wifi/euclid/reset/	POST	
wifi/rogue_ap/select/	GET	Retrieve a list of detected rogue APs.
wifi/rogue_ap/clear_all/	POST	
wifi/rogue_ap/set_status/	POST	
wifi/rogue_ap/restart/	POST	
wifi/spectrum/select/	GET	Retrieve spectrum analysis information for a specific FortiAP.
wifi/firmware/select/	GET	Retrieve a list of current and recommended firmware for FortiAPs in use.
wifi/meta/select/	GET	Retrieve WiFi related meta data.

firewall

health: select

Summary	List configured load balance server health monitors.
URI	firewall/health/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

local-in: select

Summary	List implicit and explicit local-in firewall policies.
URI	firewall/local-in/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy
Response Type	array

policy: select

Summary	List traffic statistics for all IPv4 policies.
URI	firewall/policy/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

policy: reset

Summary	Reset traffic statistics for all IPv4 policies.
URI	firewall/policy/reset/
HTTP Method	POST
Action	reset
Access Group	fwgrp.policy

policy: clear_counters

Summary	Reset traffic statistics for one or more IPv4 policies by policy ID.
URI	firewall/policy/clear_counters/
HTTP Method	POST
Action	clear_counters
Access Group	fwgrp.policy

Extra parameters

Name	Type	Summary	Required
policy	array	Array of policy IDs to reset.	No
policy	int	Single policy ID to reset.	No

policy6: select

Summary	List traffic statistics for all IPv6 policies.
URI	firewall/policy6/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

policy6: reset

Summary	Reset traffic statistics for all IPv6 policies.
URI	firewall/policy6/reset/
HTTP Method	POST
Action	reset
Access Group	fwgrp.policy

policy6: clear_counters

Summary	Reset traffic statistics for one or more IPv6 policies by policy ID.
URI	firewall/policy6/clear_counters/
HTTP Method	POST
Action	clear_counters
Access Group	fwgrp.policy

Extra parameters

Name	Type	Summary	Required
policy	array	Array of policy IDs to reset.	No
policy	int	Single policy ID to reset.	No

session: select

Summary	List all active firewall sessions (optionally filtered).
URI	firewall/session/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
ip_version	string	IP version [*ipv4 | ipv6 | ipboth].	No
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	Yes
summary	boolean	Enable/disable inclusion of session summary (setup rate, total sessions, etc).	No

session: clear_all

Summary	Immediately clear all active IPv4 and IPv6 sessions.
URI	firewall/session/clear_all/
HTTP Method	POST
Action	clear_all
Access Group	sysgrp
Response Type	int

session: close

Summary	
URI	firewall/session/close/
HTTP Method	POST
Action	close
Access Group	sysgrp

session-top: select

Summary	List of top sessions by specified grouping criteria.
URI	firewall/session-top/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
report_by	string	Criteria to group results by [source*|destination|application|web-category|web-domain].	No
sort_by	string	Criteria to sort results by [bytes|msg-counts].	No
count	int	Maximum number of entries to return.	No
filter	object	A map of filter keys to string values. The key(s) may be src_ interface, source, dst_interface, destination, policyid, application, web_category_id, web_domain.	No
srcintf	string	Filter: by source interface name.	No
source	string	Filter: by source IP.	No
dstintf	string	Filter: by destination interface name.	No
destination	string	Filter: by destination IP.	No

Name	Type	Summary	Required
policyid	int	Filter: by policy ID.	No
application	int	Filter: by application ID.	No
web_ category_id	string	Filter: by webfilter category name.	No
web_domain	string	Filter: by web domain name.	No

shaper: select

Summary	List of statistics for configured firewall shapers.
URI	firewall/shaper/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.others
Response Type	array

shaper: reset

Summary	Reset statistics for all configured traffic shapers.
URI	firewall/shaper/reset/
HTTP Method	POST
Action	reset
Access Group	fwgrp.others

load-balance: select

Summary	List all firewall load balance servers.
URI	firewall/load-balance/select/
HTTP Method	GET
Action	select

Access Group	fwgrp.others
Response Type	array

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	Yes

anomaly: select

Summary	List active IPv4 DoS anomaly meters.
URI	firewall/anomaly/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

anomaly6: select

Summary	List active IPv6 DoS anomaly meters.
URI	firewall/anomaly6/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

fortiview

statistics: select

Summary	Retrieve drill-down and summary data for FortiView (both realtime and historical).
URI	fortiview/statistics/select/

HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
realtime	boolean	Set to true to retrieve realtime results (from kernel).	No
filter	object	A map of filter keys to arrays of values.	No

sandbox-file-details: select

Summary	Retrieve FortiSandbox analysis details for a specific file checksum.
URI	fortiview/sandbox-file-details/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
checksum	string	Checksum of a specific file that has been analyzed by the connected FortiSandbox.	Yes

log

stats: select

Summary	Return number of logs sent by category per day for a specific log device.
URI	log/stats/select/

HTTP Method	GET
Action	select
Access Group	loggrp.data-access
Response Type	array

Extra parameters

Name	Type	Summary	Required
dev	string	Log device [*memory | disk | fortianalyzer | fortiguard].	No

stats: reset

Summary	Reset logging statistics for all log devices.
URI	log/stats/reset/
HTTP Method	POST
Action	reset
Access Group	loggrp.data-access

router

ipv4: select

Summary	List all active IPv4 routing table entries.
URI	router/ipv4/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	Yes
ip_mask	string	Filter: IP/netmask.	No
gateway	string	Filter: gateway.	No
type	string	Filter: route type.	No
interface	string	Filter: interface name.	No

ipv6: select

Summary	List all active IPv6 routing table entries.
URI	router/ipv6/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	Yes
ip_mask	string	Filter: IP/netmask.	No
gateway	string	Filter: gateway.	No
type	string	Filter: route type.	No
interface	string	Filter: interface name.	No

statistics: select

Summary	Retrieve routing table statistics, including number of matched routes.
URI	router/statistics/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
ip_version	int	IP version (4|6). If not present, IPv4 and IPv6 will be returned.	No
ip_mask	string	Filter: IP/netmask.	No
gateway	string	Filter: gateway.	No
type	string	Filter: route type.	No
interface	string	Filter: interface name.	No

system

dashboard: reboot

Summary	Immediately reboot this device.
URI	system/dashboard/reboot/
HTTP Method	POST
Action	reboot
Access Group	sysgrp

dashboard: shutdown

Summary	Immediately shutdown this device.

URI	system/dashboard/shutdown/
HTTP Method	POST
Action	shutdown
Access Group	sysgrp

resource: select

Summary	Retrieve system resource information, including CPU and memory usage.
URI	system/resource/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

dhcp: select

Summary	Return a list of all DHCP leases, grouped by interface.
URI	system/dhcp/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
ipv6	boolean	Include IPv6 DHCP leases in addition to IPv4 leases.	No

dhcp: revoke

Summary	Revoke a list of IPv4 leases.
URI	system/dhcp/revoke/
HTTP Method	POST

Action	revoke
Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
ip	array	List of IPv4 addresses to revoke leases for.	No

firmware: select

Summary	Retrieve a list of firmware images available to use for upgrade on this device.
URI	system/firmware/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

firmware: upgrade

Summary	
URI	system/firmware/upgrade/
HTTP Method	POST
Action	upgrade
Access Group	sysgrp

fsck: start

Summary	Reboot the device and immediately start file system check utility.
URI	system/fsck/start/
HTTP Method	POST
Action	start
Access Group	sysgrp

modem: select

Summary	Retrieve statistics for internal/external configured modem.
URI	system/modem/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

modem: reset

Summary	Reset statistics for internal/external configured modem.
URI	system/modem/reset/
HTTP Method	POST
Action	reset
Access Group	sysgrp

modem: connect

Summary	Trigger a connect for the configured modem.
URI	system/modem/connect/
HTTP Method	POST
Action	connect
Access Group	sysgrp

modem: disconnect

Summary	Trigger a disconnect for the configured modem.
URI	system/modem/disconnect/
HTTP Method	POST
Action	disconnect
Access Group	sysgrp

3g-modem: select

Summary	List all 3G modems available via FortiGuard.
URI	system/3g-modem/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

sniffer: select

Summary	Return a list of all configured packet captures.
URI	system/sniffer/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.packet-capture
Response Type	array

sniffer: restart

Summary	Restart specified packet capture.
URI	system/sniffer/restart/
HTTP Method	POST
Action	restart
Access Group	fwgrp.packet-capture
Response Type	array

Extra parameters

Name	Type	Summary	Required
mkey	int	ID of packet capture entry.	Yes

sniffer: start

Summary	Start specified packet capture.
URI	system/sniffer/start/
HTTP Method	POST
Action	start
Access Group	fwgrp.packet-capture
Response Type	array

Extra parameters

Name	Type	Summary	Required
mkey	int	ID of packet capture entry.	Yes

sniffer: stop

Summary	Stop specified packet capture.
URI	system/sniffer/stop/
HTTP Method	POST
Action	stop
Access Group	fwgrp.packet-capture
Response Type	array

Extra parameters

Name	Type	Summary	Required
mkey	int	ID of packet capture entry.	Yes

fsw: select

Summary	Retrieve statistics for configured FortiSwitches
URI	system/fsw/select/
HTTP Method	GET

Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
fsw_id	string	Filter: FortiSwitch ID.	No

fsw: update

Summary	
URI	system/fsw/update/
HTTP Method	POST
Action	update
Access Group	sysgrp

interface: select

Summary	Retrieve statistics for all system interfaces.
URI	system/interface/select/
HTTP Method	GET
Action	select
Access Group	netgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
interface_name	string	Filter: interface name.	No
include_vlan	boolean	Enable to include VLANs in result list.	No

debug: select

Summary	Log debug messages to the console (if enabled).
URI	system/debug/select/
HTTP Method	GET
Action	select
Access Group	

Extra parameters

Name	Type	Summary	Required
type	string	Type of message.	Yes
msg	string	Message content.	Yes
file	string	File name generating message.	Yes
line	string	Line number in file.	Yes

vdom-resource: select

Summary	Retrieve VDOM resource information, including CPU and memory usage.
URI	system/vdom-resource/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

extender-controller

extender: select

Summary	Retrieve statistics for specific configured FortiExtender units.
URI	extender-controller/extender/select/
HTTP Method	GET

Action	select
Access Group	netgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
id	array	List of FortiExtender IDs to query.	Yes

extender: reset

Summary	
URI	extender-controller/extender/reset/
HTTP Method	POST
Action	reset
Access Group	netgrp

user

firewall: select

Summary	List authenticated firewall users.
URI	user/firewall/select/
HTTP Method	GET
Action	select
Access Group	admingrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No

Name	Type	Summary	Required
count	int	Maximum number of entries to return.	No
ipv4	boolean	Include IPv4 user (default=true).	No
ipv6	boolean	Include IPv6 users.	No

firewall: deauth

Summary	Deauthenticate all firewall users.
URI	user/firewall/deauth/
HTTP Method	POST
Action	deauth
Access Group	admingrp

banned: select

Summary	Return a list of all banned users by IP.
URI	user/banned/select/
HTTP Method	GET
Action	select
Access Group	admingrp

banned: clear_users

Summary	Immediately clear a list of specific banned users by IP.
URI	user/banned/clear_users/
HTTP Method	POST
Action	clear_users
Access Group	admingrp

Extra parameters

Name	Type	Summary	Required
ip_addresses	array	List of banned user IPs to clear. IPv4 and IPv6 addresses are allowed.	Yes

banned: add_users

Summary	Immediately add one or more users to the banned list.
URI	user/banned/add_users/
HTTP Method	POST
Action	add_users
Access Group	admingrp

Extra parameters

Name	Type	Summary	Required
ip_addreses	array	List of IP Addresses to ban. IPv4 and IPv6 addresses are allowed.	Yes
expiry	int	Time until expiry in seconds. 0 for indefinite ban.	No

banned: clear_all

Summary	Immediately clear all banned users.
URI	user/banned/clear_all/
HTTP Method	POST
Action	clear_all
Access Group	admingrp

fortitoken: activate

Summary	Activate a set of FortiTokens by serial number.
URI	user/fortitoken/activate/
HTTP Method	POST

Action	activate
Access Group	authgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
tokens	array	List of FortiToken serial numbers to activate. If omitted, all tokens will be used.	No

fortitoken: refresh

Summary	Refresh a set of FortiTokens by serial number.
URI	user/fortitoken/refresh/
HTTP Method	POST
Action	refresh
Access Group	authgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
tokens	array	List of FortiToken serial numbers to refresh. If omitted, all tokens will be used.	No

fortitoken: provision

Summary	Provision a set of FortiTokens by serial number.
URI	user/fortitoken/provision/
HTTP Method	POST
Action	provision
Access Group	authgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
tokens	array	List of FortiToken serial numbers to provision. If omitted, all tokens will be used.	No

utm

av: select

Summary	Retrieve AntiVirus statistics.
URI	utm/av/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.antivirus

av: reset

Summary	Reset AntiVirus statistics.
URI	utm/av/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.antivirus

web: select

Summary	Retrieve WebFilter statistics.
URI	utm/web/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter

web: reset

Summary	Reset WebFilter statistics.
URI	utm/web/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.webfilter

web-cat: select

Summary	Retrieve WebFilter category statistics.
URI	utm/web-cat/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter

web-cat: reset

Summary	Reset WebFilter category statistics.
URI	utm/web-cat/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.webfilter

email: select

Summary	Retrieve Email Filter statistics.
URI	utm/email/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.spamfilter

email: reset

Summary	Reset Email Filter statistics.
URI	utm/email/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.spamfilter

dlp: select

Summary	Retrieve DLP statistics.
URI	utm/dlp/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.data-loss-prevention
Response Type	array

Extra parameters

Name	Type	Summary	Required
count	int	Maximum number of entries to return.	Yes

dlp: reset

Summary	Reset DLP statistics.
URI	utm/dlp/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.data-loss-prevention

rating-lookup: select

Summary	Lookup FortiGuard rating for a specific URL.

URI	utm/rating-lookup/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter
Response Type	object

Extra parameters

Name	Type	Summary	Required
url	string	URL to query.	Yes
url	array	List of URLs to query.	No

app: select

Summary	Retrieve application control statistics.
URI	utm/app/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.application-control

app: reset

Summary	Reset application control statistics.
URI	utm/app/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.application-control

app-lookup: select

Summary	Query remote FortiFlow database to resolve hosts to application control entries.

URI	utm/app-lookup/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	array

Extra parameters

Name	Type	Summary	Required
hosts	array	List of hosts to resolve.	No
address	string	Destination IP for one host entry.	No
dst_port	int	Destination port for one host entry.	No
protocol	int	Protocol for one host entry.	No

webfilter

override: select

Summary	List all administrative and user initiated webfilter overrides.
URI	webfilter/override/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter

override: delete

Summary	
URI	webfilter/override/delete/
HTTP Method	POST
Action	delete
Access Group	utmgrp.webfilter

visibility

device-type-dist: select

Summary	Retrieve a breakdown of detected devices by type.
URI	visibility/device-type-dist/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
include_joined	string	Include joined devices (devices with more than 1 MAC address).	No

device-os-dist: select

Summary	Retrieve a breakdown of detected devices by operating system.
URI	visibility/device-os-dist/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
include_joined	string	Include joined devices (devices with more than 1 MAC address).	No

device-list: select

Summary	Retrieve a list of detected devices.
URI	visibility/device-list/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
os_name	string	Filter: operating system name.	No
type_name	string	Filter: device type name.	No
include_ joined	string	Include joined devices (devices with more than 1 MAC address).	No

vpn

ipsec: select

Summary	Return an array of active IPsec VPNs.
URI	vpn/ipsec/select/
HTTP Method	GET
Action	select
Access Group	vpngrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
tunnel	string	Filter for a specific IPsec tunnel name.	No

Name	Type	Summary	Required
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	No

ipsec: tunnel_up

Summary	Bring up a specific IPsec VPN tunnel.
URI	vpn/ipsec/tunnel_up/
HTTP Method	POST
Action	tunnel_up
Access Group	vpngrp

Extra parameters

Name	Type	Summary	Required
p1name	string	IPsec phase1 name.	Yes
p2name	string	IPsec phase2 name.	Yes
p2serial	string	IPsec phase2 serial.	No

ipsec: tunnel_down

Summary	Bring down a specific IPsec VPN tunnel.
URI	vpn/ipsec/tunnel_down/
HTTP Method	POST
Action	tunnel_down
Access Group	vpngrp

Extra parameters

Name	Type	Summary	Required
p1name	string	IPsec phase1 name.	Yes
p2name	string	IPsec phase2 name.	Yes
p2serial	string	IPsec phase2 serial.	No

ipsec: tunnel_reset_stats

Summary	Reset statistics for a specific IPsec VPN tunnel.
URI	vpn/ipsec/tunnel_reset_stats/
HTTP Method	POST
Action	tunnel_reset_stats
Access Group	vpngrp

Extra parameters

Name	Type	Summary	Required
p2name	string	IPsec phase2 name.	Yes

auto-ipsec: select

Summary	Retrieve a list of all auto-IPsec tunnels.
URI	vpn/auto-ipsec/select/
HTTP Method	GET
Action	select
Access Group	vpngrp

auto-ipsec: accept

Summary	
URI	vpn/auto-ipsec/accept/
HTTP Method	POST
Action	accept
Access Group	vpngrp

auto-ipsec: reject

Summary	
URI	vpn/auto-ipsec/reject/

HTTP Method	POST
Action	reject
Access Group	vpngrp

ssl: select

Summary	Retrieve a list of all SSL-VPN sessions and sub-sessions.
URI	vpn/ssl/select/
HTTP Method	GET
Action	select
Access Group	vpngrp

ssl: clean_tunnel

Summary	
URI	vpn/ssl/clean_tunnel/
HTTP Method	POST
Action	clean_tunnel
Access Group	vpngrp

ssl: delete

Summary	
URI	vpn/ssl/delete/
HTTP Method	POST
Action	delete
Access Group	vpngrp

wanopt

peer_stats: select

Summary	Retrieve a list of WAN opt peer statistics.
URI	wanopt/peer_stats/select/
HTTP Method	GET
Action	select
Access Group	wanoptgrp

peer_stats: reset

Summary	Reset WAN opt peer statistics.
URI	wanopt/peer_stats/reset/
HTTP Method	POST
Action	reset
Access Group	wanoptgrp

webcache

stats: select

Summary	Retrieve webcache statistics.
URI	webcache/stats/select/
HTTP Method	GET
Action	select
Access Group	wanoptgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
period	string	Statistics period [10min|hour|day|month].	No

stats: reset

Summary	Reset all webcache statistics.
URI	webcache/stats/reset/
HTTP Method	POST
Action	reset
Access Group	wanoptgrp

wifi

client: select

Summary	Retrieve a list of connected WiFi clients.
URI	wifi/client/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	array

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	No
type	string	Request type [all*|fail-login].	No

managed_ap: select

Summary	Retrieve a list of managed FortiAPs.
URI	wifi/managed_ap/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	array

Extra parameters

Name	Type	Summary	Required
wtp_id	string	Filter: single managed FortiAP by ID.	No
incl_local	boolean	Enable to include the local FortiWiFi device in the results.	No

managed_ap: set_status

Summary	
URI	wifi/managed_ap/set_status/
HTTP Method	POST
Action	set_status
Access Group	wifi

ap_status: select

Summary	Retrieve statistics for all managed FortiAPs.
URI	wifi/ap_status/select/
HTTP Method	GET
Action	select
Access Group	wifi

interfering_ap: select

Summary	Retrieve a list of interferring APs for one FortiAP radio.
URI	wifi/interfering_ap/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	array

Extra parameters

Name	Type	Summary	Required
wtp	string	FortiAP ID to query.	Yes
radio	int	Radio ID.	Yes
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	No

euclid: select

Summary	Retrieve presence analytics statistics.
URI	wifi/euclid/select/
HTTP Method	GET
Action	select
Access Group	wifi

euclid: reset

Summary	
URI	wifi/euclid/reset/
HTTP Method	POST
Action	reset
Access Group	wifi

rogue_ap: select

Summary	Retrieve a list of detected rogue APs.
URI	wifi/rogue_ap/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	array

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No
count	int	Maximum number of entries to return.	No

rogue_ap: clear_all

Summary	
URI	wifi/rogue_ap/clear_all/
HTTP Method	POST
Action	clear_all
Access Group	wifi

rogue_ap: set_status

Summary	
URI	wifi/rogue_ap/set_status/
HTTP Method	POST
Action	set_status
Access Group	wifi

rogue_ap: restart

Summary	
URI	wifi/rogue_ap/restart/
HTTP Method	POST
Action	restart
Access Group	wifi

spectrum: select

Summary	Retrieve spectrum analysis information for a specific FortiAP.
URI	wifi/spectrum/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	object

Extra parameters

Name	Type	Summary	Required
wtp_id	string	FortiAP ID to query.	Yes

firmware: select

Summary	Retrieve a list of current and recommended firmware for FortiAPs in use.
URI	wifi/firmware/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	object

Extra parameters

Name	Type	Summary	Required
timeout	string	FortiGuard connection timeout (defaults to 2 seconds).	No

meta: select

Summary	Retrieve WiFi related meta data.
URI	wifi/meta/select/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	object

Examples

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor/firewall/policy	?vdom=root		fwgrp.policy	List traffic statistics for all IPv4 policies, vdom root
GET	/api/v2/monitor/firewall/policy	?global=1		fwgrp.policy	List traffic statistics for all IPv4 policies, all accessible vdoms

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor/firewall/policy/reset	?vdom=root		fwgrp.policy	Reset traffic statistics for all IPv4 policies, vdom root
POST	/api/v2/monitor/firewall/policy/reset	?global=1		fwgrp.policy	Reset traffic statistics for all IPv4 policies, all accessible vdoms
POST	/api/v2/monitor/firewall/policy/clear_counters	?vdom=root	{'policy': 1}	fwgrp.policy	Reset traffic statistics for single IPv4 policy, vdom root
POST	/api/v2/monitor/firewall/policy/clear_counters	?vdom=root	{'policy': [1, 2]}	fwgrp.policy	Reset traffic statistics for multiple IPv4 policies, vdom root
GET	/api/v2/monitor/firewall/session	?vdom=root&ip_version=ipv4&start=0&count=1&summary=True		sysgrp	List the first active ipv4 firewall sessions, vdom root

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor/firewall/session/clear_all	?vdom=root		sysgrp	Immediately clear all active IPv4 and IPv6 sessions, vdom root
POST	/api/v2/monitor/firewall/session/close	?vdom=root	{'pro': "udp", 'saddr': "192.168.100.110", 'daddr': "96.45.33.73", 'sport': 55933, 'dport': 8888}	sysgrp	Immediately close specific session matched with the filter, vdom root
POST	/api/v2/monitor/system/dashboard/reboot			sysgrp	Immediately reboot this device
POST	/api/v2/monitor/system/dashboard/shutdown			sysgrp	Immediately shutdown this device