FORTINET
High Performance Network Security

FortiOS - REST API Reference

VERSION 5.2.7

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 28, 2016

FortiOS 5.2.7 REST API Reference

01-526-270937-20160328

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-09-04	Updated for version 5.2.4.
2015-12-03	Updated for version 5.2.5.
2016-01-29	Updated for version 5.2.6.
2016-03-28	Updated for version 5.2.7.

Introduction

This document provides the REST API information supported in FortiOS version 5.2.7. This document covers the FortiOS GUI supported REST API reference only.

The following REST API's are supported:

- CMDB API
  - Retrieve
  - Create
  - Modify
  - Delete objects
  - Configuration
- Monitor API
  - Monitor dynamic data
  - Refresh
  - Reset stats
  - Reset
  - Restart

Authentication

When making requests to the FortiGate using REST APIs, you will need:

1. A valid authentication cookie (not including FortiManager requests).
2. Appropriate permissions for the requested object.
3. A valid Cross-Site Request Forgery (CSRF) token for `HTTP POST`/`PUT`/`DELETE` methods (`HTTP GET` does not require CSRF token).

CSRF Tokens

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.

This is an important security measure; extra care is needed when submitting direct POST requests to the FortiGate. The CSRF token must be included in the POST data with the name `CSRF_TOKEN`, or in the `X-CSRFTOKEN HTTP` header.

The value for the token is included as a hidden input named `csrftoken` on any form rendered by the GUI. It's also available from the cookie variable `ccsrftoken`.

> Please note that the `ccsrftoken` cookie variable is only used to pass the token value from the server to the client, it will not be used to authenticate the request. For authentication the token must be in the POST data or HTTP headers.

Setting Up an Authenticated Session

To acquire a valid authentication token, you must make a POST request to the FortiOS login handler with your administrative login and password.

To setup an authenticated session, make a 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
Username POST Variable	username
Password POST Variable	secretkey

If login is successful, the response will contain the authentication token in the `APSCOOKIE` cookie value. This cookie value must be included in any further requests.

The permissions for the administrative account you use will affect which objects and operations you'll have access to, so ensure the user has the permissions required for the actions you wish to perform.

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
POST Variable	none needed

FortiManager support

FortiManager queries the API using a special VDOM: `vsys_fgfm`. Requests from this VDOM do not require authentication or authorization for individual features.

All other users must first authenticate and will then be granted permissions that correspond with their assigned access profile.

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 are some of the HTTP status codes used:

HTTP Response Code	Description
200 - OK	API request successful.
400 - Bad Request	Bad request.
403 - Forbidden	Request is missing CSRF token or administrato is missing acccess profile permissions.
404 - 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	The request entity is too large.
424 - Failed Dependency	Failed dependency.
500 - Internal Server Error	Internal server error.

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)
```

CMDB API

CMDB API is used to retrieve and modify CLI configurations. All CMDB requests start with '/api/v2/cmdb/'

API directive

User can view full CMDB API directive using the following URL (available on debug build only): `https://<FG_IP>/api/v2/cmdb`

This directive provides complete documentation of the API usage.

URL format

Here is how the URL is structured for CMDB requests:

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

The path, name, mkey are based on CLI command syntax with the exception of vdom table. For examples:

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

URL parameters

Generic parameters

The following optional URL parameters are generic to all CMDB API requests"

URL Parameter	Example	Description
vdom	/api/v2/monitor/firewall/policy/?vdom=root	Return result for the specified vdom. If vdom parameter is not provided, return current vdom instead. If admin does not have access to the vdom, return permission error.

Specific parameters

Each CMDB method may have extra URL parameters unique to the method (see 2.6 for details). For example, to retrieve object schema, need to specify 'action=schema' in the request URL:

```
GET /api/v2/cmdb/firewall/policy/?action=schema
```

Body data

POST/PUT requests require body data. For example, to create new firewall address object, user needs to specify the address data in the request data:

```
POST /api/v2/cmdb/firewall/address?vdom=root {'json': {'name':"address1", 'type':
    "ipmask", 'subnet': "1.1.1.0 255.255.255.0"}}
```

GET/DELETE requests do not accept body data.

Examples

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb			Retrieve CMDB API V2 directive
GET	/api/v2/cmdb /firewall/address	?action=schema		Retrieve schema of firewall address
GET	/api/v2/cmdb /firewall/address	?action=default		Retrieve default format of firewall address
GET	/api/v2/cmdb /firewall/address	?action=select&vdom =root		Retrieve all firewall address objects, root vdom
GET	/api/v2/cmdb /firewall/address	?vdom=root&start= 0&count=10		Retrieve the first 10 firewall addresses, root vdom

Method	URL	URL Parameters	Body Data	Description
GET	/api/v2/cmdb /firewall/address	?vdom=root&datasource =1&with_meta= 1&skip=1		Retrieve all firewall addresses with datasource, with_meta and skip flag enabled, root vdom
GET	/api/v2/cmdb /firewall/address	?vdom=root&format= name|type		Retrieve all firewall addresses but only show name and type, root vdom
GET	/api/v2/cmdb /firewall/address	?vdom=root&key= type&pattern=fqdn		Retrieve all firewall addresses but only for fqdn type addresses, root vdom
GET	/api/v2/cmdb /firewall/address /address1	?action= select&vdom=root		Retrieve firewall address 'address1', root vdom
POST	/api/v2/cmdb /firewall/address	?vdom=root	{"json": {"name":"address1"}}	Create firewall address 'address1', root vdom
PUT	/api/v2/cmdb /firewall/address /address1	?vdom=root	{"json": {"name":"address2"}}	Edit 'address1' to rename to 'address2', root vdom
PUT	/api/v2/cmdb /firewall/address /address1	?vdom=root	{"json": {"comment":"test comment"}}	Edit 'address1' to modify 'comment' field to 'test comment', root vdom
POST	/api/v2/cmdb /firewall/address /address1	?vdom=root&action= clone&nkey= address1_clone		Clone 'address1' to 'address1_clone', root vdom
PUT	/api/v2/cmdb /firewall/policy/1	?vdom=root&action= move&after=2		Move policy 1 to after policy 2, root vdom
DELETE	/api/v2/cmdb /firewall/address /address1	?vdom=root		Delete firewall address 'address1', root vdom
DELETE	/api/v2/cmdb /firewall/address	?vdom=root		Purge all firewall address, root vdom
POST	/api/v2/cmdb /application/list	?vdom=root	{"json": {"name":"profile1"}}	Create application list profile1, root vdom

Method	URL	URL Parameters	Body Data	Description
PUT	/api/v2/cmdb /application/list /profile1	?vdom=root	{"json":{"entries": [{"id":1},{"id":2}]}}	Edit profile1 to create child table 'entries' with 1 and 2, root vdom
PUT	/api/v2/cmdb /application/list /profile1	?vdom=root	{"json":{"entries": [{"id":1}]}}	Edit profile1 to delete child entry 2, root vdom
PUT	/api/v2/cmdb /application/list /profile1	?vdom=root	{"json":{"entries":[]}}	Edit profile1 to purge child table 'entries', root vdom
PUT	/api/v2/cmdb /application/list /profile1	?vdom=root	{"json":{"entries": [{"id":1,"application": [{"id":31236}, {"id":31237}]}]}}	Edit profile1 to add child object '1' which has child table 'applications', root vdom
GET	/api/v2/cmdb /vpn.ssl/settings	?action=schema		Retrieve schema of vpn ssl settings object
GET	/api/v2/cmdb /vpn.ssl/settings	?action=default		Retrieve default of vpn ssl settings object
GET	/api/v2/cmdb /vpn.ssl/settings	?action=select		Retrieve vpn ssl settings object
PUT	/api/v2/cmdb /vpn.ssl/settings	?vdom=root	{"json":{"port":1443}}	Edit complex object vpn.ssl.settings to modify 'port', root vdom
PUT	/api/v2/cmdb /vpn.ssl/settings	?vdom=root	{"json": {"authentication-rule":[{"id":"1"}, {"id":"2"}]}}	Edit complex object vpn.ssl.settings to create/modify child table, root vdom

Complete documentation

List of Methods

Type	HTTP Methods	Action	Summary
collection	GET		Select all entries in a CLI table.
resource	GET	default	Return the CLI default values for this object type.

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

collection

GET

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

Extra parameters

Name	Type	Summary
datasource	int	Enable to include datasource information for each linked object.
start	int	Starting entry index.
count	int	Maximum number of entries to return.
with_meta	int	Enable to include meta information about each object (type id, references, etc).
skip	int	Enable to call CLI skip operator to hide skipped properties.

Name	Type	Summary
format	string	List of property names to include in results, separated by | (i.e. policyid|srcintf).
key	string	If present, objects will be filtered on property with this name.
pattern	string	If present, objects will be filtered on property with this value.

resource

GET: default

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

GET: schema

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

collection

DELETE

Summary	Delete all objects in this table.
HTTP Method	DELETE

POST

Summary	Create an object in this table.
HTTP Method	POST

resource

GET

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

Extra Parameters

Name	Type	Summary
datasource	int	Enable to include datasource information for each linked object.
with_meta	int	Enable to include meta information about each object (type id, references, etc).
skip	int	Enable to call CLI skip operator to hide skipped properties.
format	string	List of property names to include in results, separated by | (i.e. policyid|srcintf).

PUT

Summary	Update this specific resource.
HTTP Method	PUT

PUT: move

Summary	Move this specific resource.
HTTP Method	PUT
Action	move

Extra Parameters

Name	Type	Summary
before	string	The ID of the resource that this resource will be moved before.
after	string	The ID of the resource that this resource will be moved after.

POST: clone

Summary	Clone this specific resource.
HTTP Method	POST
Action	clone

Extra Parameters

Name	Type	Summary
nkey	string	The ID for the new resource to be created.

DELETE

Summary	Delete this specific resource.
HTTP Method	DELETE

Monitor API

FortiOS supports retrieval and control of dynamic data using the Monitor API. All Monitor API requests start with `/api/v2/monitor/`.

API directive

User can view full Monitor API directive using the following URL (available on debug build only): `https://<FG_IP>/api/v2/monitor`

This directive provides complete documentation of the API usage.

URL format

Here is how the URL is structured for Monitor requests:

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

All GET requests have default action 'select'.

URL parameters

Generic parameters

The following optional URL parameters are generic to all Monitor API requests:

URL Parameter	Example	Description
vdom	/api/v2/monitor/firewall/policy/?vdom=root	Return result for the specified vdom. If vdom parameter is not provided, return current vdom instead. If admin does not have access to the vdom, return permission error.
global	/api/v2/monitor/firewall/policy/?global=1	Return a list of results for all provisioned vdoms. Only return results for vdoms that the admins have access to.

Specific parameters

Each endpoint API may have extra URL parameters unique to the endpoint (see 3.6 for details). Some of those parameters are required for the request to work (Required: True flag). For example, to retrieve the first ten ipv4 sessions:

```
GET /api/v2/monitor/firewall/session?vdom=root&ip_version=ipv4&start=0&count=10
```

Body data

POST requests sometimes require body data which should be included in the request data body. For examples, to close a specific firewall session, need to specify session saddr, daddr, sport, dport, and protocol in the request body:

```
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}
```

GET requests do not accept body data.

Examples

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor			Retrieve schema of Monitor API version2	
GET	/api/v2/monitor /firewall/health	?vdom=root	sysgrp	List configured load balance server health monitors	
GET	/api/v2/monitor /firewall/local-in	?vdom=root	fwgrp.policy	List implicit and explicit local-in firewall policies	
GET	/api/v2/monitor /firewall/policy	?vdom=root	fwgrp.policy	List traffic statistics for all IPv4 policies	
POST	/api/v2/monitor /firewall/policy/reset	?vdom=root	fwgrp.policy	Reset traffic statistics for all IPv4 policies	

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor/firewall/policy/clear_counters	?vdom=root	{'policy': 1}	fwgrp.policy	Reset traffic statistics for one IPv4 policy by policy ID
POST	/api/v2/monitor/firewall/policy/clear_counters	?vdom=root	{'policy': [1, 2]}	fwgrp.policy	Reset traffic statistics for IPv4 policies by policy ID
GET	/api/v2/monitor/firewall/policy6	?vdom=root	fwgrp.policy	List traffic statistics for all IPv6 policies	
POST	/api/v2/monitor/firewall/policy6/reset	?vdom=root	fwgrp.policy	Reset traffic statistics for all IPv6 policies	
POST	/api/v2/monitor/firewall/policy6/clear_counters	?vdom=root	{'policy': 1}	fwgrp.policy	Reset traffic statistics for one IPv6 policy by policy ID
POST	/api/v2/monitor/firewall/policy6/clear_counters	?vdom=root	{'policy': [1, 2]}	fwgrp.policy	Reset traffic statistics for IPv6 policies by policy ID
GET	/api/v2/monitor/firewall/session	?vdom=root&ip_version=ipv4&start=0&count=1&summary=True	sysgrp	List all active firewall sessions (optionally filtered)	
POST	/api/v2/monitor/firewall/session/clear_all	?vdom=root	sysgrp	Immediately clear all active IPv4 and IPv6 sessions	

Method	URL	URL Parameters	Body Data	Access Group	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}	sysgrp	Immediately close a specific session
GET	/api/v2/monitor/firewall/session-top	?vdom=root&report_by=source&sort_by=bytes&src_interface=lan	sysgrp	List of top sessions by specified grouping criteria	
GET	/api/v2/monitor/firewall/shaper	?vdom=root	fwgrp.others	List of statistics for configured firewall shapers	
POST	/api/v2/monitor/firewall/shaper/reset	?vdom=root	fwgrp.others	Reset statistics for all configured traffic shapers	
GET	/api/v2/monitor/firewall/load-balance	?vdom=root&start=0&count=1	fwgrp.others	List all firewall load balance servers	
GET	/api/v2/monitor/fortiview/statistics	?vdom=root&realtime=True	sysgrp	Retrieve drill-down and summary data for FortiView (both realtime and historical)	
GET	/api/v2/monitor/log/stats	?vdom=root&dev=disk	loggrp.data-access	Return number of logs sent by category per day for a specific log device	
POST	/api/v2/monitor/log/stats/reset	?vdom=root	loggrp.data-access	Reset logging statistics for all log devices	

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor/router/ipv4	?vdom=root&start=0&count=1&ip_mask=1.1.1.0/24&gateway=1.1.1.1&type=static&interface=wan1	sysgrp	List all active IPv4 routing table entries	
GET	/api/v2/monitor/router/ipv6	?vdom=root&start=0&count=1&gateway=1::1&type=static&interface=wan1	sysgrp	List all active IPv6 routing table entries	
GET	/api/v2/monitor/router/statistics	?vdom=root&ip_version=4	sysgrp	Retrieve routing table stats, number of matched routes	
POST	/api/v2/monitor/system/dashboard/reboot	?vdom=root	sysgrp	Immediately reboot this device	
POST	/api/v2/monitor/system/dashboard/shutdown	?vdom=root	sysgrp	Immediately shutdown this device	
GET	/api/v2/monitor/system/resource	?vdom=root	sysgrp	Retrieve system resource information, including CPU and memory usage	
GET	/api/v2/monitor/system/dhcp	?vdom=root&ipv6=True	sysgrp	Return a list of all DHCP leases, grouped by interface	
POST	/api/v2/monitor/system/dhcp/revoke	?vdom=root	{'ip': ["1.1.1.1', "1.1.1.2"]}	sysgrp	Revoke a list of IPv4 leases

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor/system/firmware	?vdom=root	sysgrp	Retrieve a list of firmware images available to use for upgrade on this device	
POST	/api/v2/monitor/system/firmware/upgrade	?vdom=root	sysgrp		
GET	/api/v2/monitor/system/modem	?vdom=root	sysgrp	Retrieve statistics for internal/external configured modem	
POST	/api/v2/monitor/system/modem/reset	?vdom=root	sysgrp	Reset statistics for internal/external configured modem	
POST	/api/v2/monitor/system/modem/connect	?vdom=root	sysgrp	Trigger a connect for the configured modem	
POST	/api/v2/monitor/system/modem/disconnect	?vdom=root	sysgrp	Trigger a disconnect for the configured modem	
GET	/api/v2/monitor/system/3g-modem	?vdom=root	sysgrp	List all 3G modems available via FortiGuard	
GET	/api/v2/monitor/system/sniffer	?vdom=root	fwgrp.packet-capture	Return a list of all configured packet captures	
POST	/api/v2/monitor/system/sniffer/restart	?vdom=root	{'mkey': 1}	fwgrp.packet-capture	Restart specified packet capture

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor/system/sniffer/start	?vdom=root	{'mkey': 1}	fwgrp.packet-capture	Start specified packet capture
POST	/api/v2/monitor/system/sniffer/stop	?vdom=root	{'mkey': 1}	fwgrp.packet-capture	Stop specified packet capture
GET	/api/v2/monitor/system/fsw	?vdom=root&fsw_id=FSW12345	sysgrp	Retrieve statistics for configured FortiSwitches	
POST	/api/v2/monitor/system/fsw/update	?vdom=root	sysgrp		
GET	/api/v2/monitor/system/interface	?vdom=root&interface_name=lan&include_vlan=True	netgrp	Retrieve statistics for all system interfaces	
GET	/api/v2/monitor/system/debug	?vdom=root		Log debug messages to the console (if enabled)	
GET	/api/v2/monitor/extender-controller/extender	?vdom=root&id=[1,2]	netgrp	Retrieve statistics for specific configured FortiExtender units	
POST	/api/v2/monitor/extender-controller/extender/reset	?vdom=root	netgrp		
GET	/api/v2/monitor/user/firewall	?vdom=root&start=0&count=1&ipv4=True&ipv6=True	admingrp	List authenticated firewall users	
POST	/api/v2/monitor/user/firewall/deauth	?vdom=root	admingrp	Deauthenticate all firewall users	

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor/user/banned	?vdom=root	admingrp	Return a list of all banned users by IP	
POST	/api/v2/monitor/user/banned/clear_users	?vdom=root	{'ip_addresses': ["1.1.1.1"], 'ipv6': True}	admingrp	Immediately clear a list of specific banned users by IP
POST	/api/v2/monitor/user/banned/clear_all	?vdom=root	admingrp	Immediately clear all banned users	
POST	/api/v2/monitor/user/fortitoken/activate	?vdom=root	authgrp	Activate all FortiTokens	
POST	/api/v2/monitor/user/fortitoken/activate	?vdom=root	{'tokens': [1, 2]}	authgrp	Activate a set of FortiTokens by serial number
POST	/api/v2/monitor/user/fortitoken/refresh	?vdom=root	authgrp	Refresh all FortiTokens	
POST	/api/v2/monitor/user/fortitoken/refresh	?vdom=root	{'tokens': [1, 2]}	authgrp	Refresh a set of FortiTokens by serial number
POST	/api/v2/monitor/user/fortitoken/provision	?vdom=root	authgrp	Provision all FortiTokens	
POST	/api/v2/monitor/user/fortitoken/provision	?vdom=root	{'tokens': [1, 2]}	authgrp	Provision a set of FortiTokens by serial number
GET	/api/v2/monitor/utm/av	?vdom=root	utmgrp.antivirus	Retrieve AntiVirus statistics	

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor/utm/av/reset	?vdom=root	utmgrp.antivirus	Reset AntiVirus statistics	
GET	/api/v2/monitor/utm/web	?vdom=root	utmgrp.webfilter	Retrieve WebFilter statistics	
POST	/api/v2/monitor/utm/web/reset	?vdom=root	utmgrp.webfilter	Reset WebFilter statistics	
GET	/api/v2/monitor/utm/web-cat	?vdom=root	utmgrp.webfilter	Retrieve WebFilter category statistics	
POST	/api/v2/monitor/utm/web-cat/reset	?vdom=root	utmgrp.webfilter	Reset WebFilter category statistics	
GET	/api/v2/monitor/utm/email	?vdom=root	utmgrp.spamfilter	Retrieve Email Filter category statistics	
POST	/api/v2/monitor/utm/email/reset	?vdom=root	utmgrp.spamfilter	Reset Email Filter category statistics	
GET	/api/v2/monitor/utm/dlp	?vdom=root	utmgrp.data-loss-prevention	Retrieve DLP statistics	
POST	/api/v2/monitor/utm/dlp/reset	?vdom=root	utmgrp.data-loss-prevention	Reset DLP statistics	
GET	/api/v2/monitor/utm/rating-lookup	?vdom=root&url='www.url1.com'	utmgrp.webfilter	Lookup FortiGuard rating for a specific URL	
GET	/api/v2/monitor/utm/rating-lookup	?vdom=root&url=['www.url1.com', 'www.url2.com']	utmgrp.webfilter	Lookup FortiGuard rating for a specific URL	

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor/utm/app	?vdom=root	utmgrp.application-control	Retrieve application control statistics	
POST	/api/v2/monitor/utm/app/reset	?vdom=root	utmgrp.application-control	Reset application control statistics	
POST	/api/v2/monitor/utm/app-lookup	?vdom=root	{'address': "1.1.1.1"}	any	Query FortiFlow database to resolve hosts to app control entries
GET	/api/v2/monitor/webfilter/override	?vdom=root	utmgrp.webfilter	List all administrative and user initiated webfilter overrides	
POST	/api/v2/monitor/webfilter/override/delete	?vdom=root	utmgrp.webfilter		
GET	/api/v2/monitor/visibility/device-type-dist	?vdom=root	sysgrp	Retrieve a breakdown of detected devices by type	
GET	/api/v2/monitor/visibility/device-os-dist	?vdom=root	sysgrp	Retrieve a breakdown of detected devices by operating system	
GET	/api/v2/monitor/visibility/device-list	?vdom=root&os_name=android	sysgrp	Retrieve a list of detected devices	
GET	/api/v2/monitor/vpn/ipsec	?vdom=root&start=0&count=1	vpngrp	Return an array of active IPsec VPNs	

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor/vpn/ipsec/tunnel_up	?vdom=root	vpngrp	Bring up a specific IPsec VPN tunnel	
POST	/api/v2/monitor/vpn/ipsec/tunnel_down	?vdom=root	vpngrp	Bring down a specific IPsec VPN tunnel	
POST	/api/v2/monitor/vpn/ipsec/tunnel_reset_stats	?vdom=root	vpngrp	Reset statistics for a specific IPsec VPN tunnel	
GET	/api/v2/monitor/vpn/auto-ipsec	?vdom=root	vpngrp	Retrieve a list of all auto-IPsec tunnels	
POST	/api/v2/monitor/vpn/auto-ipsec/accept	?vdom=root	vpngrp		
POST	/api/v2/monitor/vpn/auto-ipsec/reject	?vdom=root	vpngrp		
GET	/api/v2/monitor/vpn/ssl	?vdom=root	vpngrp	Retrieve a list of all SSL-VPN sessions and sub-sessions	
POST	/api/v2/monitor/vpn/ssl/clean_tunnel	?vdom=root	vpngrp		
POST	/api/v2/monitor/vpn/ssl/delete	?vdom=root	vpngrp		
GET	/api/v2/monitor/wanopt/peer_stats	?vdom=root	wanoptgrp	Retrieve a list of WAN opt peer statistics	
POST	/api/v2/monitor/wanopt/peer_stats/reset	?vdom=root	wanoptgrp	Reset WAN opt peer statistics	

Method	URL	URL Parameters	Body Data	Access Group	Description
GET	/api/v2/monitor/webcache/stats	?vdom=root	wanoptgrp	Retrieve webcache statistics	
POST	/api/v2/monitor/webcache/stats/reset	?vdom=root	wanoptgrp	Reset all webcache statistics	
GET	/api/v2/monitor/wifi/client	?vdom=root&start=0&count=1&type=all	wifi	Retrieve a list of connected WiFi clients	
GET	/api/v2/monitor/wifi/managed_ap	?vdom=root&incl_local=True	wifi	Retrieve a list of managed FortiAPs	
POST	/api/v2/monitor/wifi/managed_ap/set_status	?vdom=root	wifi		
GET	/api/v2/monitor/wifi/ap_status	?vdom=root	wifi	Retrieve statistics for all managed FortiAPs	
GET	/api/v2/monitor/wifi/interfering_ap	?vdom=root	wifi	Retrieve a list of interferring APs for one FortiAP	
GET	/api/v2/monitor/wifi/euclid	?vdom=root	wifi	Retrieve presence analytics statistics	
POST	/api/v2/monitor/wifi/euclid/reset	?vdom=root	wifi		
GET	/api/v2/monitor/wifi/rogue_ap	?vdom=root&start=0&count=1	wifi	Retrieve a list of detected rogue APs	
POST	/api/v2/monitor/wifi/rogue_ap/clear_all	?vdom=root	wifi		

Method	URL	URL Parameters	Body Data	Access Group	Description
POST	/api/v2/monitor /wifi/rogue_ap /set_status	?vdom=root	wifi		
POST	/api/v2/monitor /wifi/rogue_ap /restart	?vdom=root	wifi		
GET	/api/v2/monitor /wifi/spectrum	?vdom=root	wifi	Retrieve spectrum analysis information for a specific FortiAP	

Complete documentation

List of Methods

URI	HTTP Method	Summary
/firewall/health/	GET	List configured load balance server health monitors.
/firewall/local-in/	GET	List implicit and explicit local-in firewall policies.
/firewall/policy/	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/	GET	List traffic statistics for all IPv6 policies.
/firewall/policy6/reset/	POST	Reset traffic statistics for all IPv6 policies.
/firewall/policy6/clear_ counters/	POST	Reset traffic statistics for one or more IPv6 policies by policy ID.
/firewall/session/	GET	List all active firewall sessions (optionally filtered).
/firewall/session/clear_all/	POST	Immediately clear all active IPv4 and IPv6 sessions.

URI	HTTP Method	Summary
/firewall/session/close/	POST	
/firewall/session-top/	GET	List of top sessions by specified grouping criteria.
/firewall/shaper/	GET	List of statistics for configured firewall shapers.
/firewall/shaper/reset/	POST	Reset statistics for all configured traffic shapers.
/firewall/load-balance/	GET	List all firewall load balance servers.
/firewall/anomaly/	GET	List active IPv4 DoS anomaly meters.
/firewall/anomaly6/	GET	List active IPv6 DoS anomaly meters.
/fortiview/statistics/	GET	Retrieve drill-down and summary data for FortiView (both realtime and historical).
/fortiview/sandbox-file-details/	GET	Retrieve FortiSandbox analysis details for a specific file checksum.
/log/stats/	GET	Return number of logs sent by category per day for a specific log device.
/log/stats/reset/	POST	Reset logging statistics for all log devices.
/router/ipv4/	GET	List all active IPv4 routing table entries.
/router/ipv6/	GET	List all active IPv6 routing table entries.
/router/statistics/	GET	Retrieve routing table statistics, including number of matched routes.
/system/dashboard/reboot/	POST	Immediately reboot this device.
/system/dashboard/shutdown/	POST	Immediately shutdown this device.
/system/resource/	GET	Retrieve system resource information, including CPU and memory usage.
/system/dhcp/	GET	Return a list of all DHCP leases, grouped by interface.
/system/dhcp/revoke/	POST	Revoke a list of IPv4 leases.
/system/firmware/	GET	Retrieve a list of firmware images available to use for upgrade on this device.
/system/firmware/upgrade/	POST	

URI	HTTP Method	Summary
/system/fsck/start/	POST	Reboot the device and immediately start file system check utility.
/system/modem/	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/	GET	List all 3G modems available via FortiGuard.
/system/sniffer/	GET	Return a list of all configured packet captures.
/system/sniffer/restart/	POST	Restart specified packet capture.
/system/sniffer/start/	POST	Start specified packet capture.
/system/sniffer/stop/	POST	Stop specified packet capture.
/system/fsw/	GET	Retrieve statistics for configured FortiSwitches.
/system/fsw/update/	POST	
/system/interface/	GET	Retrieve statistics for all system interfaces.
/system/debug/	GET	Log debug messages to the console (if enabled).
/extender-controller/extender/	GET	Retrieve statistics for specific configured FortiExtender units.
/extender-controller/extender/reset/	POST	
/user/firewall/	GET	List authenticated firewall users.
/user/firewall/deauth/	POST	Deauthenticate all firewall users.
/user/banned/	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.

URI	HTTP Method	Summary
/user/fortitoken/activate/	POST	Activate a set of FortiTokens by serial number.
/user/fortitoken/refresh/	POST	Refresh a set of FortiTokens by serial number.
/user/fortitoken/provision/	POST	Provision a set of FortiTokens by serial number.
/utm/av/	GET	Retrieve Antivirus statistics.
/utm/av/reset/	POST	Reset Antivirus statistics.
/utm/web/	GET	Retrieve WebFilter statistics.
/utm/web/reset/	POST	Reset WebFilter statistics.
/utm/web-cat/	GET	Retrieve WebFilter category statistics.
/utm/web-cat/reset/	POST	Reset WebFilter category statistics.
/utm/email/	GET	Retrieve Email Filter statistics.
/utm/email/reset/	POST	Reset Email Filter statistics.
/utm/dlp/	GET	Retrieve DLP statistics.
/utm/dlp/reset/	POST	Reset DLP statistics.
/utm/rating-lookup/	GET	Look up FortiGuard rating for a specific URL.
/utm/app/	GET	Retrieve application control statistics.
/utm/app/reset/	POST	Reset application control statistics.
/utm/app-lookup/	GET	Query remote FortiFlow database to resolve hosts to application control entries.
/webfilter/override/	GET	List all administrative and user initiated webfilter overrides.
/webfilter/override/delete/	POST	
/visibility/device-type-dist/	GET	Retrieve a breakdown of detected devices by type.
/visibility/device-os-dist/	GET	Retrieve a breakdown of detected devices by operating system.
/visibility/device-list/	GET	Retrieve a list of detected devices.

URI	HTTP Method	Summary
/vpn/ipsec/	GET	Return an array of active IPsec VPNs.
/vpn/ipsec/tunnel_up/	POST	Bring up a specific IPsec VPN tunnel.
/vpn/ipsec/tunnel_down/	POST	Bring down a specific IPsec VPN tunnel.
/vpn/ipsec/tunnel_reset_stats/	POST	Reset statistics for a specific IPsec VPN tunnel.
/vpn/auto-ipsec/	GET	Retrieve a list of all auto-IPsec tunnels.
/vpn/auto-ipsec/accept/	POST	
/vpn/auto-ipsec/reject/	POST	
/vpn/ssl/	GET	Retrieve a list of all SSL-VPN sessions and sub-sessions.
/vpn/ssl/clean_tunnel/	POST	
/vpn/ssl/delete/	POST	
/wanopt/peer_stats/	GET	Retrieve a list of WAN opt peer statistics.
/wanopt/peer_stats/reset/	POST	Reset WAN opt peer statistics.
/webcache/stats/	GET	Retrieve webcache statistics.
/webcache/stats/reset/	POST	Reset all webcache statistics.
/wifi/client/	GET	Retrieve a list of connected WiFi clients.
/wifi/managed_ap/	GET	Retrieve a list of managed FortiAPs.
/wifi/managed_ap/set_status/	POST	
/wifi/ap_status/	GET	Retrieve statistics for all managed FortiAPs.
/wifi/interfering_ap/	GET	Retrieve a list of interferring APs for one FortiAP radio.
/wifi/euclid/	GET	Retrieve presence analytics statistics.
/wifi/euclid/reset/	POST	
/wifi/rogue_ap/	GET	Retrieve a list of detected rogue APs.
/wifi/rogue_ap/clear_all/	POST	
/wifi/rogue_ap/set_status/	POST	

URI	HTTP Method	Summary
/wifi/rogue_ap/restart/	POST	
/wifi/spectrum/	GET	Retrieve spectrum analysis information for a specific FortiAP.

firewall

health: select

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

policy: select

Summary	List traffic statistics for all IPv4 policies.
URI	/firewall/policy/
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
policy	array	Array of policy IDs to reset.
policy	int	Single policy ID to reset.

policy6: select

Summary	List traffic statistics for all IPv6 policies.
URI	/firewall/policy6/
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
policy	array	Array of policy IDs to reset.
policy	int	Single policy ID to reset.

session: select

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

Extra parameters

Name	Type	Summary
ip_version	string	IP version [*ipv4 | ipv6 | ipboth].
start	int	Starting entry index.
count	int	Maximum number of entries to return.
summary	boolean	Enable/disable inclusion of session summary (setup rate, total sessions, etc).

session-top: 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-top: close

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

session-top: select

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

Response Type	array

Extra parameters

Name	Type	Summary
report_by	string	Criteria to group results by [source*|destination|application|web-category|web-domain].
sort_by	string	Criteria to sort results by [bytes|msg-counts].
count	int	Maximum number of entries to return.
filter	object	A map of filter keys to string values. The key(s) may be src_interface, source, dst_interface, destination, policyid, application, web_category_id, web_domain.
srcintf	string	Filter: by source interface name.
source	string	Filter: by source IP.
dstintf	string	Filter: by destination interface name.
destination	string	Filter: by destination IP.
policyid	int	Filter: by policy ID.
application	int	Filter: by application ID.
web_category_id	string	Filter: by webfilter category name.
web_domain	string	Filter: by web domain name.

shaper: select

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

Extra parameters

Name	Type	Summary
start	int	Starting entry index.
count	int	Maximum number of entries to return.

anomaly: select

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

anomaly6: select

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

fortiview

statistics: select

Summary	Retrieve drill-down and summary data for FortiView (both realtime and historical).
URI	/fortiview/statistics/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary
realtime	boolean	Set to true to retrieve realtime results (from kernel).
filter	object	A map of filter keys to arrays of values.

sandbox-file-details: select

Summary	Retrieve FortiSandbox analysis details for a specific file checksum.
URI	/fortiview/sandbox-file-details/
HTTP Method	GET
Action	select

Access Group	sysgrp
Response Type	object

Extra parameters

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

log

status: select

Summary	Return number of logs sent by category per day for a specific log device.
URI	/log/stats/
HTTP Method	GET
Action	select
Access Group	loggrp.data-access
Response Type	array

Extra parameters

Name	Type	Summary
dev	string	Log device [*memory | disk | fortianalyzer | fortiguard].

status: reset

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

router

ipv4: select

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

Extra parameters

Name	Type	Summary
start	int	Starting entry index.
count	int	Maximum number of entries to return.
ip_mask	string	Filter: IP/netmask.
gateway	string	Filter: gateway.
type	string	Filter: route type.
interface	string	Filter: interface name.

ipv6: select

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

Extra parameters

Name	Type	Summary
start	int	Starting entry index.
count	int	Maximum number of entries to return.
ip_mask	string	Filter: IP/netmask.
gateway	string	Filter: gateway.
type	string	Filter: route type.
interface	string	Filter: interface name.

statistics: select

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

Extra parameters

Name	Type	Summary
ip_version	int	IP version (4|6). If not present, IPv4 and IPv6 will be returned.
ip_mask	string	Filter: IP/netmask.
gateway	string	Filter: gateway.
type	string	Filter: route type.
interface	string	Filter: interface name.

system

dashboard: reboot

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

dashboard: shutdown

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

resource: select

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

dhcp: select

Summary	Return a list of all DHCP leases, grouped by interface.
URI	/system/dhcp/
HTTP Method	GET

Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary
ipv6	boolean	Include IPv6 DHCP leases in addition to IPv4 leases.

dhcp: revoke

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

Extra parameters

Name	Type	Summary
ip	array	List of IPv4 addresses to revoke leases for.

firmware: select

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

firmware: upgrade

URI	/system/firmware/upgrade/

HTTP Method	POST
Action	upgrade
Access Group	sysgrp

fsck: start

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

modem: select

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

sniffer: select

Summary	Return a list of all configured packet captures.
URI	/system/sniffer/
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
mkey	int	ID of packet capture entry.

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
mkey	int	ID of packet capture entry.

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
mkey	int	ID of packet capture entry.

fsw:select

Summary	Retrieve statistics for configured FortiSwitches.
URI	/system/fsw/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary
fsw_id	string	Filter: FortiSwitch ID

fsw:update

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

interface:select

Summary	Retrieve statistics for all system interfaces.
URI	/system/interface/

HTTP Method	GET
Action	select
Access Group	netgrp
Response Type	array

Extra parameters

Name	Type	Summary
interface_name	string	Filter: interface name.
include_vlan	boolean	Enable to include VLANs in result list.

debug:select

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

Extra parameters

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

extender - controller

extender - select

Summary	Retrieve statistics for specific configured FortiExtender units.
URI	/extender-controller/extender/

HTTP Method	GET
Action	select
Access Group	netgrp
Response Type	array

Extra parameters

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

extender - reset

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

user

firewall: select

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

Extra parameters

Name	Type	Summary
start	int	Starting entry index.

Name	Type	Summary
count	int	Maximum number of entries to return.
ipv4	boolean	Include IPv4 user (default=true).
ipv6	boolean	Include IPv6 users.

firewall: deauth

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

banned: select

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

banned: clear_users

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

Extra parameters

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

banned: add_users

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

Extra parameters

Name	Type	Summary
ip_addresses	array	List of IP Addresses to ban. IPv4 and IPv6 addresses are allowed.
expiry	int	Time until expiry in seconds. 0 for indefinite ban.

banned: clear_all

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

fortitoken: activate

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

Action	activate
Access Group	authgrp
Response Type	array

Extra parameters

Name	Type	Summary
tokens	array	List of FortiToken serial numbers to activate. If omitted, all tokens will be used.

fortitoken: refresh

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

Extra parameters

Name	Type	Summary
tokens	array	List of FortiToken serial numbers to refresh. If omitted, all tokens will be used.

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
tokens	array	List of FortiToken serial numbers to provision. If omitted, all tokens will be used.

utm

av: select

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

av: reset

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

web: select

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

web: reset

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

web-cat: select

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

web-cat: reset

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

email: select

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

email: reset

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

dlp: select

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

Extra parameters

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

dlp: reset

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

rating-lookup: select

Summary	Lookup FortiGuard rating for a specific URL.
URI	/utm/rating-lookup/

HTTP Method	GET
Action	select
Access Group	utmgrp.application-control
Response Type	object

Extra parameters

Name	Type	Summary
url	string	URL to query.
url	array	List of URLs to query.

app: select

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

app: reset

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

app-lookup: select

Summary	Query remote FortiFlow database to resolve hosts to application control entries.
URI	/utm/app-lookup/

HTTP Method	GET
Action	select
Access Group	any
Response Type	array

Extra parameters

Name	Type	Summary
hosts	array	List of hosts to resolve.
address	string	Destination IP for one host entry.
dst_port	int	Destination port for one host entry.
protocol	int	Protocol for one host entry.

webfilter

override: select

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

override: delete

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

visibility

device-type-dist: select

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

Extra parameters

Name	Type	Summary
include_joined	string	Include joined devices (devices with more than 1 MAC address).

device-os-dist: select

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

Extra parameters

Name	Type	Summary
include_joined	string	Include joined devices (devices with more than 1 MAC address).

device-list: select

Summary	Retrieve a list of detected devices.

URI	/visibility/device-list/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	array

Extra parameters

Name	Type	Summary
os_name	string	Filter: operating system name.
type_name	string	Filter: device type name.
include_joined	string	Include joined devices (devices with more than 1 MAC address).

vpn

ipsec:select

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

Extra parameters

Name	Type	Summary
tunnel	string	Filter for a specific IPsec tunnel name.
start	int	Starting entry index.
count	int	Maximum number of entries to return.

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
p1name	string	IPsec phase1 name.
p2name	string	IPsec phase2 name.
p2serial	string	IPsec phase2 serial.

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
p1name	string	IPsec phase1 name.
p2name	string	IPsec phase2 name.
p2serial	string	IPsec phase2 serial.

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
p2name	string	IPsec phase2 name.

auto-ipsec: select

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

auto-ipsec: accept

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

auto-ipsec: reject

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

ssl: select

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

ssl: clean_tunnel

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

ssl: delete

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

wanopt

peer_stats: select

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

peer_stats: reset

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

webcache

stats: select

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

Extra Parameters

Name	Type	Summary
period	string	Statistics period [10min|hour|day|month].

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/
HTTP Method	GET
Action	select
Access Group	wifi
Response Type	array

Extra parameters

Name	Type	Summary
start	int	Starting entry index.
count	int	Maximum number of entries to return.
type	string	Request type [all*|fail-login].

managed_ap: select

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

Extra Parameters

Name	Type	Summary
wtp_id	string	Filter: single managed FortiAP by ID.
incl_local	boolean	Enable to include the local FortiWiFi device in the results.

managed_ap: set_status

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

ap_status: select

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

interfering_ap: select

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

Extra Parameters

Name	Type	Summary
wtp	string	FortiAP ID to query.
radio	int	Radio ID.
start	int	Starting entry index.
count	int	Maximum number of entries to return.

euclid: select

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

euclid: reset

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

rogue_ap: select

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

Extra Parameters

Name	Type	Summary
start	int	Starting entry index.
count	int	Maximum number of entries to return.

rogue_ap: clear_all

URI	/wifi/rogue_ap/clear_all

HTTP Method	POST
Action	clear_all
Access Group	wifi

rogue_ap: set_status

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

rogue_ap: restart

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

spectrum: select

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

Extra Parameters

Name	Type	Summary
wtp_id	string	FortiAP ID to query

FORTINET®

High Performance Network Security