



# FortiOS - REST API Reference

VERSION 5.4.0

**FORTINET DOCUMENT LIBRARY**

<http://docs.fortinet.com>

**FORTINET VIDEO GUIDE**

<http://video.fortinet.com>

**FORTINET BLOG**

<https://blog.fortinet.com>

**CUSTOMER SERVICE & SUPPORT**

<https://support.fortinet.com>

**FORTIGATE COOKBOOK**

<http://cookbook.fortinet.com>

**FORTINET TRAINING SERVICES**

<http://www.fortinet.com/training>

**FORTIGUARD CENTER**

<http://www.fortiguard.com>

**END USER LICENSE AGREEMENT**

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

**FEEDBACK**

Email: [techdocs@fortinet.com](mailto:techdocs@fortinet.com)



December 18, 2015

FortiOS 5.4.0 REST API Reference

05-540-270937-20151218

# TABLE OF CONTENTS

<b>Change Log</b>	<b>5</b>
<b>Introduction</b>	<b>6</b>
Authentication	6
CSRF Tokens	6
Setting Up an Authenticated Session	7
Logging out of an Authenticated Session	7
FortiManager support	7
Supported HTTP methods	7
Response codes	8
Debugging	8
<b>CMDB API</b>	<b>10</b>
URL format	10
Parameters	11
List of Methods	11
collection	12
resource	13
collection	14
resource	14
<b>Monitor API</b>	<b>16</b>
URL format	16
Parameters	16
List of Methods	17
endpoint-control	23
firewall	27
fortiview	35
log	36
router	38
system	40
extender - controller	55
user	56
utm	60
virtual-wan	61
webfilter	62
vpn	63

wanopt .....	66
webcache .....	66
wifi .....	67
switch-controller .....	71

## Change Log

Date	Change Description
2015-12-18	Initial Release

# Introduction

This document provides the REST API information supported in FortiOS version 5.2.4. 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 FG (FortiGate)

## 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.

<b>Login URL</b>	<code>/logincheck</code>
<b>Username POST Variable</b>	<code>username</code>
<b>Password POST Variable</b>	<code>secretkey</code>

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.

<b>Logout URL</b>	<code>/logout</code>
<b>POST Variable</b>	<code>none needed</code>

## 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 administrator is missing access 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

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

```
https://<FG_IP>/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 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 examples:

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

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.

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

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.
resource	GET	default	Return the CLI default values for entire CLI tree.
resource	GET	schema	Return the CLI schema for this object type.
resource	GET	schema	Return schema for entire CLI tree.

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

## collection

### GET

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

### Extra parameters

Name	Type	Summary
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.
format	string	List of property names to include in results, separated by   (i.e. policyid srcintf).

Name	Type	Summary
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: default

Summary	Return the CLI default values for entire CLI tree.
HTTP Method	GET
Action	default
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

### GET: schema

Summary	Return schema for entire CLI tree.
---------	------------------------------------

HTTP Method	GET
Action	schema
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

## GET

Summary	Select a specific entry from a CLI table.
HTTP Method	GET

# 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://<FG_IP>/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

URI	HTTP Method	Summary
/endpoint-control/profile/xml/	GET	List XML representation for each endpoint-control profile.
/endpoint-control/registration-password/check/	POST	Check if provided registration password is valid for current VDOM.
/endpoint-control/record-list/	GET	List endpoint records.
/endpoint-control/registration/quarantine/	POST	Quarantine endpoint by FortiClient UID or MAC.
/endpoint-control/registration/unquarantine/	POST	Unquarantine endpoint by FortiClient UID or MAC.
/endpoint-control/registration/block/	POST	Block endpoint by FortiClient UID or MAC.
/endpoint-control/registration/unblock/	POST	Unblock endpoint by FortiClient UID or MAC.
/endpoint-control/registration/deregister/	POST	Deregister endpoint by FortiClient UID or MAC.
/firewall/health/	GET	List configured load balance server health monitors.
/firewall/local-in/	GET	List implicit and explicit local-in firewall policies.
/firewall/acl/	GET	List counters for all IPv4 ACL.
/firewall/acl/clear_counters/	POST	Reset counters for one or more IPv4 ACLs by policy ID.
/firewall/acl6/	GET	List counters for all IPv6 ACL.
/firewall/acl6/clear_counters/	POST	Reset counters for one or more IPv6 ACLs by policy ID.
/firewall/policy/	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.

URI	HTTP Method	Summary
/firewall/policy6/reset/	POST	Reset traffic statistics for all IPv6 policies.
/firewall/policy6/clear_counters/	POST	Reset traffic statistics for one or more IPv6 policies by policy ID.
/firewall/explicit-proxy-policy/	GET	List traffic statistics for all explicit proxy policies.
/firewall/explicit-proxy-policy/clear_counters/	POST	Reset traffic statistics for one or more explicit proxy policies by policy ID.
/firewall/policy-lookup/	GET	Performs a policy lookup by creating a dummy packet and asking the kernel which policy would be hit.
/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.
/firewall/address-fqdns/	GET	List of FQDN address objects and the IPs they resolved to.
/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/current-disk-usage/	GET	Return current used, free and total disk bytes.
/log/hourly-disk-usage/	GET	Return historic hourly disk usage in bytes.
/log/historic-daily-remote-logs/	GET	Returns the amount of logs in bytes sent daily to a remote logging service (FortiCloud or FortiAnalyzer).
/log/stats/reset/	POST	Reset logging statistics for all log devices.

URI	HTTP Method	Summary
/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.
/router/lookup/	GET	Performs a route lookup by querying the routing table.
/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/fsck/start/	POST	Reboot the device and immediately start file system check utility.
/system/storage/	GET	Retrieve information for the non-boot disk.
/system/change-password/	POST	Save admin and guest-admin passwords.
/system/password-policy-conform/	POST	Check whether password conforms to the password policy.
/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.

URI	HTTP Method	Summary
/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/available-interfaces/	GET	Retrieve a list of all interfaces along with some meta information regarding their availability.
/system/resolve-fqdn/	GET	Resolves the given FQDN to an IP Address.
/system/usb-log/	GET	Retrieve information about connected USB drives, including estimated log sizes.
/system/usb-log/start/	POST	Start backup of logs from current VDOM to USB drive.
/system/usb-log/stop/	POST	Stop backup of logs to USB drive.
/system/ipconf/	GET	Determine if there is an IP conflict for a specific IP using ARP.
/system/fortiguard/update/	POST	Immediately update status for FortiGuard services.
/system/fortiguard/clear-cache/	POST	Immediately clear all FortiGuard statistics.
/system/fortiguard/test-availability/	POST	Test availability of FortiGuard services.
/system/debug/	GET	Log debug messages to the console (if enabled).
/system/botnet/stat/	GET	Retrieve statistics for FortiGuard botnet database.
/system/botnet/	GET	List all known IP-based botnet entries in FortiGuard botnet database.
/system/botnet-domains/	GET	List all known domain-based botnet entries in FortiGuard botnet database.
/system/ha-statistics/	GET	List of statistics for members of HA cluster
/system/ha-checksums/	GET	List of checksums for members of HA cluster

URI	HTTP Method	Summary
/system/link-monitor/	GET	Retrieve per-interface statistics for active link monitors.
/system/compliance/run/	POST	Immediately run compliance checks for the selected VDOM.
/system/config/restore/	POST	Restore system configuration from uploaded file or from USB.
/system/config/backup/	GET	Backup system config
/system/config/usb-filelist/	GET	List configuration files available on connected USB drive.
/system/sandbox/	GET	Retrieve statistics for FortiSandbox.
/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.
/user/fortitoken/activate/	POST	Activate a set of FortiTokens by serial number.
/user/device/	GET	Retrieve a list of detected devices.
/user/fortitoken/refresh/	POST	Refresh a set of FortiTokens by serial number.
/user/fortitoken/provision/	POST	Provision a set of FortiTokens by serial number.
/user/fortitoken/send-activation/	POST	Send a FortiToken activation code to a user via SMS or Email.
/utm/rating-lookup/	GET	Lookup FortiGuard rating for a specific URL.

URI	HTTP Method	Summary
/utm/app-lookup/	GET	Query remote FortiFlow database to resolve hosts to application control entries.
/virtual-wan/health-check/	GET	Retrieve statistics for each virtual WAN link.
/webfilter/override/	GET	List all administrative and user initiated webfilter overrides.
/webfilter/override/delete/	POST	
/webfilter/malicious-urls/	GET	List all URLs in FortiSandbox malicious URL database.
/webfilter/malicious-urls/stat/	GET	Retrieve statistics for the FortiSandbox malicious URL database.
/webfilter/trusted-urls/	GET	List all URLs in FortiGuard trusted URL database.
/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/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.

URI	HTTP Method	Summary
/wifi/interfering_ap/	GET	Retrieve a list of interfering 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	
/wifi/rogue_ap/restart/	POST	
/wifi/spectrum/	GET	Retrieve spectrum analysis information for a specific FortiAP .
/switch-controller/managed-switch/faceplate-xml/	GET	Retrieve XML for rendering FortiSwitch faceplate widget.

## endpoint-control

### profile: xml

Summary	List configured load balance server health monitors.
URI	/endpoint-control/profile/xml/
HTTP Method	GET
Action	xml
Access Group	endpoint-control-grp
Response Type	array

### Extra parameters

Name	Type	Summary
mkey	string	Name of endpoint-control profile.

**registration-password: check**

Summary	Check if provided registration password is valid for current VDOM.
URI	/endpoint-control/registration-password/check/
HTTP Method	POST
Action	check
Access Group	endpoint-control-grp
Response Type	boolean

**Extra parameters**

Name	Type	Summary
password	string	Registration password to test.

**record-list: select**

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

**registration: quarantine**

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



**Extra Parameters**

Name	Type	Summary
uid	array	Array of FortiClient UIDs to quarantine.
uid	string	Single FortiClient UID to quarantine.
mac	array	Array of MACs to quarantine.
mac	string	Single MAC to quarantine.

**registration: unquarantine**

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

**Extra Parameters**

Name	Type	Summary
uid	array	Array of FortiClient UIDs to unquarantine.
uid	string	Single FortiClient UID to unquarantine.
mac	array	Array of MACs to unquarantine.
mac	string	Single MAC to unquarantine.

**registration: block**

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

**Extra Parameters**

Name	Type	Summary
uid	array	Array of FortiClient UIDs to block.
uid	string	Single FortiClient UID to block.
mac	array	Array of MACs to block.
mac	string	Single MAC to block.

**registration: unblock**

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

**Extra Parameters**

Name	Type	Summary
uid	array	Array of FortiClient UIDs to unblock.
uid	string	Single FortiClient UID to unblock.
mac	array	Array of MACs to unblock.
mac	string	Single MAC to unblock.

**registration: deregister**

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

**Extra Parameters**

Name	Type	Summary
uid	array	Array of FortiClient UIDs to deregister.
uid	string	Single FortiClient UID to deregister.
mac	array	Array of MACs to deregister.
mac	string	Single MAC to deregister.

**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

**acl: select**

Summary	List counters for all IPv4 ACL.
---------	---------------------------------

URI	/firewall/acl/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy

### acl: clear\_counters

Summary	Reset counters for one or more IPv4 ACLs by policy ID.
URI	/firewall/acl/clear_counters/
HTTP Method	POST
Action	clear_counters
Access Group	fwgrp.policy

### Extra Parameters

Name	Type	Summary
policy	array	Array of policy IDs to reset.
policy	int	Single policy ID to reset.

### acl6: select

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

### acl6: clear\_counters

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

Action	clear_counters
Access Group	fwgrp.policy

**Extra Parameters**

Name	Type	Summary
policy	array	Array of policy IDs to reset.
policy	int	Single policy ID to reset.

**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.

**explicit-proxy-policy: select**

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

**explicit-proxy-policy: clear\_counters**

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

**policy-lookup: select**

Summary	Performs a policy lookup by creating a dummy packet and asking the kernel which policy would be hit.
URI	/firewall/policy-lookup/

HTTP Method	GET
Action	select
Access Group	fwgrp.policy
Response Type	object

**Extra Parameters**

Name	Type	Summary
ipv6	boolean	Perform an IPv6 lookup?
srcintf	string	Source interface
sourceport	int	Source port
protocol	string	Protocol
dest	string	Destination IP/FQDN
desport	int	Destination port
icmptype	int	ICMP type
icmpcode	int	ICMP code

**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].



Name	Type	Summary
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 srcintf dstintf policy country].
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 srcintf, source, dstintf, destination, policyid, application, web_category_id, web_domain, country.

**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.

**address-fqdns: select**

Summary	List of FQDN address objects and the IPs they resolved to.
URI	/firewall/address-fqdns/
HTTP Method	GET
Action	select
Access Group	fwgrp.policy
Response Type	object

**fortiview****statistics: select**

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

**current-disk-usage: select**

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

**hourly-disk-usage: select**

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

**historic-daily-remote-logs: select**

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

**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.

Name	Type	Summary
type	string	Filter: route type.
interface	string	Filter: interface name.

### lookup: select

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

### Extra Parameters

Name	Type	Summary
ipv6	boolean	Perform an IPv6 lookup?
destination	string	Destination IP/FQDN

## 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
Response Type	object

**fsck: start**

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

**storage: select**

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

**change-password: select**

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

**password-policy-conform: select**

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

**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.

**available-interfaces: select**

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

**resolve-fqdn: select**

Summary	Resolves the given FQDN to an IP Address.
URI	/system/resolve-fqdn/
HTTP Method	GET
Action	select
Response Type	object

**Extra Parameters**

Name	Type	Summary
ipv6	boolean	Resolve for the AAAA record?
fqdn	string	FQDN

**usb-log: select**

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

**usb-log: start**

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



**usb-log: stop**

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

**ipconf: select**

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

**Extra Parameters**

Name	Type	Summary
dev	object	List of interfaces to check for conflict.
ipaddr	string	IPv4 address to check for conflict.

**fortiguard: update**

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

**fortiguard: clear-cache**

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

**fortiguard: test-availability**

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

**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.

**botnet: stat**

Summary	Retrieve statistics for FortiGuard botnet database.
URI	/system/botnet/stat/
HTTP Method	GET
Action	stat
Access Group	sysgrp
ETag Caching	Enabled
Response Type	object

**botnet: select**

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

**Extra Parameters**

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

**botnet-domains: select**

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

Action	select
Access Group	sysgrp
ETag Caching	Enabled
Response Type	array

**Extra Parameters**

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

**ha-statistics: select**

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

**ha-checksums: select**

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

**link-monitor: select**

Summary	Retrieve per-interface statistics for active link monitors.
---------	---

URI	/system/link-monitor/
HTTP Method	GET
Action	select
Access Group	sysgrp

**Extra Parameters**

Name	Type	Summary
mkey	string	Name of link monitor.

**compliance: run**

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

**config: restore**

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

**Extra Parameters**

Name	Type	Summary
source	string	Configuration file data source [upload   usb].

Name	Type	Summary
usb_filename	string	When using 'usb' source: the filename to restore from the connected USB device.
file_content	string	When using 'upload' source: base64 encoded configuration file data. Must not contain whitespace or other invalid base64 characters.
password	string	Password to decrypt configuration data.
vdom	string	If specified, restore configuration to VDOM else a Global configuration restore is performed.

### config: backup

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

### Extra Parameters

Name	Type	Summary
destination	string	Configuration file destination [file*   usb].
usb_filename	string	When using 'usb' destination: the filename to save to on the connected USB device.
password	string	Password to encrypt configuration data.
backup_vdom	string	If specified, backup configuration from a VDOM else Global configuration backup is performed.

### config: usb-filelist

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

Action	usb-filelist
Access Group	sysgrp
Response Type	array

### sandbox: select

Summary	Retrieve statistics for FortiSandbox.
URI	/system/sandbox/
HTTP Method	GET
Action	select
Access Group	sysgrp

## 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	authgrp
Response Type	array

### Extra parameters

Name	Type	Summary
start	int	Starting entry index.
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	authgrp



**banned: select**

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

**banned: clear\_users**

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

**Extra parameters**

Name	Type	Summary
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	authgrp

**Extra parameters**

Name	Type	Summary
ip_addresses	array	List of IP Addresses to ban. IPv4 and IPv6 addresses are allowed.

Name	Type	Summary
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	authgrp

**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.

**device: select**

Summary	Retrieve a list of detected devices.
URI	/user/device/
HTTP Method	GET
Action	select

Access Group	sysgrp
Response Type	array

**Extra Parameters**

Name	Type	Summary
master_only	boolean	List of master device only.

**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.

**fortitoken: send-activation**

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

**Extra Parameters**

Name	Type	Summary
user_name	string	Username.
token	string	User's FortiToken serial number.
method	string	Method to send activation code ('email' or 'sms').
email	string	User's email address (required if using 'email' method).
sms_phone	string	User's SMS phone number (required if using 'sms' method).

**utm****rating-lookup: select**

Summary	Lookup FortiGuard rating for a specific URL.
URI	/utm/rating-lookup/
HTTP Method	GET
Action	select

Access Group	utmgrp.webfilter
Response Type	object

**Extra parameters**

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

**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.

**virtual-wan****health-check: select**

Summary	Retrieve statistics for each virtual WAN link.
---------	--

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

## 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

### malicious-urls: select

Summary	List all URLs in FortiSandbox malicious URL database.
URI	/webfilter/malicious-urls/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter
ETag Caching	Enabled
Response Type	object

**malicious-urls: stat**

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

**trusted-urls: select**

Summary	List all URLs in FortiGuard trusted URL database.
URI	/webfilter/trusted-urls/
HTTP Method	GET
Action	select
Access Group	utmgrp.webfilter
ETag Caching	Enabled
Response Type	object

**vpn****ipsec:select**

Summary	Return an array of active IPsec VPNs
URI	/vpn/ipsec/
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.

**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 interfering 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.

**switch-controller****managed-switch: faceplate-xml**

Summary	Retrieve XML for rendering FortiSwitch faceplate widget.
URI	/switch-controller/managed-switch/faceplate-xml/
HTTP Method	GET
Action	faceplate-xml
Access Group	wifi
Response Type	array

**Extra Parameters**

Name	Type	Summary
mkey	string	Name of managed FortiSwitch.





**FORTINET®**

High Performance Network Security



Copyright© 2015 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.