WHM API 1 Functions - modsec_get_settings

Description

This function retrieves the server's ModSecurity™ configuration settings. The system stores these settings in the `/usr/local/apache/conf/modsec2.conf` file.

Important:
In cPanel & WHM version 76 and later, when you disable the `WebServer` role, the system **disables** this function. For more information, read our How to Use Server Profiles documentation.

Examples

JSON API

```
https://hostname.example.com:2087/cpsess##########/json-api/modsec_get_settings?api.version=1
```

XML API

```
https://hostname.example.com:2087/cpsess##########/xml-api/modsec_get_settings?api.version=1
```

Function information

About WHM API 1

WHM API 1 performs functions and accesses data in WHM.

Notes:

- So
  ro
  us
- Yo
  mu
  us
  20
  or
  20
) to

Command Line

```
whmapi1
modsec_get_settings
```

Notes:

- Unless otherwise noted, you **must** URI-encode values.
- For more information and additional output options, read our Guide to WHM API 1 documentation or run the `whmapi1 --help` command.
- If you run CloudLinux™, you **must** use the full path of the `whmapi1` command:

```
/usr/local
/cpanel/bi
n/whmapi1
```

Output (JSON)


```
{
   "metadata":{

"command":"modsec_get
_settings",
      "reason":"OK",
      "result":1,
      "version":1
   },
   "data":{
      "settings":[
         {

"type":"radio",

"directive":"SecAudit
Engine",

"description":"This
setting controls the
behavior of the audit
engine.",

"engine":1,

"default":"Off",

"url":"https://github
```


Find a function

- WHM API 1 Functions - modsec_add_rule — This function adds a new rule to a ModSecurity™ configuration staging file.

```
.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secauditengine",

"setting_id":0,

"name":"Audit Log Level",

"state":"",

"radio_options":[
                {

"name":"Log all transactions.",

"option":"On"
                },
                {

"name":"Do not log any transactions.",

"option":"Off"
                },
                {

"option":"RelevantOnly",

"name":"Only log noteworthy transactions."
                }
            ],

"missing":1
          },
          {

"description":"This setting controls the behavior of the connections engine.",

"engine":1,

"default":"Off",

"type":"radio",
```


- WHM API 1 Functions - modsec_add_vendor — This function adds a new ModSecurity™ vendor ruleset to the server.
- WHM API 1 Functions - modsec_batch_settings — This function adds, updates, and removes global ModSecurity™ configuration directives.

```
"directive":"SecConnEngine",

"missing":1,

"setting_id":1,

"url":"https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secconnengine",

"state":"",

"name":"Connections Engine",

"radio_options":[
                {

"option":"On",

"name":"Process the rules."
                },
                {

"option":"Off",

"name":"Do not process the rules."
                },
                {

"option":"DetectionOnly",

"name":"Process the rules in verbose mode, but do not execute disruptive actions."
                }
            ]
        },
        {

"missing":1,

"name":"Rules Engine",
```


- WHM API 1 Functions - modsec_clone_rule — This function copies a ModSecurity™ rule with a new rule ID.

```
"state":"",

"radio_options":[
                {

"name":"Process the
rules.",

"option":"On"
                },
                {

"name":"Do not
process the rules.",

"option":"Off"
                },
                {

"name":"Process the
rules in verbose
mode, but do not
execute disruptive
actions.",

"option":"DetectionOn
ly"
                }
            ],

"url":"https://github
.com/SpiderLabs/ModSe
curity/wiki/Reference
-Manual#secruleengine
",

"setting_id":2,

"engine":1,

"default":"Off",

"description":"This
setting controls the
behavior of the rules
engine.",

"type":"radio",

"directive":"SecRuleE
ngine"
        },
        {
```

flush_cphulk_login_history_for_ips

get_countries_with_known_ip_ranges

get_cphulk_brutes

get_cphulk_excessive_brutes

get_cphulk_failed_logins

get_cphulk_user_brutes

load_cphulk_config

read_cphulk_records

save_cphulk_config

set_cphulk_config_key

Databases

background_mysql_upgrade_status

current_mysql_version

installable_mysql_versions

latest_available_mysql_version

list_database_users

list_databases

list_mysql_databases_and_users

remote_mysql_create_profile

remote_mysql_create_profile_via_ssh

remote_mysql_delete_profile

remote_mysql_initiate_profile_activat


```
"description":"Disables backend compression while leaving the frontend compression enabled.",

"default":"Off",

"type":"radio",

"directive":"SecDisableBackendCompression",

"missing":1,

"url":"https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secdisablebackendcompression",

"setting_id":3,

"name":"Backend Compression",

"state":"",

"radio_options":[
                {

"name":"Disabled",

"option":"On"
                },
                {

"name":"Enabled",

"option":"Off"
                }
            ]
        },
        {

"missing":1,

"validation":[
                "path"
            ],
```

```
"url":"https://github
.com/SpiderLabs/ModSe
curity/wiki/Reference
-Manual#secgeolookupd
b",

"setting_id":4,

"name":"Geolocation
Database",

"state":"",

"description":"Specif
y a path for the
geolocation
database.",

"directive":"SecGeoLo
okupDb",

"type":"text"
        },
        {

"url":"https://github
.com/SpiderLabs/ModSe
curity/wiki/Reference
-Manual#secgsblookupd
b",

"setting_id":5,

"state":"",

"name":"Google Safe
Browsing Database",

"missing":1,

"validation":[
              "path"
           ],

"directive":"SecGsbLo
okupDb",

"type":"text",

"description":"Specif
y a path for the
Google Safe Browsing
```

killdns

listmxs

listzones

lookupnsip

lookupnsips

removezonerecord

resetzone

resolvedomainname

savemxs

setresolvers

update_nameservers_config

EasyApache

ea4_get_currently_installed_packages

ea4_get_ea_pkgs_state

ea4_list_profiles

ea4_metainfo

ea4_migration

ea4_pre_migrate_check

ea4_recommendations

ea4_save_profile

ea4_tomcat85_add

ea4_tomcat85_list

ea4_tomcat85_rem

Greylisting

cpgreylist_is_server_netblock_trusted

cpgreylist_list_entries_for_common_mail_provider

cpgreylist_load_common_mail_provid


```
Database."
         },
         {

"validation":[
               {

"name":"startsWith",

"arg":"[|]"
               },
               "path"
            ],

"missing":1,

"state":"",

"name":"Guardian
Log",

"setting_id":6,

"url":"https://github
.com/SpiderLabs/ModSe
curity/wiki/Reference
-Manual#secguardianlo
g",

"description":"Specif
y an external program
to pipe transaction
log information to
for additional
analysis. The syntax
is analogous to the
.forward file, in
which a pipe at the
beginning of the
field indicates
piping to an external
program.",

"type":"text",

"directive":"SecGuard
ianLog"
         },
         {

"description":"Specif
y a Project Honey Pot
API Key for use with
```

```
the @rbl operator.",

"type":"text",

"directive":"SecHttpBlKey",

"validation":[

"honeypotAccessKey"
            ],

"missing":1,

"state":"",

"name":"Project Honey Pot Http:BL API Key",

"setting_id":7,

"url":"https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#sechttpblkey"
        },
        {

"directive":"SecPcreMatchLimit",

"type":"number",

"default":1500,

"description":"Define the match limit of the Perl Compatible Regular Expressions library.",

"name":"Perl Compatible Regular Expressions Library Match Limit",

"state":"",

"url":"https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secpcrematchlimit",
```

```
"setting_id":8,

"missing":1,

"validation":[

"positiveInteger"
            ]
        },
        {

"url":"https://github
.com/SpiderLabs/ModSe
curity/wiki/Reference
-Manual#secpcrematchl
imitrecursion",

"setting_id":9,

"state":"",

"name":"Perl
Compatible Regular
Expressions Library
Match Limit
Recursion",

"missing":1,

"validation":[

"positiveInteger"
            ],

"directive":"SecPcreM
atchLimitRecursion",

"type":"number",

"description":"Define
the match limit
recursion of the Perl
Compatible Regular
Expressions
library.",

"default":1500
        }
```

```
        ]
    }
}
```

Output (XML)

```
<result>
    <metadata>

<version>1</version>

<result>1</result>

<reason>OK</reason>

<command>modsec_get_settings</command>
    </metadata>
    <data>
        <settings>

<directive>SecAuditEngine</directive>

<missing>1</missing>

<default>Off</default>

<engine>1</engine>

<description>
                This setting controls the behavior of the audit engine.

</description>
            <state/>

<type>radio</type>

<setting_id>0</setting_id>
            <url>

https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secauditengine
            </url>
```

```
<name>Audit Log
Level</name>

<radio_options>

<name>Log all
transactions.</name>

<option>On</option>

</radio_options>

<radio_options>

<name>Do not log any
transactions.</name>

<option>Off</option>

</radio_options>

<radio_options>

<name>Only log
noteworthy
transactions.</name>

<option>RelevantOnly<
/option>

</radio_options>
        </settings>
        <settings>

<name>Connections
Engine</name>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secconnengine
            </url>

<setting_id>1</settin
g_id>

<radio_options>

<option>On</option>

<name>Process the
```

```
rules.</name>

</radio_options>

<radio_options>

<name>Do not process
the rules.</name>

<option>Off</option>

</radio_options>

<radio_options>

<name>

Process the rules in
verbose mode, but do
not execute
disruptive actions.

</name>

<option>DetectionOnly
</option>

</radio_options>

<directive>SecConnEng
ine</directive>

<description>
               This
setting controls the
behavior of the
connections engine.

</description>

<missing>1</missing>

<engine>1</engine>

<default>Off</default
>

<type>radio</type>
            <state/>
        </settings>
        <settings>

<radio_options>
```

```
<option>On</option>

<name>Process the
rules.</name>

</radio_options>

<radio_options>

<option>Off</option>

<name>Do not process
the rules.</name>

</radio_options>

<radio_options>

<name>

Process the rules in
verbose mode, but do
not execute
disruptive actions.

</name>

<option>DetectionOnly
</option>

</radio_options>

<setting_id>2</settin
g_id>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secruleengine
            </url>

<name>Rules
Engine</name>
            <state/>

<type>radio</type>

<engine>1</engine>

<missing>1</missing>
```

```
<default>Off</default
>

<description>
                This
setting controls the
behavior of the rules
engine.

</description>

<directive>SecRuleEng
ine</directive>
        </settings>
        <settings>

<type>radio</type>
            <state/>

<directive>SecDisable
BackendCompression</d
irective>

<description>

Disables backend
compression while
leaving the frontend
compression enabled.

</description>

<default>Off</default
>

<missing>1</missing>

<name>Backend
Compression</name>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secdisablebackendcom
pression
            </url>

<setting_id>3</settin
g_id>

<radio_options>
```

```
<option>On</option>

<name>Disabled</name>

</radio_options>

<radio_options>

<name>Enabled</name>

<option>Off</option>

</radio_options>
        </settings>
        <settings>

<name>Geolocation
Database</name>

<setting_id>4</settin
g_id>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secgeolookupdb
            </url>

<type>text</type>
            <state/>

<validation>path</val
idation>

<directive>SecGeoLook
upDb</directive>

<description>Specify
a path for the
geolocation
database.</descriptio
n>

<missing>1</missing>
        </settings>
        <settings>

<setting_id>5</settin
g_id>
            <url>

https://github.com/Sp
```

```
iderLabs/ModSecurity/
wiki/Reference-Manual
#secgsblookupdb
            </url>

<name>Google Safe
Browsing
Database</name>

<directive>SecGsbLook
upDb</directive>

<missing>1</missing>

<description>

Specify a path for
the Google Safe
Browsing Database.

</description>
            <state/>

<type>text</type>

<validation>path</val
idation>
        </settings>
        <settings>
            <state/>

<type>text</type>

<validation>

<arg>[|]</arg>

<name>startsWith</nam
e>

</validation>

<validation>path</val
idation>

<directive>SecGuardia
nLog</directive>

<missing>1</missing>

<description>

Specify an external
```

```
program to pipe
transaction log
information to for
additional analysis.
The syntax is
analogous to the
.forward file, in
which a pipe at the
beginning of the
field indicates
piping to an external
program.

</description>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secguardianlog
            </url>

<setting_id>6</settin
g_id>

<name>Guardian
Log</name>
        </settings>
        <settings>

<setting_id>7</settin
g_id>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#sechttpblkey
            </url>

<name>Project Honey
Pot Http:BL API
Key</name>

<missing>1</missing>

<description>

Specify a Project
Honey Pot API Key for
use with the @rbl
operator.
```

get_service_config_key
get_tcp4_sockets
get_tcp6_sockets
get_tweaksetting
get_udp4_sockets
get_udp6_sockets
get_update_availability
get_users_links
getdiskusage
gethostname
is_role_enabled
list_configclusterservers
loadavg
nvget
nvset
personalization_get
personalization_set
purchase_a_license
reboot
remove_in_progress_exim_config_edit
restartservice
restore_config_from_file
restore_config_from_upload
run_cpkeyclt
send_test_posturl
send_test_pushbullet_note
servicestatu

```
</description>

<directive>SecHttpBlKey</directive>

<validation>honeypotAccessKey</validation>
            <state/>

<type>text</type>
        </settings>
        <settings>
            <name>
                Perl Compatible Regular Expressions Library Match Limit
            </name>

<setting_id>8</setting_id>
            <url>

https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secpcrematchlimit
            </url>

<type>number</type>
            <state/>

<validation>positiveInteger</validation>

<directive>SecPcreMatchLimit</directive>

<description>

Define the match limit of the Perl Compatible Regular Expressions library.

</description>

<missing>1</missing>

<default>1500</default>
        </settings>
        <settings>
```

```
            <name>
                Perl
Compatible Regular
Expressions Library
Match Limit Recursion
            </name>

<setting_id>9</settin
g_id>
            <url>

https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secpcrematchlimitrec
ursion
            </url>

<directive>SecPcreMat
chLimitRecursion</dir
ective>

<description>

Define the match
limit recursion of
the Perl Compatible
Regular Expressions
library.

</description>

<default>1500</defaul
t>

<missing>1</missing>

<type>number</type>
            <state/>

<validation>positiveI
nteger</validation>
```

```
            </settings>
        </data>
    </result>
```

Note:
Use WHM's *API Shell* interface (*WHM >> Home >> Development >> API Shell*) to directly test WHM API calls.

Parameters

This function does not accept parameters.

Returns

Return	Type	Description	Possible values	Example
`settings`	*array of hashes*	A array of ModSecurity global configuration setting hashes.	Each hash includes the `setting_id`, `name`, `default`, `description`, `engine`, `directive`, `type`, `state`, and `url` returns and the `radio_options` and `validation` arrays.	
`setting_id`	*integer*	The setting ID. The function returns this value in the `settings` array.	A positive integer.	`0`
`name`	*string*	The setting's name. The function returns this value in the `settings` array.	A valid string.	`Audit logging level`
`default`	*string*	The setting's default value. The function returns this value in the `settings` array.	A positive integer.	`1500`

	`description`	*string*	The setting's description. The function returns this value in the `settings` array.	A valid string.	Click to view... `This setting allows you to define the match limit of the PCRE library.`
	`engine`	*Boolean*	Whether the setting is an engine directive. The function returns this value in the `settings` array.	• `1` — Engine directive. • `0` — Normal directive.	`1`
	`directive`	*string*	The setting's Apache configuration directive. The function returns this value in the `settings` array.	A valid directive name.	`SecPcreMatchLimitRecursion`
	`type`	*string*	The form element that the WHM interface uses to display this setting. The function returns this value in the `settings` array.	• `text` — WHM users modify this setting via a text box. • `radio` — WHM users modify this setting via a radio button. • `number` — WHM users modify this setting via a text box that only allows numeric values.	`text`
	`state`	*string*	The setting's current state. The function returns this value in the `settings` array.	A valid option name.	`On`
	`url`	*string*	The URL of the setting's entry in the ModSecurity reference manual. The function returns this value in the `settings` array.	A valid URL.	Click to view... `https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secpcrematchlimit`

`radio_options`	*array of hashes*	An array of hashes of the options that the client should display, as radio buttons, for this setting in a user interface. **Note:** The function **only** returns this array of hashes when the `type` parameter's value is `radio`. The function returns this array in the `settings` array.	Read the Radio options section below for a list of possible values.	
`validation`	*array*	An array of validators to apply. The function returns this array in the `settings` array.	Read the Validators section below for a list of possible values.	`positiveInteger`

Validators

Click to view...

The function may specify one or more validators for a setting. The client should use these validators to perform front-end validation through the preferred implementation methods.

The function may represent each validator as either a string or a hash.

- When the function represents the validator as a string, no arguments exist for the validator.
- When the function represents the validator as a hash, the WHM API may also include an argument for the validator.

Validator	Validator description	Argument description	Example
`path`	Instructs the client to verify that the user's input is a valid path.	(none)	`path`

set_tier

update_updateconf

version

`startsWith`	Instructs the client to verify that the user's input begins with the pattern that the argument specifies.	A string that represents a regular expression to apply against the user input.	`{ r` **Note:** This example is JSON-encoded, to illustrate the validator's structure.
`honeypotAccessKey`	Instructs the client to verify that the user's input fits the constraints of an `Http:BL` API access key.	(none)	`honeypotAccessKey`
`positiveInteger`	Instructs the client to verify that the user's input is a positive integer.	(none)	`positiveInteger`

Radio options

Click to view...

The function **only** returns this data if the setting's value for the `type` parameter is `radio`. The function returns this information as a set of hashes within the `radio_options` array.

Each hash contains the following returns:

Return	Type	Description	Possible values	Example
`option`	*string*	The setting name that the WHM API uses to select the setting's state. **Note:**	A valid string.	On

		The string that the `option` key returns is identical to the string that the client sends in the `state` field when users select this option. In most cases, do **not** display this value to the user. Instead, display the `name` value.		

`name`	*string*	The setting name to display to the user. The user's locale may translate this value.	A valid string.	`Log all transactions.`