FortiOS REST API

VERSION 5.2.3

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 24, 2015

FortiOS 5.2.3 REST API

05-523-270937-201500324

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-03-05	Initial release.
2015-03-10	Updated for formatting and styling issues.
2015-03-24	Updated the authentication section.

Introduction

This document provides the REST API information supported in FortiOS version 5.2.3. 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 FGT (FortiGate)

Authentication

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

1. A valid authentication token.
2. Appropriate permissions for the requested object.
3. A valid CSRF token (for `HTTP POST`/`PUT`/`DELETE` methods (`HTTP GET` does not require CSRF token)).

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.

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.

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.

FortiOS REST API HTTP Response Codes

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

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.
424	Failed Dependency.
500	Internal Server Error.

CMDB API

FortiOS supports retrieval and modification of CLI configuration using the CMDB API. The CMDB API can be accessed using the following URL:

```
https://192.168.1.99/api/v2/cmdb
```

Example: CMDB API on firewall address and policy object

Request

```
{
   "http_method":"GET"
},
```

Response

```
{
   "type":"array"
}
},
{
   "path":"firewall",
   "name":"local-in",
   "action":"select",
   "access_group":"fwgrp.policy",
   "summary":"List implicit and explicit local-in
```

URL format

The URL for CMDB REST API has the following URL format.

Resource path	Description
path	Collection "path" (Required)
name	Collection "name" (Required)
mkey	The unique name/ID of a specific resource to query

For example; to retrieve a list of all configured IPV4 firewall policies use the following URL:

```
https://192.168.1.99/api/v2/cmdb/firewall/policy/
```

Or else, you could also retrieve only firewall policy ID 1 using this URL:

```
https://192.168.1.99/api/v2/cmdb/firewall/policy/1/
```

The path & name values above directly map to the CLI syntax on FortiOS. The following table lists some of the url, path, and name retrieved for a CMDB API:

Examples: CMDB API URL

CLI	URL	Path	Name
configure firewall policy	/api/v2/cmdb/firewall/policy/	firewall	policy
configure firewall policy6	/api/v2/cmdb/firewall/policy6/	firewall	policy6
/api/v2/cmdb/firewall/policy	/api/v2/cmdb/firewall/policy/	firewall	policy
configure firewall schedule recurring	/api/v2/cmdb/firewall.schedule/recurring/	firewall schedule	recurring

Parameters

The following optional parameters can be specified for any of the supported APIs.

Additionally, each API may have a list of parameters that are specific to that API. These parameters will be documented with the individual API methods.

Parameter	Example	Description
VDOM	/api/v2/cmdb/firewall/policy/?vdom=root	Use the provided VDOM name for this request only. Administrator must have management rights for the specified VDOM.
Action	/api/v2/cmdb/firewall/policy/?action=schema	Perform a specific action on this resource. Supported actions are listed in the resources section.

List of Methods

Type	HTTP Methods	Action	Summary
Collection	GET		Select all entries in a CLI table.
	GET	default	Return the CLI default values for this object type.
	GET	schema	Return the CLI schema for this object type.
	POST		
	DELETE		Delete all objects in this table.
Resource	GET		Select a specific entry from a CLI table.
	PUT	move	Move this specific resource.
	POST	clone	Clone this specific 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	boolean	Enable to include datasource information for each linked object.
start	int	Starting entry index.
count	int	Maximum number of entries to return.
with_meta	boolean	Enable to include meta information about each object (type id, references, etc).
skip	boolean	Enable to call CLI skip operator to hide skipped properties.
format	boolean	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.

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

DELETE

Summary	Delete all objects in this table.
HTTP Method	DELETE

POST

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

PUT

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 resouce 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. The monitor API can be accessed using the following URL:

```
https://192.168.1.99/api/v2/monitor
```

URL format

The URL for API has the following format:

Resource Path	Description
path	Resource "path" (see list of resources)
name	Resource "name" (see list of resources)
action	Action for specified resource (see list of resources). (Optional: Defaults to "select")
mkey	The name/ID of the resource to query. (Optional)

Parameters

The following optional parameters can be specified for any of the supported APIs.

Parameter Name	Example	Description
vdom	/api/v2/monitor/firewall/policy/?vdom=root	Use the provided VDOM name for this request only. Administrator must have management rights to specified VDOM.

Additionally, each API may have a list of parameters that are specific to that API. These parameters will be documented with the individual API methods.

List of Methods

URL	HTTP Method	Summary
/firewall/health/	GET	List configured load balance server health monitors.

URL	HTTP Method	Summary
/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.
/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.
/fortiview/statistics/	GET	Retrieve drill-down and summary data for FortiView (both realtime and historical).
/log/stats/	GET	Return number of logs sent by category per day for a specific log device.

URL	HTTP Method	Summary
/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	
/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.

URL	HTTP Method	Summary
/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/clear_all/	POST	Immediately clear all banned users.
/user/fortitoken/activate/	POST	Activate a set of FortiTokens by serial number.
/user/fortitoken/refresh/	POST	Refresh a set of FortiTokens by serial number.

URL	HTTP Method	Summary
/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	Lookup 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.

URL	HTTP Method	Summary
/visibility/device-os-dist/	GET	Retrieve a breakdown of detected devices by operating system.
/visibility/device-list/	GET	Retrieve a list of detected devices.
/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 .

URL	HTTP Method	Summary
/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 .
/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	
/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.
URL	/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.
URL	/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.
URL	/firewall/policy/
HTTP Method	GET
Action	select

Access Group	fwgrp.policy

policy: reset

Summary	Reset traffic statistics for all IPv4 policies.
URL	/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.
URL	/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.

URL	/firewall/policy6/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

policy6: reset

Summary	Reset traffic statistics for one or more IPv6 policies by policy ID.
URL	/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.
URL	/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).
URL	/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.
URL	/firewall/session/clear_all/
HTTP Method	POST
Action	clear_all
Access Group	sysgrp
Response type	int

session-top: close

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

session-top: select

Summary	List of top sessions by specified grouping criteria.
URL	/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.
src_interface	string	Filter: by source interface name.
source	string	Filter: by source IP.
dst_interface	string	Filter: by destination interface name.
destination	string	Filter: by destination IP.

Name	Type	Summary
policy_id	int	Filter: by policy ID.
app_id	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.
URL	/firewall/shaper/
HTTP Method	GET
Action	select
Access Group	fwgrp.others
Response Type	array

shaper: reset

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

load-balance: select

Summary	List all firewall load balance servers.
URL	/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.

fortiview

statistics: select

Summary	Retrieve drill-down and summary data for FortiView (both realtime and historical).
URL	/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).

log

status: select

Summary	Return number of logs sent by category per day for a specific log device.
URL	/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.
URL	/log/stats/reset/
HTTP Method	POST
Action	reset
Access Group	loggrp.data-access

router

ipv4: select

Summary	List all active IPv4 routing table entries.
URL	/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.
URL	/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.
URL	/router/statistics/
HTTP Method	GET
Action	select
Access Group	sysgrp
Response Type	object

Extra parameters

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

Name	Type	Summary
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.
URL	/system/dashboard/reboot/
HTTP Method	POST
Action	reboot
Access Group	sysgrp

dashboard: shutdown

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

resource: select

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

dhcp: select

Summary	Return a list of all DHCP leases, grouped by interface.
URL	/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.
URL	/system/dhcp/revoke/
HTTP Method	POST
Action	revoke
Access Group	sysgrp

Extra parameters

Name	Type	Summary
id	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.
URL	/system/firmware/
HTTP Method	GET
Action	select
Access Group	sysgrp

firmware: upgrade

URL	/system/firmware/upgrade/
HTTP Method	POST
Action	upgrade
Access Group	sysgrp

modem: select

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

modem: reset

Summary	Reset statistics for internal/external configured modem.

URL	/system/modem/reset
HTTP Method	POST
Action	reset
Access Group	sysgrp

modem: connect

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

modem: disconnect

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

3g-modem: select

Summary	List all 3G modems available via FortiGuard
URL	/system/3g-modem/
HTTP Method	GET

Action	select
Access Group	sysgrp

sniffer: select

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

sniffer: restart

Summary	Restart specified packet capture.
URL	/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.
URL	/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.
URL	/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
URL	/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

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

interface:select

Summary	Retrieve statistics for all system interfaces.
URL	/system/interface/
HTTP Method	GET
Action	select

Access Group	netgrp
Response Type	array

Extra parameters

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

fsw: update

URL	/system/fsw/update/
HTTP Method	POST
Action	update
Access Group	netgrp

interface:select

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

Extra parameters

Name	Type	Summary
interface_name boolean	string	Filter: interface name.

Name	Type	Summary
include_vlan	boolean	Enable to include VLANs in result list.

debug:select

Summary	Log debug messages to the console (if enabled).
URL	/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.
URL	/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

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

user

firewall: select

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

firewall: deauth

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

banned: select

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

banned: clear_users

Summary	Immediately clear a list of specific banned users by IP.
URL	/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. Each entry in the array must be an object with the 'ip' property set to the IP of the banned user.
ipv6	boolean	IPv6 flag that can be set per IP address listed in 'ip_addresses'.

banned: clear_all

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

fortitoken: activate

Summary	Activate a set of FortiTokens by serial number.

URL	/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.
URL	/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.
URL	/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.
URL	/utm/av/
HTTP Method	GET
Action	select
Access Group	utmgrp.antivirus

av: reset

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

web-cat: select

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

web-cat: reset

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

email: select

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

email: reset

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

dlp: select

Summary	Reset DLP statistics.

URL	/utm/dlp/
HTTP Method	GEt
Action	select
Access Group	utmgrp.data-loss-prevention.

dlp: reset

Summary	Reset DLP statistics.
URL	/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.
URL	/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.
URL	/utm/app/
HTTP Method	GET
Action	select
Access Group	utmgrp.application-control

app: reset

Summary	Reset application control statistics.
URL	/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.
URL	/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.
URL	/webfilter/override/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter

override: delete

URL	/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.
URL	/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.
URL	/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.
URL	/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
URL	/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.
URL	/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.
URL	/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.
URL	/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.
URL	/vpn/auto-ipsec/
HTTP Method	GETw
Action	select
Access Group	vpngrp

auto-ipsec: accept

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

auto-ipsec: reject

URL	/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

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

wanopt

peer_stats: select

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

peer_stats: reset

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

webcache

stats: select

Summary	Retrieve webcache statistics.
URL	/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.
URL	/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
URL	/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

Summary	Retrieve statistics for all managed FortiAPs.
URL	/wifi/managed_ap/set_status/
HTTP Method	POST
Action	set_status

ap_status: select

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

interfering_ap: select

Summary	Retrieve a list of interferring APs for one FortiAP.
URL	/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_id	int	Radio ID.

euclid: select

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

euclid: reset

URL	/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

URL	/wifi/rogue_ap/clear_all
HTTP Method	POST
Action	clear_all
Access Group	wifi

rogue_ap: set_status

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

rogue_ap: restart

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

spectrum: select

Summary	Retrieve spectrum analysis information for a specific FortiAP .
URL	/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