FortiOS - REST API Reference

VERSION 5.6.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

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

FEEDBACK

Email: techdocs@fortinet.com

March 31, 2017

FortiOS 5.6.0 REST API Reference

01-560-414177-20170331

TABLE OF CONTENTS

Change Log

Date	Change Description
2017-03-31	Initial release.

Introduction

This document provides the REST API information supported in FortiOS 5.6.0. This document covers a reference of the REST API supported by the FortiOS GUI.

FortiOS 5.6.0 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
  - Upload/Download file
  - Restore/Backup config
  - Upgrade/Downgrade firmware
  - Restart/Shutdown FGT

What's New in the REST API

FortiOS 5.6.0 includes minor updates and bug fixes, including:

- Added support for various new Monitor APIs
- Fixed minor bugs

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 (HTTP 401 error code).

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`. See test script sample for how to handle CSRF token.

A 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.

A 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 `admintimeout` 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 REST APIs.

HTTP Response Code	Description
200 - OK	Request returns successful.
400 - Bad Request	Request cannot be processed by the API.
401 - Not Authorized	Request without successful login session.
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.

HTTP Response Code	Description
424 - Failed Dependency	Fail dependency can be duplicate resource, missing required parameter, missing required attribute, 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)/<child_name>(optional)/<child_mkey>
    (optional)/
```

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

CLI Command	path	name	mkey	child_ name	child_ mkey	Full 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 schedule recurring	firewall. schedule	recurring				/api/v2/cmdb/ firewall.schedule/recurring/
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 policy, edit 1, set srcintf	firewall	policy	1	srcintf		/api/v2/cmdb/firewall/ policy/1/srcintf/
configure firewall policy, edit 1, delete srcintf lan	firewall	policy	1	srcintf	lan	/api/v2/cmdb/firewall/ policy/1/srcintf/lan/

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.

For operations on the child table, child_name is required. For example, retrieve child table, purge child table, add new entry to child table.

For operations on the child table entry, child_mkey is required. For example, delete/move child object.

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'
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

URL parameter	Example	Description
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
filter=type==fqdn	GET /api/v2/cmdb/firewall/address /?filter=type==fqdn	Return all addresses with type fqdn
filter=type== fqdn,type==ipmask&filter= visibility==enable	GET /api/v2/cmdb/firewall/address /?filter=type==fqdn,type== ipmask&filter=visibility==enable	Return all addresses with type fqdn or ipmask which has visibility enabled

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

Limitation

If the body data has the same name as some reserved URL parameters, such as name, path, or action, the request would fail due to the conflict. For example, firewall policy has 'name' and 'action' attribute which conflict with the reserved URL parameter 'name' and 'action'. POST/PUT with normal method would fail with 405 error. A workaround is to enclosed all object data in a 'json' keyword so the API can correctly identify object data. For example:

Request	Body data	Description
POST /api/v2/cmdb /firewall/policy? vdom=root	{'name':"test_policy", 'srcintf': [{"name":"port1"}], 'dstintf': [{"name":"port2"}],'srcaddr': [{"name":"all"}],'dstaddr': [{"name":"all"}],'action':"accept",'status':"enable", 'schedule':"always",'service':[{'name':"ALL"}],'nat':"disable"}	This would fail with 405 error

Request	Body data	Description
POST /api/v2/cmdb /firewall/policy? vdom=root	{'json':{'name':"test_policy", 'srcintf': [{"name":"port1"}], 'dstintf': [{"name":"port2"}],'srcaddr': [{"name":"all"}], 'dstaddr': [{"name":"all"}],'action':"accept",'status': "enable",'schedule':"always",'service':[{'name':"ALL"}], 'nat':"disable"}}	This would work

Filter with multiple key/value pairs

Filtering multiple key/value pairs are also supported for all CMDB retrieval requests via 'filter' URL parameter.

Filter Syntax

Filters are defined in the following syntax: *key operator pattern*

Key	Operator	Pattern	Full Request	Description
schedule	==	always	GET /api/v2/cmdb/firewall/policy /?filter=schedule==always	Only return firewall policy with schedule 'always'
schedule	!=	always	GET /api/v2/cmdb/firewall/policy /?filter=schedule!=always	Return all firewall policy with schedule other than 'always'

Filter Operators

Operator	Description
==	Case insensitive match with pattern.
!=	Does not match with pattern (case insensitive).
=@	Pattern found in object value (case insensitive).
!@	Pattern not found in object value (case insensitive).
<=	Value must be less than or equal to pattern.
<	Value must be less than pattern.
>=	Value must be greater than or equal to pattern.
>	Value must be greater than pattern.

Combining Filters

Filters can be combined to create complex queries.

Combination	Description	Example
Logical OR	Separate filters using commas ",". The following example returns all policies using the always schedule or the once schedule.	GET /api/v2/cmdb/firewall /policy?filter=schedule== always,schedule==once
Logical AND	Filter strings can be combined to create logical AND queries by including multiple filters in the request. This example includes all policies using schedule always AND action accept.	GET /api/v2/cmdb/firewall /policy/?filter=schedule== always&filter=action==accept
Combining AND and OR	You can combine AND and OR filters together to create more complex filters. This example includes all policies using schedule always AND action accept OR action deny.	GET /api/v2/cmdb/firewall /policy/?filter=schedule== always&filter=action==accept, action==deny

Reserved Characters

The following characters need to be escaped if they are part of a filter pattern.

Character	Escaped Value
,	\,
\	\\

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	default	Return the CLI default values for entire CLI tree.
resource	GET	schema	Return the CLI schema for this object type.
resource	GET	schema	Return schema for entire CLI tree.
collection	DELETE		Delete all objects in this table.

Type	HTTP Method	Action	Summary
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.
resource	GET		Build API directory.

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	boolean	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	boolean	Enable to include meta information about each object (type id, references, etc).	No
skip	boolean	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

Name	Type	Summary	Required
filter	string	Comma separated list of key value pairs to filter on. Filters will be logically OR'd together.	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: default

Summary	Return the CLI default values for entire CLI tree.
HTTP Method	GET
Response Type	object

GET: schema

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

GET: schema

Summary	Return schema for entire CLI tree.
HTTP Method	GET
Response Type	object

DELETE

Summary	Delete all objects in this table.
HTTP Method	DELETE

POST

Summary	Create an object in this table.
HTTP Method	POST

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	boolean	Enable to include datasource information for each linked object.	No
with_meta	boolean	Enable to include meta information about each object (type id, references, etc).	No
skip	boolean	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

GET

Summary	Build API directory.
HTTP Method	GET

Examples

Retrieve table

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/firewall/address	?vdom=root		Retrieve all IPv4 firewall addresses, vdom root

Method	URL	URL Parameters	Body Data	Description
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
GET	/api/v2/cmdb/firewall/address	?vdom=root&filter=type==fqdn		Retrieve all fqdn firewall addresses, vdom root
GET	/api/v2/cmdb/firewall/address	?vdom=root&filter=type==fqdn,type==iprange		Retrieve all fqdn or iprange firewall addresses, vdom root
GET	/api/v2/cmdb/firewall/address	?vdom=root&filter=type==fqdn&filter=associated-interface==lan		Retrieve all fqdn firewall addresses that belong to lan interface, vdom root

Retrieve table schema

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/firewall/address	?action=schema		Retrieve firewall address object's schema

Retrieve table default

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/firewall/address	?action=default		Retrieve firewall address object's default

Purge table

Method	URL	URL Parameters	Body Data	Description
DELETE	/api/v2/cmdb/firewall/address	?vdom=root		Purge all firewall addresses, vdom root

Retrieve object

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

Create object

Method	URL	URL Parameters	Body Data	Description
POST	/api/v2/cmdb/firewall/address	?vdom=root	{"name":"address1"}	Create firewall address 'address1', root vdom
POST	/api/v2/cmdb/application/list	?vdom=root	{"name":"profile1"}	Create application list profile1, vdom root

Edit object

Method	URL	URL Parameters	Body Data	Description
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
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

Delete object

Method	URL	URL Parameters	Body Data	Description
DELETE	/api/v2/cmdb/firewall/address/address1	?vdom=root		Delete firewall address 'address1', root vdom

Clone object

Method	URL	URL Parameters	Body Data	Description
POST	/api/v2/cmdb/firewall/address/address1	?vdom=root&action=clone&nkey=address1_clone		Clone 'address1' to 'address1_clone', root vdom

Move object

Method	URL	URL Parameters	Body Data	Description
PUT	/api/v2/cmdb/firewall/policy/1	?vdom=root&action=move&after=2		Move policy 1 to after policy 2, root vdom

Append child object

Method	URL	URL Parameters	Body Data	Description
POST	/api/v2/cmdb/application/list/profile1/entries	?vdom=root	{"id":3}	Add 3 to application profile1 child table entries, vdom root

Edit child object

Method	URL	URL Parameters	Body Data	Description
PUT	/api/v2/cmdb/application/list/profile1/entries/3	?vdom=root	{"application":[{"id":31236},{"id":31237}]}	Edit child entry 3 to update child application list, vdom root

Delete child object

Method	URL	URL Parameters	Body Data	Description
DELETE	/api/v2/cmdb/application/list/profile1/entries/3	?vdom=root		Delete 3 from application profile1 child table entries, vdom root

Purge child table

Method	URL	URL Parameters	Body Data	Description
DELETE	/api/v2/cmdb/application /list/profile1/entries	?vdom=root		Purge application profile1 child table entries, vdom root

Retrieve complex table

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/vpn.ssl/settings	?action=select		Retrieve vpn ssl settings object

Edit complex table

Method	URL	URL Parameters	Body Data	Description
PUT	/api/v2/cmdb/ vpn.ssl/settings	?vdom=root	{"authentication-rule":[{"id":"1"}, {"id":"2"}]}	Edit complex object vpn.ssl.settings to create/modify child table, vdom root

Global requests (apply to all accessible vdoms)

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb/ firewall/address	?global=1		Retrieve all IPv4 firewall addresses, all accessible vdoms
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 FGT, backup/restore config file.

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
/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.

Required parameters are marked with "required: true" flag.

Below are some examples.

URL parameter	Example	Description
count=-1	GET /api/v2/monitor/firewall/session?count=1	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.

Required body data are marked with "required: true" flag.

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

File upload

File upload is supported for some endpoints. For example, upload VM license, restore config file. The upload file must be stored in the HTTP body. There are two different methods to do so: via JSON data or multi-part file.

File upload via JSON data

The upload file can be encoded directly into the HTTP body as JSON data using the `'file_content'` field.

The JSON data must be encoded in base64 format.

For instance, below is how you can upload/restore config file via JSON data using Python Requests module.

```
self.session.post(url='/api/v2/monitor/system/config/restore',
   params={"vdom": "vdom1"},
   data={"source": "upload",
      "scope": "vdom",
      "file_content": b64encode(open("vd1.conf.txt", "r").read())})
```

File upload via multi-part file

Another way to store upload file in HTTP body is to include it as a multi-part file.

The multi-part file does not need to be encoded in base64 format.

For instance, below is how you can upload/restore config file via multi-part file using Python Requests module.

```
self.session.post(url='/api/v2/monitor/system/config/restore',
   params={"vdom": "vdom1"},
   data={"source": "upload",
      "scope": "vdom"},
   files=[('random_name',
      ('random_conf.conf', open("vd1.conf.txt", "r"), 'text/plain'))])
```

File download

File download is also supported in some endpoints. For example, download CA certificate, backup config file. **The downloaded file is stored in the response's raw content, not JSON data**.

For example, here is the request to download global certificate name `Fortinet_Factory`, type `local`, scope global:

```
GET /api/v2/monitor/system/certificate/download?mkey=Fortinet_
    Factory&type=local&scope=global
```

File download via browser

When sending file download request via a browser, the browser automatically checks the response's header for `'Content-Disposition': attachment`. If present, the browser will download the file to local directory using the name.

File download via script

When sending file download request via a script, the script will need to manually perform the above steps to convert the response's content into a file. For example, the script needs to check the response header for `'Content-Disposition': attachment`, and write the content into a local file with the given name.

List of Methods

URI	HTTP Method	Summary
endpoint-control/profile/xml/	GET	List XML representation for each endpoint-control profile.
endpoint-control/registration-password/check/	POST	Check if provided registration password is valid for current VDOM.
endpoint-control/record-list/select/	GET	List endpoint records.

URI	HTTP Method	Summary
endpoint-control/registration/summary/	GET	Summary of FortiClient registrations.
endpoint-control/registration/quarantine/	POST	Quarantine endpoint by FortiClient UID or MAC.
endpoint-control/registration/unquarantine/	POST	Unquarantine endpoint by FortiClient UID or MAC.
endpoint-control/registration/block/	POST	Block endpoint by FortiClient UID or MAC.
endpoint-control/registration/unblock/	POST	Unblock endpoint by FortiClient UID or MAC.
endpoint-control/registration/deregister/	POST	Deregister endpoint by FortiClient UID or MAC.
endpoint-control/installer/select/	GET	List available FortiClient installers.
endpoint-control/installer/download/	GET	Download a FortiClient installer via FortiGuard.
endpoint-control/avatar/download/	GET	Download an endpoint avatar image.
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/acl/select/	GET	List counters for all IPv4 ACL.
firewall/acl/clear_counters/	POST	Reset counters for one or more IPv4 ACLs by policy ID.
firewall/acl6/select/	GET	List counters for all IPv6 ACL.
firewall/acl6/clear_counters/	POST	Reset counters for one or more IPv6 ACLs by policy ID.
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.
firewall/policy6/select/	GET	List traffic statistics for all IPv6 policies.

URI	HTTP Method	Summary
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/proxy-policy/select/	GET	List traffic statistics for all explicit proxy policies.
firewall/proxy-policy/clear_counters/	POST	Reset traffic statistics for one or more explicit proxy policies by policy ID.
firewall/policy-lookup/select/	GET	Performs a policy lookup by creating a dummy packet and asking the kernel which policy would be hit.
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	Close a specific firewall session that matches all provided criteria.
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/address-fqdns/select/	GET	List of FQDN address objects and the IPs they resolved to.
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.
geoip/geoip-query/select/	GET	Retrieve location details for IPs queried against FortiGuard's geoip service.
ips/rate-based/select/	GET	Returns a list of rate-based signatures in IPS package.
license/status/select/	GET	Get current license and registration status.
license/database/upgrade/	POST	Upgrade IPS database on this device using uploaded file.

URI	HTTP Method	Summary
license/forticare-resellers/select/	GET	Get current FortiCare resellers for the requested country.
license/forticare-org-list/select/	GET	Get FortiCare organization size and industry lists.
log/current-disk-usage/select/	GET	Return current used, free and total disk bytes.
log/device/state/	GET	Retrieve information on state of log devices.
log/forticloud/select/	GET	Return FortiCloud log status.
log/fortianalyzer/select/	GET	Return FortiAnalyzer/FortiManager log status.
log/fortianalyzer-queue/select/	GET	Retrieve information on FortiAnalyzer's queue state. Note:- FortiAnalyzer logs are queued only if upload-option is realtime.
log/hourly-disk-usage/select/	GET	Return historic hourly disk usage in bytes.
log/historic-daily-remote-logs/select/	GET	Returns the amount of logs in bytes sent daily to a remote logging service (FortiCloud or FortiAnalyzer).
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.
log/forticloud-report/download/	GET	Download PDF report from FortiCloud.
log/ips-archive/download/	GET	Download IPS/application control packet capture files. Uses configured log display device.
log/policy-archive/download/	GET	Download policy-based packet capture archive.
log/av-archive/download/	GET	Download file quarantined by AntiVirus.
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.
router/lookup/select/	GET	Performs a route lookup by querying the routing table.
system/admin/toggle-vdom-mode/	POST	Toggles VDOM mode on/off. Enables or disables VDOM mode if it is disabled or enabled respectively.

URI	HTTP Method	Summary
system/config-revision/select/	GET	Returns a list of system configuration revisions.
system/config-revision/update-comments/	POST	Updates comments for a system configuration file.
system/config-revision/delete/	POST	Deletes one or more system configuration revisions.
system/config-revision/file/	GET	Download a specific configuration revision.
system/config-revision/info/	GET	Retrieve meta information for a specific configuration revision.
system/config-revision/save/	POST	Create a new config revision checkpoint.
system/current-admins/select/	GET	Return a list of currently logged in administrators.
system/disconnect-admin-s/select/	POST	Disconnects logged in administrators.
system/time/set/	POST	Sets current system time stamp.
system/time/select/	GET	Gets current system time stamp.
system/os/reboot/	POST	Immediately reboot this device.
system/os/shutdown/	POST	Immediately shutdown this device.
system/vdom-resource/select/	GET	Retrieve VDOM resource information, including CPU and memory usage.
system/dhcp/select/	GET	Returns a list of all DHCP IPv4 and IPv6 DHCP leases.
system/dhcp/revoke/	POST	Revoke IPv4 DHCP leases.
system/dhcp6/revoke/	POST	Revoke IPv6 DHCP leases.
system/firmware/select/	GET	Retrieve a list of firmware images available to use for upgrade on this device.
system/firmware/upgrade/	POST	Upgrade firmware image on this device using uploaded file.
system/fsck/start/	POST	Reboot the device and immediately start file system check utility.
system/storage/select/	GET	Retrieve information for the non-boot disk.

URI	HTTP Method	Summary
system/change-password/select/	POST	Save admin and guest-admin passwords.
system/password-policy-conform/select/	POST	Check whether password conforms to the password policy.
system/csf/select/	GET	Retrieve a full tree of downstream FortiGates registered to the Security Fabric.
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/resource/usage/	GET	Retreive current and historical usage data for a provided resource.
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/sniffer/download/	GET	Download a stored packet capture.
system/fsw/select/	GET	Retrieve statistics for configured FortiSwitches
system/fsw/update/	POST	Update administrative state for a given FortiSwitch (enable or disable authorization).
system/fsw/restart/	POST	Restart a given FortiSwitch.
system/fsw/upgrade/	POST	Upgrade firmware image on the given FortiSwitch using uploaded file.
system/fsw-firmware/select/	GET	Retrieve a list of recommended firmware for managed FortiSwitches.
switch-controller/managed-switch/faceplate-xml/	GET	Retrieve XML for rendering FortiSwitch faceplate widget.

URI	HTTP Method	Summary
system/interface/select/	GET	Retrieve statistics for all system interfaces.
system/available-interfaces/select/	GET	Retrieve a list of all interfaces along with some meta information regarding their availability.
system/available-interfaces/ha/	GET	Retrieve a list of all interfaces along with some meta information regarding their availability. Includes extra meta information useful when dealing with interfaces related to HA configuration. Interfaces that are used by an HA cluster as management interfaces are also included in this view
system/interface-bandwidth/select/	GET	Retrieve bandwidth of all interfaces.
system/acquired-dns/select/	GET	Retrieve a list of interfaces and their acquired DNS servers.
system/resolve-fqdn/select/	GET	Resolves the provided FQDNs to FQDN -> IP mappings.
system/usb-log/select/	GET	Retrieve information about connected USB drives, including estimated log sizes.
system/usb-log/start/	POST	Start backup of logs from current VDOM to USB drive.
system/usb-log/stop/	POST	Stop backup of logs to USB drive.
system/ipconf/select/	GET	Determine if there is an IP conflict for a specific IP using ARP.
system/fortiguard/update/	POST	Immediately update status for FortiGuard services.
system/fortiguard/clear-cache/	POST	Immediately clear all FortiGuard statistics.
system/fortiguard/test-availability/	POST	Test availability of FortiGuard services.
system/fortiguard/server-info/	GET	Get FortiGuard server list and information.
system/fortimanager/status/	GET	Get FortiManager status.
system/fortimanager/config/	POST	Configure FortiManager address.
system/available-certificates/select/	GET	Get available certificates.

URI	HTTP Method	Summary
system/certificate/download/	GET	Download certificate.
system/debug/select/	POST	Log debug messages to the console (if enabled).
system/debug/download/	GET	Download debug report for technical support.
system/com-log/dump/	POST	Dump system com-log to file.
system/com-log/update/	GET	Fetch system com-log file dump progress.
system/com-log/download/	GET	Download com-log file (after file dump is complete).
system/botnet/stat/	GET	Retrieve statistics for FortiGuard botnet database.
system/botnet/select/	GET	List all known IP-based botnet entries in FortiGuard botnet database.
system/botnet-domains/select/	GET	List all known domain-based botnet entries in FortiGuard botnet database.
system/botnet-domains/stat/	GET	List statistics on domain-based botnet entries in FortiGuard botnet database.
system/ha-statistics/select/	GET	List of statistics for members of HA cluster
system/ha-checksums/select/	GET	List of checksums for members of HA cluster
system/ha-peer/select/	GET	Get configuration of peer(s) in HA cluster. Uptime is expressed in seconds.
system/ha-peer/update/	POST	Update configuration of peer in HA cluster.
system/ha-peer/disconnect/	POST	Update configuration of peer in HA cluster.
system/link-monitor/select/	GET	Retrieve per-interface statistics for active link monitors.
system/compliance/run/	POST	Immediately run compliance checks for the selected VDOM.
system/config/restore/	POST	Restore system configuration from uploaded file or from USB.
system/config/backup/	GET	Backup system config
system/config/usb-filelist/	GET	List configuration files available on connected USB drive.

URI	HTTP Method	Summary
system/sandbox/status/	GET	Retrieve sandbox status.
system/sandbox/stats/	GET	Retrieve sandbox statistics.
system/object/usage/	GET	Retrieve all objects that are currently using as well as objects that can use the given object.
system/timezone/select/	GET	Get world timezone and daylight saving time.
system/vmlicense/upload/	POST	Update VM license using uploaded file. Reboots immediately if successful.
system/sensor-info/select/	GET	Retrieve system sensor status.
system/audit/select/	GET	Retrieve Security Fabric audit results.
system/fortiguard-blacklist/select/	GET	Retrieve blacklist information for a specified IP.
extender-controller/extender/select/	GET	Retrieve statistics for specific configured FortiExtender units.
extender-controller/extender/reset/	POST	Reset a specific FortiExtender unit.
user/firewall/select/	GET	List authenticated firewall users.
user/firewall/deauth/	POST	Deauthenticate single, multiple, or 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/select/	GET	List FortiTokens and their status.
user/fortitoken/activate/	POST	Activate a set of FortiTokens by serial number.
user/device/select/	GET	Retrieve a list of detected devices.
user/fortitoken/refresh/	POST	Refresh a set of FortiTokens by serial number.
user/fortitoken/provision/	POST	Provision a set of FortiTokens by serial number.

URI	HTTP Method	Summary
user/fortitoken/send-activation/	POST	Send a FortiToken activation code to a user via SMS or Email.
user/fsso/refresh-server/	POST	Refresh remote agent group list for all fsso agents.
user/fsso/select/	GET	Get a list of fsso and fsso polling status.
utm/rating-lookup/select/	GET	Lookup FortiGuard rating for a specific URL.
utm/app-lookup/select/	GET	Query remote FortiFlow database to resolve hosts to application control entries.
utm/application-categories/select/	GET	Retrieve a list of application control categories.
utm/antivirus/stats/	GET	Retrieve antivirus scanning statistics.
virtual-wan/health-check/select/	GET	Retrieve statistics for each SD-WAN link.
webfilter/override/select/	GET	List all administrative and user initiated webfilter overrides.
webfilter/override/delete/	POST	Delete a configured webfilter override.
webfilter/malicious-urls/select/	GET	List all URLs in FortiSandbox malicious URL database.
webfilter/malicious-urls/stat/	GET	Retrieve statistics for the FortiSandbox malicious URL database.
webfilter/category-quota/select/	GET	Retrieve quota usage statistics for webfilter categories.
webfilter/category-quota/reset/	POST	Reset webfilter quota for user or IP.
webfilter/fortiguard-categories/select/	GET	Return FortiGuard web filter categories.
webfilter/trusted-urls/select/	GET	List all URLs in FortiGuard trusted URL database.
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.

URI	HTTP Method	Summary
vpn/ssl/select/	GET	Retrieve a list of all SSL-VPN sessions and sub-sessions.
vpn/ssl/clear_tunnel/	POST	Remove all active tunnel sessions in current virtual domain.
vpn/ssl/delete/	POST	Terminate the provided SSL-VPN session.
vpn/ssl/stats/	GET	Return statistics about the SSL-VPN.
wanopt/history/select/	GET	Retrieve WAN opt. statistics history.
wanopt/history/reset/	POST	Reset WAN opt. statistics.
wanopt/webcache/select/	GET	Retrieve webcache statistics history.
wanopt/webcache/reset/	POST	Reset webcache statistics.
wanopt/peer_stats/select/	GET	Retrieve a list of WAN opt peer statistics.
wanopt/peer_stats/reset/	POST	Reset WAN opt peer statistics.
webproxy/pacfile/download/	GET	Download webproxy PAC file.
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.
wifi/managed_ap/set_status/	POST	Update administrative state for a given FortiAP (enable or disable authorization).
wifi/firmware/select/	GET	Retrieve a list of current and recommended firmware for FortiAPs in use.
wifi/managed_ap/restart/	POST	Restart a given FortiAP.
wifi/managed_ap/upgrade/	POST	Upgrade firmware image on the given FortiAP using uploaded file.
wifi/ap_status/select/	GET	Retrieve statistics for all managed FortiAPs.
wifi/interfering_ap/select/	GET	Retrieve a list of interfering APs for one FortiAP radio.

URI	HTTP Method	Summary
wifi/euclid/select/	GET	Retrieve presence analytics statistics.
wifi/euclid/reset/	POST	Reset presence analytics statistics.
wifi/rogue_ap/select/	GET	Retrieve a list of detected rogue APs.
wifi/rogue_ap/clear_all/	POST	Clear all detected rogue APs.
wifi/rogue_ap/set_status/	POST	Mark detected APs as rogue APs.
wifi/spectrum/select/	GET	Retrieve spectrum analysis information for a specific FortiAP.
coverage/download/select/	GET	Download code coverage.

endpoint-control

profile: xml

Summary	List XML representation for each endpoint-control profile.
URI	endpoint-control/profile/xml/
HTTP Method	GET
Action	xml
Access Group	endpoint-control-grp
Response Type	array

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of endpoint-control profile.	No

registration-password: check

Summary	Check if provided registration password is valid for current VDOM.
URI	endpoint-control/registration-password/check/

HTTP Method	POST
Action	check
Access Group	endpoint-control-grp
Response Type	boolean

Extra parameters

Name	Type	Summary	Required
password	string	Registration password to test.	Yes

record-list: select

Summary	List endpoint records.
URI	endpoint-control/record-list/select/
HTTP Method	GET
Action	select
Access Group	endpoint-control-grp
Response Type	array

Extra parameters

Name	Type	Summary	Required
intf_name	string	Filter: Name of interface where the endpoint was detected.	No

registration: summary

Summary	Summary of FortiClient registrations.
URI	endpoint-control/registration/summary/
HTTP Method	GET
Action	summary
Access Group	endpoint-control-grp

registration: quarantine

Summary	Quarantine endpoint by FortiClient UID or MAC.
URI	endpoint-control/registration/quarantine/
HTTP Method	POST
Action	quarantine
Access Group	endpoint-control-grp

Extra parameters

Name	Type	Summary	Required
uid	array	Array of FortiClient UIDs to quarantine.	No
uid	string	Single FortiClient UID to quarantine.	No
mac	array	Array of MACs to quarantine.	No
mac	string	Single MAC to quarantine.	No

registration: unquarantine

Summary	Unquarantine endpoint by FortiClient UID or MAC.
URI	endpoint-control/registration/unquarantine/
HTTP Method	POST
Action	unquarantine
Access Group	endpoint-control-grp

Extra parameters

Name	Type	Summary	Required
uid	array	Array of FortiClient UIDs to unquarantine.	No
uid	string	Single FortiClient UID to unquarantine.	No
mac	array	Array of MACs to unquarantine.	No
mac	string	Single MAC to unquarantine.	No

registration: block

Summary	Block endpoint by FortiClient UID or MAC.
URI	endpoint-control/registration/block/
HTTP Method	POST
Action	block
Access Group	endpoint-control-grp

Extra parameters

Name	Type	Summary	Required
uid	array	Array of FortiClient UIDs to block.	No
uid	string	Single FortiClient UID to block.	No
mac	array	Array of MACs to block.	No
mac	string	Single MAC to block.	No

registration: unblock

Summary	Unblock endpoint by FortiClient UID or MAC.
URI	endpoint-control/registration/unblock/
HTTP Method	POST
Action	unblock
Access Group	endpoint-control-grp

Extra parameters

Name	Type	Summary	Required
uid	array	Array of FortiClient UIDs to unblock.	No
uid	string	Single FortiClient UID to unblock.	No
mac	array	Array of MACs to unblock.	No
mac	string	Single MAC to unblock.	No

registration: deregister

Summary	Deregister endpoint by FortiClient UID or MAC.
URI	endpoint-control/registration/deregister/
HTTP Method	POST
Action	deregister
Access Group	endpoint-control-grp

Extra parameters

Name	Type	Summary	Required
uid	array	Array of FortiClient UIDs to deregister.	No
uid	string	Single FortiClient UID to deregister.	No
mac	array	Array of MACs to deregister.	No
mac	string	Single MAC to deregister.	No

installer: select

Summary	List available FortiClient installers.
URI	endpoint-control/installer/select/
HTTP Method	GET
Action	select
Access Group	endpoint-control-grp

Extra parameters

Name	Type	Summary	Required
min_version	string	Filter: Minimum installer version. (String of the format n[.n[.n]]).	No

installer: download

Summary	Download a FortiClient installer via FortiGuard.
URI	endpoint-control/installer/download/

HTTP Method	GET
Action	download
Access Group	endpoint-control-grp
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of installer (image_id).	Yes

avatar: download

Summary	Download an endpoint avatar image.
URI	endpoint-control/avatar/download/
HTTP Method	GET
Action	download
Access Group	endpoint-control-grp
ETag Caching	Enabled
Response Type	object

Extra parameters

Name	Type	Summary	Required
uid	string	Single FortiClient UID.	No
user	string	User name of the endpoint.	No
alias	string	Alias of the device. Used to lookup device avatar when end-point avatar is not available.	No
default	string	Default avatar name ['authuser'|'unauthuser']. Default avatar when endpoint / device avatar is not available.	No

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

acl: select

Summary	List counters for all IPv4 ACL.
URI	firewall/acl/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

acl: clear_counters

Summary	Reset counters for one or more IPv4 ACLs by policy ID.

URI	firewall/acl/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

acl6: select

Summary	List counters for all IPv6 ACL.
URI	firewall/acl6/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

acl6: clear_counters

Summary	Reset counters for one or more IPv6 ACLs by policy ID.
URI	firewall/acl6/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

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

proxy-policy: select

Summary	List traffic statistics for all explicit proxy policies.
URI	firewall/proxy-policy/select/
HTTP Method	GET

Action	select
Access Group	fwgrp.policy

proxy-policy: clear_counters

Summary	Reset traffic statistics for one or more explicit proxy policies by policy ID.
URI	firewall/proxy-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

policy-lookup: select

Summary	Performs a policy lookup by creating a dummy packet and asking the kernel which policy would be hit.
URI	firewall/policy-lookup/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy
Response Type	object

Extra parameters

Name	Type	Summary	Required
ipv6	boolean	Perform an IPv6 lookup?	No
srcintf	string	Source interface.	Yes

Name	Type	Summary	Required
sourceport	int	Source port.	No
sourceip	int	Source IP.	Yes
protocol	string	Protocol.	Yes
dest	string	Destination IP/FQDN.	Yes
destport	int	Destination port.	Yes
icmptype	int	ICMP type.	No
icmpcode	int	ICMP code.	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
sourceport	int	Filter: Source port.	No
policyid	int	Filter: Policy ID.	No
application	int	Filter: Application ID.	No

Name	Type	Summary	Required
protocol	int	Filter: Protocol name [all|igmp|tcp|udp|icmp|etc].	No
destport	int	Filter: Destination port.	No
srcintf	string	Filter: Source interface name.	No
dstintf	string	Filter: Destination interface name.	No
source	string	Filter: Source IP address.	No
destination	string	Filter: Destination IP address.	No
username	string	Filter: Authenticated username.	No
shaper	string	Filter: Forward traffic shaper name.	No
country	string	Filter: Destination country name.	No
natsourceaddress	string	Filter: NAT source address.	No
natsourceport	string	Filter: NAT source port.	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	Close a specific firewall session that matches all provided criteria.
URI	firewall/session/close/
HTTP Method	POST
Action	close
Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
pro	string	Protocol name [tcp|udp|icmp|...].	Yes
saddr	string	Source address.	Yes
daddr	string	Destination address.	Yes
sport	string	Source port.	Yes
dport	string	Destination port.	Yes

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|srcintf|dstintf|policy|country].	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 srcintf, source, dstintf, destination, policyid, application, web_category_id, web_domain, country.	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

address-fqdns: select

Summary	List of FQDN address objects and the IPs they resolved to.

URI	firewall/address-fqdns/select/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy
Response Type	object

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

geoip

geoip-query: select

Summary	Retrieve location details for IPs queried against FortiGuard's geoip service.
URI	geoip/geoip-query/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
ip_addresses	string	One or more IP address strings to query for location details.	Yes

ips

rate-based: select

Summary	Returns a list of rate-based signatures in IPS package.
URI	ips/rate-based/select/
HTTP Method	GET
Action	select

Access Group	utmgrp.ips
Response Type	array

license

status: select

Summary	Get current license and registration status.
URI	license/status/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

database: upgrade

Summary	Upgrade IPS database on this device using uploaded file.
URI	license/database/upgrade/
HTTP Method	POST
Action	upgrade
Access Group	updategrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
db_name	string	Security service database name [ips_appctrl|antivirus|...]	No
file_content	string	Provided when uploading a file: base64 encoded file data. Must not contain whitespace or other invalid base64 characters. Must be included in HTTP body.	No

forticare-resellers: select

Summary	Get current FortiCare resellers for the requested country.
URI	license/forticare-resellers/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
country_code	int	FortiGuard country code	No

forticare-org-list: select

Summary	Get FortiCare organization size and industry lists.
URI	license/forticare-org-list/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

log

current-disk-usage: select

Summary	Return current used, free and total disk bytes.
URI	log/current-disk-usage/select/
HTTP Method	GET
Action	select
Access Group	loggrp.data-access

device: state

Summary	Retrieve information on state of log devices.
URI	log/device/state/
HTTP Method	GET
Action	state
Access Group	loggrp.data-access
Response Type	object

forticloud: select

Summary	Return FortiCloud log status.
URI	log/forticloud/select/
HTTP Method	GET
Action	select
Access Group	loggrp.config

fortianalyzer: select

Summary	Return FortiAnalyzer/FortiManager log status.
URI	log/fortianalyzer/select/
HTTP Method	GET
Action	select
Access Group	loggrp.config

Extra parameters

Name	Type	Summary	Required
server	string	FortiAnalyzer/FortiManager address.	No

fortianalyzer-queue: select

Summary	Retrieve information on FortiAnalyzer's queue state. Note:- FortiAnalyzer logs are queued only if upload-option is realtime.
URI	log/fortianalyzer-queue/select/
HTTP Method	GET
Action	select
Access Group	loggrp.config
Response Type	object

Extra parameters

Name	Type	Summary	Required
scope	string	Scope from which to retrieve FortiAnalyzer's queue state [vdom*|global].	No

hourly-disk-usage: select

Summary	Return historic hourly disk usage in bytes.
URI	log/hourly-disk-usage/select/
HTTP Method	GET
Action	select
Access Group	loggrp.data-access

historic-daily-remote-logs: select

Summary	Returns the amount of logs in bytes sent daily to a remote logging service (FortiCloud or FortiAnalyzer).
URI	log/historic-daily-remote-logs/select/
HTTP Method	GET
Action	select
Access Group	loggrp.data-access

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 | forticloud].	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

forticloud-report: download

Summary	Download PDF report from FortiCloud.
URI	log/forticloud-report/download/
HTTP Method	GET
Action	download
Access Group	loggrp.data-access
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	int	FortiCloud Report ID.	Yes
inline	int	Set to 1 to download the report inline.	No

ips-archive: download

Summary	Download IPS/application control packet capture files. Uses configured log display device.
URI	log/ips-archive/download/
HTTP Method	GET
Action	download
Access Group	loggrp.data-access
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	int	IPS archive ID.	Yes
pcap_no	int	Packet capture roll number (required when log device is 'disk')	No
pcap_category	int	Packet capture category (required when log device is 'disk')	No

policy-archive: download

Summary	Download policy-based packet capture archive.
URI	log/policy-archive/download/
HTTP Method	GET
Action	download
Access Group	loggrp.data-access
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	int	Session ID (from traffic log).	Yes
srcip	string	Source IP.	Yes
dstip	string	Destination IP.	Yes

av-archive: download

Summary	Download file quarantined by AntiVirus.
URI	log/av-archive/download/
HTTP Method	GET
Action	download
Access Group	loggrp.data-access
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Checksum for quarantined file.	Yes

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 (Default for all routes).	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

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 (Default for all routes).	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

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

lookup: select

Summary	Performs a route lookup by querying the routing table.
URI	router/lookup/select/
HTTP Method	GET
Action	select
Access Group	routegrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
ipv6	boolean	Perform an IPv6 lookup?	No
destination	string	Destination IP/FQDN	Yes

system

admin: toggle-vdom-mode

Summary	Toggles VDOM mode on/off. Enables or disables VDOM mode if it is disabled or enabled respectively.
URI	system/admin/toggle-vdom-mode/
HTTP Method	POST
Action	toggle-vdom-mode
Access Group	sysgrp
Response Type	object

config-revision: select

Summary	Returns a list of system configuration revisions.
URI	system/config-revision/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

config-revision: update-comments

Summary	Updates comments for a system configuration file.
URI	system/config-revision/update-comments/
HTTP Method	POST
Action	update-comments
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
config_id	int	Configuration id.	No
comments	string	Configuration comments.	No

config-revision: delete

Summary	Deletes one or more system configuration revisions.
URI	system/config-revision/delete/
HTTP Method	POST
Action	delete
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
config_ids	array	List of configuration ids.	Yes

config-revision: file

Summary	Download a specific configuration revision.
URI	system/config-revision/file/
HTTP Method	GET
Action	file
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
config_id	int	Configuration id.	No

config-revision: info

Summary	Retrieve meta information for a specific configuration revision.
URI	system/config-revision/info/
HTTP Method	GET
Action	info
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
config_id	int	Configuration id.	No

config-revision: save

Summary	Create a new config revision checkpoint.
URI	system/config-revision/save/
HTTP Method	POST
Action	save
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
comments	string	Optional revision comments	No

current-admins: select

Summary	Return a list of currently logged in administrators.
URI	system/current-admins/select/
HTTP Method	GET

Action	select
Access Group	sysgrp
Response Type	array

disconnect-admins: select

Summary	Disconnects logged in administrators.
URI	system/disconnect-admins/select/
HTTP Method	POST
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
id	int	Admin ID	No
method	string	Login method used to connect admin to FortiGate.	No
admins	array	List of objects with admin id and method.	No

time: set

Summary	Sets current system time stamp.
URI	system/time/set/
HTTP Method	POST
Action	set
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
year	int	Specifies the year for setting/updating time manually.	Yes
month	int	Specifies the month (0 - 11) for setting/updating time manually.	Yes
day	int	Specifies the day for setting/updating time manually.	Yes
hour	int	Specifies the hour (0 - 23) for setting/updating time manually.	Yes
minute	int	Specifies the minute (0 - 59) for setting/updating time manually.	Yes
second	int	Specifies the second (0 - 59) for setting/updating time manually.	Yes

time: select

Summary	Gets current system time stamp.
URI	system/time/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

os: reboot

Summary	Immediately reboot this device.
URI	system/os/reboot/
HTTP Method	POST
Action	reboot
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
event_log_message	string	Message to be logged in event log.	No

os: shutdown

Summary	Immediately shutdown this device.
URI	system/os/shutdown/
HTTP Method	POST
Action	shutdown
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
event_log_message	string	Message to be logged in event log.	No

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

dhcp: select

Summary	Returns a list of all DHCP IPv4 and IPv6 DHCP leases.
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 addresses in the response.	No

dhcp: revoke

Summary	Revoke IPv4 DHCP leases.
URI	system/dhcp/revoke/
HTTP Method	POST
Action	revoke
Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
ip	array	Optional list of addresses to revoke. Defaults to all addresses if not provided.	No

dhcp6: revoke

Summary	Revoke IPv6 DHCP leases.
URI	system/dhcp6/revoke/
HTTP Method	POST
Action	revoke
Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
ip	array	Optional list of addresses to revoke. Defaults to all addresses if not provided.	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	Upgrade firmware image on this device using uploaded file.
URI	system/firmware/upgrade/
HTTP Method	POST
Action	upgrade
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
source	string	Firmware file data source [upload|usb|fortiguard].	Yes
filename	string	Name of file on fortiguard or USB disk to upgrade to.	No
format_partition	boolean	Set to true to format boot partition before upgrade.	No
file_content	string	Provided when uploading a file: base64 encoded file data. Must not contain whitespace or other invalid base64 characters. Must be included in HTTP body.	No

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

storage: select

Summary	Retrieve information for the non-boot disk.
URI	system/storage/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

change-password: select

Summary	Save admin and guest-admin passwords.
URI	system/change-password/select/
HTTP Method	POST
Action	select
Access Group	any

password-policy-conform: select

Summary	Check whether password conforms to the password policy.
URI	system/password-policy-conform/select/
HTTP Method	POST
Action	select
Access Group	any

csf: select

Summary	Retrieve a full tree of downstream FortiGates registered to the Security Fabric.
URI	system/csf/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
ETag Caching	Enabled
Response Type	object

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

resource: usage

Summary	Retreive current and historical usage data for a provided resource.
URI	system/resource/usage/
HTTP Method	GET
Action	usage
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
resource	string	Resource to get usage data for [cpu|memory|disk|sessions|lograte]. Defaults to all resources if not provided.	No
interval	string	Time interval of resource usage [1-min|10-min|30-min|1-hour|12-hour|24-hour]. Defaults to all intervals if not provided.	No

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

sniffer: download

Summary	Download a stored packet capture.
URI	system/sniffer/download/
HTTP Method	GET
Action	download
Access Group	fwgrp.packet-capture

Response Type	object

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
poe	boolean	Filter: Retrieve PoE statistics for ports of configured FortiSwitches. Port power usage is in Watt units.	No

fsw: update

Summary	Update administrative state for a given FortiSwitch (enable or disable authorization).
URI	system/fsw/update/
HTTP Method	POST
Action	update
Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
fswname	string	FortiSwitch name.	No
admin	string	New FortiSwitch administrative state [enable|disable|discovered].	No

fsw: restart

Summary	Restart a given FortiSwitch.
URI	system/fsw/restart/
HTTP Method	POST
Action	restart
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of managed FortiSwitch.	Yes

fsw: upgrade

Summary	Upgrade firmware image on the given FortiSwitch using uploaded file.
URI	system/fsw/upgrade/
HTTP Method	POST
Action	upgrade
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of managed FortiSwitch.	Yes
source	string	Firmware file data source [upload|fortiguard].	Yes
file_content	string	Provided when uploading a file: base64 encoded file data. Must not contain whitespace or other invalid base64 characters. Must be included in HTTP body.	No

fsw-firmware: select

Summary	Retrieve a list of recommended firmware for managed FortiSwitches.
URI	system/fsw-firmware/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Filter: FortiSwitch ID.	No
timeout	string	FortiGuard connection timeout (defaults to 3 seconds).	No

switch-controller

managed-switch: faceplate-xml

Summary	Retrieve XML for rendering FortiSwitch faceplate widget.
URI	switch-controller/managed-switch/faceplate-xml/
HTTP Method	GET
Action	faceplate-xml

Access Group	wifi
Response Type	array

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of managed FortiSwitch.	No

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

available-interfaces: select

Summary	Retrieve a list of all interfaces along with some meta information regarding their availability.
URI	system/available-interfaces/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	array

available-interfaces: ha

Summary	Retrieve a list of all interfaces along with some meta information regarding their availability. Includes extra meta information useful when dealing with interfaces related to HA configuration. Interfaces that are used by an HA cluster as management interfaces are also included in this view
URI	system/available-interfaces/ha/
HTTP Method	GET
Action	ha
Access Group	any
Response Type	array

interface-bandwidth: select

Summary	Retrieve bandwidth of all interfaces.
URI	system/interface-bandwidth/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	object

acquired-dns: select

Summary	Retrieve a list of interfaces and their acquired DNS servers.
URI	system/acquired-dns/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	array

resolve-fqdn: select

Summary	Resolves the provided FQDNs to FQDN -> IP mappings.
URI	system/resolve-fqdn/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	object

Extra parameters

Name	Type	Summary	Required
ipv6	boolean	Resolve for the AAAA record?	No
fqdn	string	FQDN	Yes
fqdn	array	List of FQDNs to be resolved	No

usb-log: select

Summary	Retrieve information about connected USB drives, including estimated log sizes.
URI	system/usb-log/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

usb-log: start

Summary	Start backup of logs from current VDOM to USB drive.
URI	system/usb-log/start/
HTTP Method	POST
Action	start
Access Group	sysgrp

usb-log: stop

Summary	Stop backup of logs to USB drive.
URI	system/usb-log/stop/
HTTP Method	POST
Action	stop
Access Group	sysgrp

ipconf: select

Summary	Determine if there is an IP conflict for a specific IP using ARP.
URI	system/ipconf/select/
HTTP Method	GET
Action	select
Access Group	netgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
dev	object	List of interfaces to check for conflict.	No
ipaddr	string	IPv4 address to check for conflict.	No

fortiguard: update

Summary	Immediately update status for FortiGuard services.
URI	system/fortiguard/update/
HTTP Method	POST
Action	update
Access Group	sysgrp

fortiguard: clear-cache

Summary	Immediately clear all FortiGuard statistics.
URI	system/fortiguard/clear-cache/
HTTP Method	POST
Action	clear-cache
Access Group	sysgrp

fortiguard: test-availability

Summary	Test availability of FortiGuard services.
URI	system/fortiguard/test-availability/
HTTP Method	POST
Action	test-availability
Access Group	sysgrp

fortiguard: server-info

Summary	Get FortiGuard server list and information.
URI	system/fortiguard/server-info/
HTTP Method	GET
Action	server-info
Access Group	sysgrp

fortimanager: status

Summary	Get FortiManager status.
URI	system/fortimanager/status/
HTTP Method	GET
Action	status
Access Group	sysgrp

fortimanager: config

Summary	Configure FortiManager address.
URI	system/fortimanager/config/
HTTP Method	POST
Action	config
Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
fortimanager_ip	string	FortiManager IP or domain to connect to and register with.	Yes
unregister	boolean	Set to true to unregister from FortiManager.	No

available-certificates: select

Summary	Get available certificates.
URI	system/available-certificates/select/
HTTP Method	GET
Action	select
Access Group	any

Extra parameters

Name	Type	Summary	Required
scope	string	Scope of certificate [vdom*|global].	No

certificate: download

Summary	Download certificate.
URI	system/certificate/download/
HTTP Method	GET
Action	download

Access Group	vpngrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of certificate.	Yes
type	string	Type of certificate [local|csr|remote|ca|crl].	Yes
scope	string	Scope of certificate [vdom*|global].	No

debug: select

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

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

debug: download

Summary	Download debug report for technical support.
URI	system/debug/download/
HTTP Method	GET
Action	download

Access Group	mntgrp
Response Type	object

com-log: dump

Summary	Dump system com-log to file.
URI	system/com-log/dump/
HTTP Method	POST
Action	dump
Access Group	sysgrp

com-log: update

Summary	Fetch system com-log file dump progress.
URI	system/com-log/update/
HTTP Method	GET
Action	update
Access Group	sysgrp

com-log: download

Summary	Download com-log file (after file dump is complete).
URI	system/com-log/download/
HTTP Method	GET
Action	download
Access Group	sysgrp
Response Type	object

botnet: stat

Summary	Retrieve statistics for FortiGuard botnet database.

URI	system/botnet/stat/
HTTP Method	GET
Action	stat
Access Group	sysgrp
ETag Caching	Enabled
Response Type	object

botnet: select

Summary	List all known IP-based botnet entries in FortiGuard botnet database.
URI	system/botnet/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
ETag Caching	Enabled
Response Type	array

Extra parameters

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

botnet-domains: select

Summary	List all known domain-based botnet entries in FortiGuard botnet database.
URI	system/botnet-domains/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

ETag Caching	Enabled
Response Type	array

Extra parameters

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

botnet-domains: stat

Summary	List statistics on domain-based botnet entries in FortiGuard botnet database.
URI	system/botnet-domains/stat/
HTTP Method	GET
Action	stat
Access Group	sysgrp
ETag Caching	Enabled
Response Type	object

ha-statistics: select

Summary	List of statistics for members of HA cluster
URI	system/ha-statistics/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

ha-checksums: select

Summary	List of checksums for members of HA cluster

URI	system/ha-checksums/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

ha-peer: select

Summary	Get configuration of peer(s) in HA cluster. Uptime is expressed in seconds.
URI	system/ha-peer/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary	Required
serial_no	string	Serial number of the HA member. If not specified, fetch information for all HA members	No
vcluster_id	int	Virtual cluster number. If not specified, fetch information for all active vclusters	No

ha-peer: update

Summary	Update configuration of peer in HA cluster.
URI	system/ha-peer/update/
HTTP Method	POST
Action	update
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
serial_no	string	Serial number of the HA member.	Yes
vcluster_id	int	Virtual cluster number.	No
priority	int	Priority to assign to HA member.	No
hostname	string	Name to assign the HA member.	No

ha-peer: disconnect

Summary	Update configuration of peer in HA cluster.
URI	system/ha-peer/disconnect/
HTTP Method	POST
Action	disconnect
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
serial_no	string	Serial number of the HA member.	Yes
interface	string	Name of the interface which should be assigned for management.	Yes
ip	string	IP to assign to the selected interface.	Yes
mask	string	Full network mask to assign to the selected interface.	Yes

link-monitor: select

Summary	Retrieve per-interface statistics for active link monitors.
URI	system/link-monitor/select/
HTTP Method	GET
Action	select

Access Group	sysgrp

Extra parameters

Name	Type	Summary	Required
mkey	string	Name of link monitor.	No

compliance: run

Summary	Immediately run compliance checks for the selected VDOM.
URI	system/compliance/run/
HTTP Method	POST
Action	run
Access Group	sysgrp

config: restore

Summary	Restore system configuration from uploaded file or from USB.
URI	system/config/restore/
HTTP Method	POST
Action	restore
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
source	string	Configuration file data source [upload | usb | revision].	Yes
usb_filename	string	When using 'usb' source: the filename to restore from the connected USB device.	No
config_id	int	When using 'revision' source: valid ID of configuration stored on disk to revert to.	No
password	string	Password to decrypt configuration data.	No

Name	Type	Summary	Required
scope	string	Specify global or VDOM only restore [global | vdom].	Yes
vdom	string	If 'vdom' scope specified, the name of the VDOM to restore configuration.	No
file_content	string	Provided when uploading a file: base64 encoded file data. Must not contain whitespace or other invalid base64 characters. Must be included in HTTP body.	No

config: backup

Summary	Backup system config
URI	system/config/backup/
HTTP Method	GET
Action	backup
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
destination	string	Configuration file destination [file* | usb]	No
usb_filename	string	When using 'usb' destination: the filename to save to on the connected USB device	No
password	string	Password to encrypt configuration data.	No
scope	string	Specify global or VDOM only backup [global | vdom].	Yes
vdom	string	If 'vdom' scope specified, the name of the VDOM to backup configuration.	No

config: usb-filelist

Summary	List configuration files available on connected USB drive.
URI	system/config/usb-filelist/
HTTP Method	GET

Action	usb-filelist
Access Group	sysgrp
Response Type	array

sandbox: status

Summary	Retrieve sandbox status.
URI	system/sandbox/status/
HTTP Method	GET
Action	status
Access Group	sysgrp
Response Type	object

sandbox: stats

Summary	Retrieve sandbox statistics.
URI	system/sandbox/stats/
HTTP Method	GET
Action	stats
Access Group	sysgrp
Response Type	object

object: usage

Summary	Retrieve all objects that are currently using as well as objects that can use the given object.
URI	system/object/usage/
HTTP Method	GET
Action	usage
Access Group	any
Response Type	object

Extra parameters

Name	Type	Summary	Required
path	string	The CMDB table's path	No
name	string	The CMDB table's name	No
qtypes	array	List of CMDB table qTypes	No
mkey	string	The mkey for the object	Yes

timezone: select

Summary	Get world timezone and daylight saving time.
URI	system/timezone/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	array

vmlicense: upload

Summary	Update VM license using uploaded file. Reboots immediately if successful.
URI	system/vmlicense/upload/
HTTP Method	POST
Action	upload
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
file_content	string	Provided when uploading a file: base64 encoded file data. Must not contain whitespace or other invalid base64 characters. Must be included in HTTP body.	No

sensor-info: select

Summary	Retrieve system sensor status.
URI	system/sensor-info/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

audit: select

Summary	Retrieve Security Fabric audit results.
URI	system/audit/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

fortiguard-blacklist: select

Summary	Retrieve blacklist information for a specified IP.
URI	system/fortiguard-blacklist/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
ip	string	IPv4 address to check against.	Yes
timeout	int	Timeout period in seconds (defaults to 5).	No

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	Reset a specific FortiExtender unit.
URI	extender-controller/extender/reset/
HTTP Method	POST
Action	reset
Access Group	netgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
id	string	FortiExtender ID to reset.	Yes

user

firewall: select

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

Extra parameters

Name	Type	Summary	Required
start	int	Starting entry index.	No
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 single, multiple, or all firewall users.
URI	user/firewall/deauth/
HTTP Method	POST
Action	deauth
Access Group	authgrp

Extra parameters

Name	Type	Summary	Required
user_type	string	User type [proxy|firewall]. Required for both proxy and firewall users.	No

Name	Type	Summary	Required
id	int	User ID. Required for both proxy and firewall users.	No
ip	string	User IP address. Required for both proxy and firewall users.	No
ip_version	string	IP version [ip4|ip6]. Only required if user_type is firewall.	No
method	string	Authentication method [fsso|rsso|ntlm|firewall|wsso|fsso_citrix|sso_guest]. Only required if user_type is firewall.	No
all	boolean	Set to true to deauthenticate all users. Other parameters will be ignored.	No
users	array	Array of user objects to deauthenticate. Use this to deauthenticate multiple users at once. Each object should include the above properties.	No

banned: select

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

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	authgrp

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	authgrp

Extra parameters

Name	Type	Summary	Required
ip_addresses	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	authgrp

fortitoken: select

Summary	List FortiTokens and their status.
URI	user/fortitoken/select/
HTTP Method	GET
Action	select
Access Group	authgrp
Response Type	object

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

device: select

Summary	Retrieve a list of detected devices.
URI	user/device/select/
HTTP Method	GET
Action	select
Access Group	sysgrp
ETag Caching	Enabled
Response Type	array

Extra parameters

Name	Type	Summary	Required
master_only	boolean	List of master device only.	No
fortilink_visibility	boolean	Add port and switch info for devices behind a managed FortiSwitch.	No
compliance_visibility	boolean	Add compliance status to indicate if a device is 'exempt' or 'non-compliant' by interface's FortiClient host check.	No

Name	Type	Summary	Required
intf_name	string	Filter: Name of interface where the device was detected. Only available when compliance_visibility is true.	No
master_mac	string	Filter: Master MAC of a device. Multiple entries could be returned.	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

fortitoken: send-activation

Summary	Send a FortiToken activation code to a user via SMS or Email.
URI	user/fortitoken/send-activation/
HTTP Method	POST
Action	send-activation
Access Group	authgrp
Response Type	object

Extra parameters

Name	Type	Summary	Required
user_name	string	Username.	No
token	string	User's FortiToken serial number.	No
method	string	Method to send activation code ('email' or 'sms').	No
email	string	User's email address (required if using 'email' method).	No
sms_phone	string	User's SMS phone number (required if using 'sms' method).	No

fsso: refresh-server

Summary	Refresh remote agent group list for all fsso agents.
URI	user/fsso/refresh-server/
HTTP Method	POST
Action	refresh-server
Access Group	authgrp

fsso: select

Summary	Get a list of fsso and fsso polling status.
URI	user/fsso/select/
HTTP Method	GET

Action	select
Access Group	authgrp

utm

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-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

application-categories: select

Summary	Retrieve a list of application control categories.
URI	utm/application-categories/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	array

antivirus: stats

Summary	Retrieve antivirus scanning statistics.
URI	utm/antivirus/stats/
HTTP Method	GET
Action	stats
Access Group	utmgrp.antivirus
Response Type	object

virtual-wan

health-check: select

Summary	Retrieve statistics for each SD-WAN link.

URI	virtual-wan/health-check/select/
HTTP Method	GET
Action	select
Access Group	sysgrp

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	Delete a configured webfilter override.
URI	webfilter/override/delete/
HTTP Method	POST
Action	delete
Access Group	utmgrp.webfilter

Extra parameters

Name	Type	Summary	Required
mkey	string	ID of webfilter override to delete.	No

malicious-urls: select

Summary	List all URLs in FortiSandbox malicious URL database.
URI	webfilter/malicious-urls/select/

HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter
ETag Caching	Enabled
Response Type	object

malicious-urls: stat

Summary	Retrieve statistics for the FortiSandbox malicious URL database.
URI	webfilter/malicious-urls/stat/
HTTP Method	GET
Action	stat
Access Group	utmgrp.webfilter
ETag Caching	Enabled
Response Type	object

category-quota: select

Summary	Retrieve quota usage statistics for webfilter categories.
URI	webfilter/category-quota/select/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter

Extra parameters

Name	Type	Summary	Required
profile	string	Webfilter profile.	No
user	string	User or IP (required if profile specified).	No

category-quota: reset

Summary	Reset webfilter quota for user or IP.
URI	webfilter/category-quota/reset/
HTTP Method	POST
Action	reset
Access Group	utmgrp.webfilter

Extra parameters

Name	Type	Summary	Required
profile	string	Webfilter profile to reset.	No
user	string	User or IP to reset with.	No

fortiguard-categories: select

Summary	Return FortiGuard web filter categories.
URI	webfilter/fortiguard-categories/select/
HTTP Method	GET
Action	select
Access Group	any
Response Type	array

Extra parameters

Name	Type	Summary	Required
include_ unrated	boolean	Include Unrated category in result list.	No

trusted-urls: select

Summary	List all URLs in FortiGuard trusted URL database.
URI	webfilter/trusted-urls/select/
HTTP Method	GET

Action	select
Access Group	utmgrp.webfilter
ETag Caching	Enabled
Response Type	object

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
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
p1name	string	IPsec phase1 name.	Yes

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: clear_tunnel

Summary	Remove all active tunnel sessions in current virtual domain.
URI	vpn/ssl/clear_tunnel/
HTTP Method	POST
Action	clear_tunnel
Access Group	vpngrp

ssl: delete

Summary	Terminate the provided SSL-VPN session.
URI	vpn/ssl/delete/
HTTP Method	POST
Action	delete
Access Group	vpngrp

Extra parameters

Name	Type	Summary	Required
type	string	The session type [websession|subsession].	Yes
index	int	The session index.	Yes

ssl: stats

Summary	Return statistics about the SSL-VPN.

URI	vpn/ssl/stats/
HTTP Method	GET
Action	stats
Access Group	vpngrp

wanopt

history: select

Summary	Retrieve WAN opt. statistics history.
URI	wanopt/history/select/
HTTP Method	GET
Action	select
Access Group	wanoptgrp

Extra parameters

Name	Type	Summary	Required
period	string	Statistics period [10-min*|hour|day|week|30-day].	No

history: reset

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

webcache: select

Summary	Retrieve webcache statistics history.
URI	wanopt/webcache/select/

HTTP Method	GET
Action	select
Access Group	wanoptgrp

Extra parameters

Name	Type	Summary	Required
period	string	Statistics period [10-min*|hour|day|week|30-day].	No

webcache: reset

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

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

webproxy

pacfile: download

Summary	Download webproxy PAC file.
URI	webproxy/pacfile/download/
HTTP Method	GET
Action	download
Access Group	netgrp
Response Type	object

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	Update administrative state for a given FortiAP (enable or disable authorization).
URI	wifi/managed_ap/set_status/
HTTP Method	POST
Action	set_status
Access Group	wifi

Extra parameters

Name	Type	Summary	Required
wtpname	string	FortiAP name.	No
admin	string	New FortiAP administrative state [enable|disable|discovered].	No

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

managed_ap: restart

Summary	Restart a given FortiAP.
URI	wifi/managed_ap/restart/
HTTP Method	POST
Action	restart
Access Group	wifi

Extra parameters

Name	Type	Summary	Required
wtpname	string	FortiAP name.	No

managed_ap: upgrade

Summary	Upgrade firmware image on the given FortiAP using uploaded file.
URI	wifi/managed_ap/upgrade/
HTTP Method	POST
Action	upgrade
Access Group	wifi
Response Type	object

Extra parameters

Name	Type	Summary	Required
mkey	string	Serial number of FortiAP to upgrade.	Yes
source	string	Firmware file data source [upload|fortiguard].	Yes
filename	string	Firmware image file for when 'source' is 'upload'.	No
image_id	string	Fortiguard image file ID for when 'source' is 'fortiguard'.	No
file_content	string	Provided when uploading a file: base64 encoded file data. Must not contain whitespace or other invalid base64 characters. Must be included in HTTP body.	No

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 interfering 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	Reset presence analytics statistics.
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	Clear all detected rogue APs.
URI	wifi/rogue_ap/clear_all/
HTTP Method	POST
Action	clear_all
Access Group	wifi

rogue_ap: set_status

Summary	Mark detected APs as rogue APs.
URI	wifi/rogue_ap/set_status/
HTTP Method	POST
Action	set_status
Access Group	wifi

Extra parameters

Name	Type	Summary	Required
bssid	array	List of rogue AP MAC addresses.	No
ssid	array	Corresponding list of rogue AP SSIDs.	No
status	string	Status to assign matching APs [unclassified|rogue|accepted|suppressed].	No

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

coverage

download: select

Summary	Download code coverage.
URI	coverage/download/select/
HTTP Method	GET
Action	select
Access Group	any
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
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/policy6/clear_counters	?vdom=root	{'policy': 1,}	fwgrp.policy	Reset traffic statistics for single IPv4 policy, vdom root
POST	/api/v2/monitor/firewall/policy6/clear_counters	?vdom=root	{'policy': [1, 2]}	fwgrp.policy	Reset traffic statistics for multiple IPv4 policies, vdom root

Method	URL	URL Parameters	Body Data	Access Group	Description
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
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/os/reboot			sysgrp	Immediately reboot this device
POST	/api/v2/monitor/system/os/shutdown			sysgrp	Immediately shutdown this device