

WHM API 1 Functions - modsec_get_settings

Guide to WHM API 1

- Return Data
- Filter Output
- Sort Output
- Paginate Output
- Output Columns
- Call cPanel API 2 and UAPI

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 `WebServerRole`, 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
```

- Account Restoration
- restore_modules_summary
- restore_queue_activate
- restore_queue_add_task
- restore_queue_clear_all_completed_tasks
- restore_queue_clear_all_failed_tasks
- restore_queue_clear_all_pending_tasks
- restore_queue_clear_all_tasks
- restore_queue_clear_completed_task
- restore_queue_clear_pending_task
- restore_queue_is_active
- restore_queue_list_active
- restore_queue_list_completed
- restore_queue

Function Information

About WHM API 1

WHM API 1 performs functions and accesses data in WHM.

Notes:

- Scro
- Ycmtus20 or 20)tc

ue_list_pending
restore_queue_state
restoreaccount
verify_new_username_for_restore

Accounts

accountsummary
applist
createacct
domainuserdata
editquota
forcepasswordchange
get_disk_usage
get_domain_info
getdomainowner
has_digest_auth
has_mycnf_for_cpuser
limitbw
list_users
listaccts
listlockedaccounts
listsuspended
modifyacct
myprivs
passwd
quota_enabled
removeacct
set_digest_auth
showbw
suspendacct
unsuspendacct
untrack_acct

Command Line

```
whmapil  
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 `whmapil --help` command.
- If you run CloudLinux™, you **must** use the full path of the `whmapil` command:

```
/usr/local  
/cpanel/bin/whmapil
```

Output (JSON)

```
{  
  "metadata": {  
    "command": "modsec_get_settings",  
    "reason": "OK",  
    "result": 1,  
    "version": 1  
  },  
  "data": {  
    "settings": [  
      {  
        "type": "radio",  
        "directive": "SecAuditEngine",  
        "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 Mod Security™ configuration staging file.

_id

verify_new_username

▼ Addon Domains

convert_addon_fetch_conversion_details

convert_addon_fetch_domain_details

convert_addon_get_conversion_status

convert_addon_initiate_conversion

convert_addon_list_addon_domains

convert_addon_list_conversions

▼ Authentication

api_token_create

api_token_list

api_token_revoke

api_token_update

disable_authentication_provider

disable_failing_authentication_providers

enable_authentication_provider

get_available_authentication_providers

get_login_url

get_provider_client_configurations

get_provider_configuration_fields

get_provider_display_co

```
.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 Mod Security™ vendor rule set to the server.
- WHM API 1 Functions - modsec_batch_settings — This function adds, updates, and removes global Mod Security™ configuration directives.

```

nfigurations
get_users_authn_linked_accounts
link_user_authn_provider
set_provider_client_configurations
set_provider_display_configurations
twofactorauth_disable_policy
twofactorauth_enable_policy
twofactorauth_generate_tfa_config
twofactorauth_get_issuer
twofactorauth_get_user_configs
twofactorauth_policy_status
twofactorauth_remove_user_config
twofactorauth_set_issuer
twofactorauth_set_tfa_config
unlink_user_authn_provider
validate_login_token

```

▼ Backups

```

backup_config_get
backup_config_set
backup_data_list
backup_destination_add
backup_destination_delete

```

```

"directive": "SecConnE
ngine",
"missing": 1,
"setting_id": 1,
"url": "https://github
.com/SpiderLabs/ModSe
curity/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": "DetectionOn
ly",
"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.

backup_destination_get
backup_destination_list
backup_destination_set
backup_destination_validate
backup_get_transport_status
backup_list_transported
backup_set_list
backup_set_list_combined
backup_skip_users_all
backup_skip_users_all_status
backup_user_list
convert_and_migrate_from_legacy_config
get_users_with_backup_metadata
list_cparchive_files
start_background_package
toggle_user_backup_status
▼ cPHulk
cphulk_statuses
create_cphulk_record
delete_cphulk_record
disable_cphulk
enable_cphulk
flush_cphulk_login_history

```
"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_activation
```

```
"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"
],
```

ion

remote_mysql_monitor_profile_activation

remote_mysql_read_profile

remote_mysql_read_profiles

remote_mysql_update_profile

remote_mysql_validate_profile

rename_mysql_database

rename_mysql_user

rename_postgresql_database

rename_postgresql_user

set_local_mysql_root_password

set_mysql_password

set_postgresql_password

start_background_mysql_upgrade

▼ DNS

adddns

addzonerecord

addzonerecord (Reverse DNS)

dumpzone

editzonerecord

get_nameserver_config

getzonerecord

has_local_authority

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

```
"setting_id": 4,
```

```
"name": "Geolocation Database",
```

```
"state": "",
```

```
"description": "Specify a path for the geolocation database.",
```

```
"directive": "SecGeoLookupDb",
```

```
"type": "text"
```

```
},  
{
```

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

```
"setting_id": 5,
```

```
"state": "",
```

```
"name": "Google Safe Browsing Database",
```

```
"missing": 1,
```

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

```
"directive": "SecGsbLookupDb",
```

```
"type": "text",
```

```
"description": "Specify a path for the Google Safe Browsing
```

killdns
listmxs
listzones
lookupnsip
lookupnsips
removezone
record
resetzone
resolvedom
ainname
savemxs
setresolvers
update_nam
eservers_co
nfig

▼ EasyApache

ea4_get_cur
rently_install
ed_package
s
ea4_get_ea
_pkgs_state
ea4_list_pro
files
ea4_metainf
o
ea4_migrati
on
ea4_pre_mi
grate_check
ea4_recom
mendations
ea4_save_p
rofile
ea4_tomcat
85_add
ea4_tomcat
85_list
ea4_tomcat
85_rem

▼ Greylisting

cpgreylist_is
_server_net
block_truste
d
cpgreylist_li
st_entries_f
or_common
_mail_provid
er
cpgreylist_lo
ad_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
```


ers_config
cpgreylis_t
ave_commo
n_mail_provi
ders_config
cpgreylis_st
atus
cpgreylis_tr
ust_entries_
for_common
_mail_provid
er
cpgreylis_u
ntrust_entri
es_for_comm
on_mail_pro
vider
create_cpgr
eylist_truste
d_host
delete_cpgr
eylist_truste
d_host
disable_cpgr
eylist
enable_cpgr
eylist
load_cpgrey
list_config
read_cpgrey
list_deferred
_entries
read_cpgrey
list_trusted_
host
save_cpgrey
list_config

▼ Integration

batch
cpanel
create_integ
ration_group
create_integ
ration_link
get_integrati
on_link_user
_config
list_integrati
on_groups
list_integrati
on_links
remove_inte
gration_grou
p
remove_inte

```
the @rbl operator.",  
  
"type": "text",  
  
"directive": "SecHttpB  
lKey",  
  
"validation": [  
  
  "honeypotAccessKey"  
    ],  
  
"missing": 1,  
  
"state": "",  
  
"name": "Project Honey  
Pot Http:BL API Key",  
  
"setting_id": 7,  
  
"url": "https://github  
.com/SpiderLabs/ModSe  
curity/wiki/Reference  
-Manual#sechttpblkey"  
    },  
    {  
  
"directive": "SecPcreM  
atchLimit",  
  
"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/ModSe  
curity/wiki/Reference  
-Manual#secpcrematchl  
imit",
```

gration_link	"setting_id":8,
update_inte gration_link _token	"missing":1,
▼ IP Addresses	"validation":[
addips	"positiveInteger"
delip]
get_public_i p	},
get_shared_ ip	{
ipv6_disable _account	"url":"https://github .com/SpiderLabs/ModSe curity/wiki/Reference -Manual#secprematchl imitrecursion",
ipv6_enable _account	"setting_id":9,
ipv6_range_ add	"state":"","
ipv6_range_ edit	"name":"Perl Compatible Regular Expressions Library Match Limit Recursion",
ipv6_range_ list	"missing":1,
ipv6_range_ remove	"validation":[
ipv6_range_ usage	"positiveInteger"
listips],
nat_checkip	"directive":"SecPcreM atchLimitRecursion",
nat_set_pub lic_ip	"type":"number",
setsiteip	"description":"Define the match limit recursion of the Perl Compatible Regular Expressions library.",
▼ Mail	"default":1500
disable_dki m	}
disable_mail _sni	
emailtrack_s earch	
emailtrack_s tats	
emailtrack_u ser_stats	
enable_dkim	
enable_mail _sni	
ensure_dki m_keys_exi st	
exim_config uration_che ck	
expunge_m	

ailbox_messages
expunge_messages_for_mailbox_guid
fetch_dkim_private_keys
fetch_mail_queue
generate_mobileconfig
get_mailbox_status
get_mailbox_status_list
get_unique_recipient_count_per_sender_for_user
get_unique_sender_recipient_count_per_user
get_user_email_forward_destination
hold_outgoing_email
install_dkim_private_keys
install_spf_records
is_sni_supported
list_pops_for_mail_sni_status
rebuild_mail_sni_config
release_outgoing_email
save_spamd_config
set_user_email_forward_destination
suspend_outgoing_email
unsuspend_outgoing_email

```
]
}
}
```

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

validate_current_installexim_config

validate_current_dkims

validate_current_ptrs

validate_current_spfs

validate_exim_configuration_syntax

▼ Market

disable_market_provider

enable_market_provider

get_adjusted_market_providers_products

get_market_providers_commission_config

get_market_providers_list

get_market_providers_product_metadata

get_market_providers_products

set_market_product_attribute

set_market_provider_commission_id

▼ ModSecurity™

modsec_added_rule

modsec_added_vendor

modsec_assemble_config_text

modsec_batch_settings

modsec_check_rule

modsec_clone_rule

```
<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/SpiderLabs/ModSecurity/wiki/Reference-Manual#seconnengine
```

```
</url>
```

```
<setting_id>1</setting_id>
```

```
<radio_options>
```

```
<option>On</option>
```

```
<name>Process the
```

modsec_de
ploy_all_rule
_changes

modsec_de
ploy_rule_ch
anges

modsec_de
ploy_setting
s_changes

modsec_dis
able_rule

modsec_dis
able_vendor

modsec_dis
able_vendor
_configs

modsec_dis
able_vendor
_updates

modsec_dis
card_all_rul
e_changes

modsec_dis
card_rule_c
hanges

modsec_edit
_rule

modsec_en
able_vendor

modsec_en
able_vendor
_configs

modsec_en
able_vendor
_updates

modsec_get
_config_text

modsec_get
_configs

modsec_get
_configs_wit
h_changes_
pending

modsec_get
_log

modsec_get
_rules

modsec_get
_settings

modsec_get
_vendors

modsec_is_i
nstalled

modsec_ma
ke_config_a
ctive

```
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>
```

```

modsec_make_config_in
active

modsec_preview_vendor

modsec_remove_rule

modsec_remove_setting

modsec_remove_vendor

modsec_report_rule

modsec_set_config_text

modsec_set_setting

modsec_un
disable_rule

modsec_update_vendor

▼ Packages
_getpkgextensionform

add_override_features_for_user

addpkg

addpkgext

changepackage

create_featurelist

delete_featurelist

delpkgext

editpkg

get_available_applications

get_available_featurelists

get_feature_metadata

get_feature_names

get_featurelist_data

get_featureli

```

```

<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</setting_id>

<url>

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

<name>Rules
Engine</name>

<state/>

<type>radio</type>

<engine>1</engine>

<missing>1</missing>

```

sts
get_users_features_settings
getfeaturelist
getpkginfo
killpkg
listpkgs
manage_features
matchpkgs
read_featurelist
remove_override_features_for_user
update_featurelist
verify_user_has_feature

▼ PHP

convert_all_domains_to_fpm
get_fpm_count_and_utilization
is_conversion_in_progress
php_get_default_accounts_to_fpm
php_get_handlers
php_get_impacted_domains
php_get_installed_versions
php_get_old_fpm_flag
php_get_system_default_version
php_get_versions_by_version
php_get_versions
php_ini_get_content

```
<default>Off</default>
>
<description>
    This setting controls the behavior of the rules engine.
</description>
<directive>SecRuleEngine</directive>
    </settings>
    <settings>
<type>radio</type>
    <state/>
<directive>SecDisableBackendCompression</directive>
<description>
    Disables backend compression while leaving the frontend compression enabled.
</description>
<default>Off</default>
>
<missing>1</missing>
<name>BackendCompression</name>
    <url>
    https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secdisablebackendcompression
    </url>
<setting_id>3</setting_id>
<radio_options>
```

php_ini_get_directives	<option>On</option>
php_ini_set_content	<name>Disabled</name>
php_ini_set_directives	</radio_options>
php_set_default_accounts_to_fpm	<radio_options>
php_set_handler	<name>Enabled</name>
php_set_old_fpm_flag	<option>Off</option>
php_set_session_save_path	</radio_options>
php_set_system_default_version	</settings>
php_set_whoost_versions	<settings>
▼ Resellers	<name>Geolocation Database</name>
acccounts	<setting_id>4</setting_id>
get_public_contact	<url>
getresellers	https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secgeolookupdb
listaccls	</url>
listresellers	<type>text</type>
resellerstats	<state/>
saveacllist	<validation>path</validation>
set_public_contact	<directive>SecGeoLookupDb</directive>
setaccls	<description>Specify a path for the geolocation database.</description>
setresellers	<missing>1</missing>
setresellerlimits	</settings>
setresellermainip	<settings>
setresellerameservers	<setting_id>5</setting_id>
setresellerackagelimit	<url>
setupreseller	https://github.com/Sp
suspendreseller	
terminatereseller	
unsetuprese	


```

ller
unsuspendr
eseller
  v RPM
    delete_rpm_
    version
    edit_rpm_ve
    rsion
    get_rpm_ver
    sion_data
    install_rpm_
    plugin
    list_rpms
    package_m
    anager_fixc
    ache
    package_m
    anager_get_
    build_log
    package_m
    anager_get_
    package_inf
    o
    package_m
    anager_is_p
    erforming_a
    ctions
    package_m
    anager_list_
    packages
    package_m
    anager_reso
    lve_actions
    package_m
    anager_sub
    mit_actions
    package_m
    anager_upgr
    ade
    uninstall_rp
    m_plugin
  v Script Hooks
    delete_hook
    edit_hook
    list_hooks
    reorder_hoo
    ks
  v Security
    accesshash
    authorizessh
    key
    check_remo
    te_ssh_conn
    ection

```

```

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

```

```
convertopen
sshtoputty

deletesshke
y

fetch_securi
ty_advice

generatessh
keypair

importsshke
y

listsshkeys
```

▼ Server

Administration

```
add_configl
usterserver

configureba
ckgroundpro
cesskiller

configurese
rvice

cors_proxy_
get

create_user
_session

delete_conf
igclusterserv
er

enable_mon
itor_all_ena
bled_service
s

get_all_cont
act_importa
nces

get_appconf
ig_applicatio
n_list

get_applicati
on_contact_
event_import
ance

get_applicati
on_contact_
importance

get_availabl
e_profiles

get_current_
profile

get_passwor
d_strength

get_remote_
access_has
h

get_service_
config
```

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/SpiderLabs/ModSecurity/wiki/Reference-Manual#secguardianlog
        </url>
```

```
<setting_id>6</setting_id>
```

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

```
<setting_id>7</setting_id>
        <url>
```

```
https://github.com/SpiderLabs/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	</description>
get_tcp4_sockets	<directive>SecHttpBlkKey</directive>
get_tcp6_sockets	<validation>honeypotAccessKey</validation>
get_tweaksetting	<state/>
get_udp4_sockets	<type>text</type>
get_udp6_sockets	</settings>
get_update_availability	<settings>
get_users_links	<name>
getdiskusage	Perl
gethostname	Compatible Regular Expressions Library Match Limit
is_role_enabled	</name>
list_configlusterservers	<setting_id>8</setting_id>
loadavg	<url>
nvget	https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secprematchlimit
nvset	</url>
personalization_get	<type>number</type>
personalization_set	<state/>
purchase_license	<validation>positiveInteger</validation>
reboot	<directive>SecPcreMatchLimit</directive>
remove_in_progress_exim_configedit	<description>
restartservice	Define the match limit of the Perl Compatible Regular Expressions library.
restore_config_from_file	</description>
restore_config_from_upload	<missing>1</missing>
run_cpkeyctl	<default>1500</default>
send_test_posturl	<t>
send_test_pushbullet_note	</settings>
servicestatus	<settings>

s	<name>
set_applicati	Perl
on_contact_	Compatible Regular
event_impor	Expressions Library
tance	Match Limit Recursion
set_applicati	</name>
on_contact_	
importance	<setting_id>9</settin
set_primary	g_id>
_servername	<url>
e	
set_service_	https://github.com/Sp
config_key	iderLabs/ModSecurity/
set_tweakse	wiki/Reference-Manual
tting	#secprematchlimitrec
sethostname	ursion
e	</url>
setminimum	
passwordstr	<directive>SecPcreMat
engths	chLimitRecursion</dir
start_profile	ective>
_activation	
system_nee	<description>
ds_reboot	
systemloada	Define the match
vg	limit recursion of
update_conf	the Perl Compatible
igclusterserv	Regular Expressions
er	library.
update_cont	</description>
act_email	
verify_aim_a	<default>1500</defaul
ccess	t>
verify_icq_a	<missing>1</missing>
ccess	
verify_oscar	<type>number</type>
_access	<state/>
verify_postu	
rl_access	<validation>positiveI
verify_pushb	nteger</validation>
ullet_access	
▼ SSL	
disable_aut	
ossl	
fetch_servic	
e_ssl_comp	
onents	
fetch_ssl_ce	
rtificates_for	
_fqdns	
fetch_ssl_vh	
osts	
fetch_vhost	
_ssl_compo	
nents	

fetchcrtinfo
 fetchsslinfo
 generatessl
 get_autossl
 _check_sch
 edule
 get_autossl
 _log
 get_autossl
 _logs_catalo
 g
 get_autossl
 _metadata
 get_autossl
 _pending_q
 ueue
 get_autossl
 _pending_q
 ueue_for_do
 main
 get_autossl
 _pending_q
 ueue_for_us
 er
 get_autossl
 _problems_f
 or_domain
 get_autossl
 _problems_f
 or_user
 get_autossl
 _providers
 get_best_ssl
 domain_for_
 service
 install_servi
 ce_ssl_certif
 icate
 installssl
 listcrts
 rebuildinstall
 edssldb
 rebuildusers
 sldb
 reset_autossl
 _provider
 reset_servic
 e_ssl_certifi
 cate
 set_autossl_
 metadata
 set_autossl_
 metadata_k
 ey

```

    </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

[set_autoss_provider](#)
[start_autossil_check_for_all_users](#)
[start_autossil_check_for_one_user](#)
 ▾ [Styles and Themes](#)
[generate_cpanel_plugin](#)
[list_styles](#)
[load_style](#)
[remove_log](#)
[remove_style](#)
[save_style](#)
[set_default](#)
 ▾ [Support Tickets](#)
[ticket_create_stub_ticket](#)
[ticket_get_support_agreement](#)
[ticket_get_support_info](#)
[ticket_grant](#)
[ticket_list](#)
[ticket_remove_closed](#)
[ticket_revoke](#)
[ticket_ssh_test](#)
[ticket_ssh_test_start](#)
[ticket_update_service_agreement_approval](#)
[ticket_validate_oauth2_code](#)
[ticket_whitelist_check](#)
[ticket_whitelist_setup](#)
[ticket_whitelist_unsetup](#)

▾ [Transfers](#)

	description	string	<p>The setting's description.</p> <p>The function returns this value in the settings array.</p>	A valid string.	<p>▾ Click to view...</p> <p>This setting allows you to define the match limit of the PCRE library.</p>
	engine	Boolean	<p>Whether the setting is an engine directive.</p> <p>The function returns this value in the settings array.</p>	<ul style="list-style-type: none"> 1 — Engine directive. 0 — Normal directive. 	1
	directive	string	<p>The setting's Apache configuration directive.</p> <p>The function returns this value in the settings array.</p>	A valid directive name.	SecPcreMatchLimitRecursion
	type	string	<p>The form element that the WHM interface uses to display this setting.</p> <p>The function returns this value in the settings array.</p>	<ul style="list-style-type: none"> 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	<p>The setting's current state.</p> <p>The function returns this value in the settings array.</p>	A valid option name.	On
	url	string	<p>The URL of the setting's entry in the ModSecurity reference manual.</p> <p>The function returns this value in the settings array.</p>	A valid URL.	<p>▾ Click to view...</p> <p>https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secpcrematchlimit</p>

[abort_transfer_session](#)
[analyze_transfer_session_remote](#)
[available_transfer_modules](#)
[create_remote_root_transfer_session](#)
[create_remote_user_transfer_session](#)
[delete_account_archives](#)
[enqueue_transfer_item](#)
[fetch_transfer_session_log](#)
[get_transfer_session_state](#)
[pause_transfer_session](#)
[remote_basic_credential_check](#)
[retrieve_transfer_session_remote_analysis](#)
[start_transfer_session](#)
[transfer_module_schema](#)
[validate_system_user](#)

▼ Updates

[accept_eula](#)
[get_available_tiers](#)
[get_current_tls_expiration_status](#)
[get_tls_wexpire](#)
[getlongterm support](#)
[installed_versions](#)
[set_cpanel_updates](#)

radio_options	array of hashes	<p>An array of hashes of the options that the client should display, as radio buttons, for this setting in a user interface.</p> <div style="border: 1px solid orange; padding: 5px; margin: 10px 0;"> <p>Note : The function only returns this array of hashes when the type parameter's value is radio.</p> </div> <p>The function returns this array in the settings array.</p>	Read the Radio options section below for a list of possible values.	
validation	array	<p>An array of validators to apply.</p> <p>The function returns this array in the settings array.</p>	Read the Validators section below for a list of possible values.	positiveInteger

Validators

▼ [Click to view...](#)

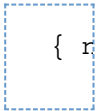
The function may specify one or more validators for a setting. The client should use these validators to perform front-end validation through the preferred implementation methods.

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_upd
 ateconf
 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.	 Note: This example is JSON-escaped, 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	<i>string</i>	The setting name that the WHM API uses to select the setting's state. <div style="border: 1px solid orange; padding: 5px; width: fit-content; margin: 10px auto;"> Note: </div>	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	<i>string</i>	The setting name to display to the user. The user's locale may translate this value.	A valid string.	Log all transactions.
------	---------------	--	-----------------	-----------------------