

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_or_restore

Accounts

accountsummary
applist
createacct
domainuserdata
editquota
forcepasswordchange
get_disk_usage
get_domain_info
getdomainowner
has_digest_auth
has_mycnf_or_cpuser
limitbw
list_users
listaccts
listlockedaccounts
listsuspended
modifyacct
myprivs
passwd
removeacct
set_digest_auth
showbw
suspendacct
unsuspendacct
untrack_acct_id
verify_new_

Command Line

```
whmapil  
modsec_get_settings
```

Notes:

- 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.

```

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_configurations
    get_users_a

```

```

.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_assemble_config_text — This function adds text to a Mod Security™ configuration file.
- WHM API 1 Functions - modsec_add_vendor — This function adds a new Mod Security™ vendor or rule set to the server.

uthn_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_logintoken

▼ Backups

backup_config_get
backup_config_set
backup_date_list
backup_destination_add
backup_destination_delete
backup_destination_get

```
"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_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
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": "DetectionOnly"
  }
],
"url": "https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secruleengine",
"setting_id": 2,
"engine": 1,
"default": "Off",
"description": "This setting controls the behavior of the rules engine.",
"type": "radio",
"directive": "SecRuleEngine"
},
{
```

ry_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"  
],
```

```
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

```
addns
addzonerecord
addzonerecord (Reverse DNS)
dumpzone
editzonerecord
get_nameserver_config
getzonerecord
has_local_authority
killdns
```

```
"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
```

```

listmxs
listzones
lookupnsip
lookupnsips
removezone
record
resetzone
resolvedom
ainname
savemxs
setresolvers
update_nam
eservers_co
nfig
  v 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
  v Greylisting
    cpgreylist_is
    _server_net
    block_truste
    d
    cpgreylist_li
    st_entries_f
    or_common
    _mail_provid
    er
    cpgreylist_lo
    ad_common
    _mail_provid
    ers_config

```

```

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

```


cpgreylist_s
ave_commo
n_mail_provi
ders_config

cpgreylist_st
atus

cpgreylist_tr
ust_entries_
for_common
_mail_provid
er

cpgreylist_u
ntrust_entrie
s_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
gration_link

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",

update_integrations_link_token

▼ IP Addresses

- addips
- delip
- get_public_ip
- get_shared_ip
- ipv6_disable_account
- ipv6_enable_account
- ipv6_range_add
- ipv6_range_edit
- ipv6_range_list
- ipv6_range_remove
- ipv6_range_usage
- listips
- nat_checkip
- nat_set_public_ip
- setsiteip

▼ Mail

- disable_dkim
- disable_mail_sni
- emailtrack_search
- emailtrack_stats
- emailtrack_user_stats
- enable_dkim
- enable_mail_sni
- ensure_dkim_keys_exist
- exim_configuration_check
- expunge_mailbox_messages

```
"setting_id":8,  
"missing":1,  
"validation":[  
  "positiveInteger"  
],  
{  
  "url":"https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secprematchlimitrecursion",  
  "setting_id":9,  
  "state":"","  
  "name":"Perl Compatible Regular Expressions Library Match Limit Recursion",  
  "missing":1,  
  "validation":[  
    "positiveInteger"  
  ],  
  "directive":"SecPcreMatchLimitRecursion",  
  "type":"number",  
  "description":"Define the match limit recursion of the Perl Compatible Regular Expressions library.",  
  "default":1500  
}
```

expunge_m
essages_for
_mailbox_gu
id

fetch_dkim_
private_keys

fetch_mail_
queue

generate_m
obileconfig

get_mailbox
_status

get_mailbox
_status_list

get_unique_
recipient_co
unt_per_sen
der_for_user

get_unique_
sender_reci
pient_count
_per_user

get_user_e
mail_forwar
d_destinatio
n

hold_outgoi
ng_email

install_dkim
_private_key
s

install_spf_r
ecords

is_sni_supp
orted

list_pops_for

mail_sni_sta
tus

rebuild_mail
_sni_config

release_out
going_email

save_spamd
_config

set_user_e
mail_forwar
d_destinatio
n

suspend_ou
tgoing_email

unsuspend_
outgoing_e
mail

validate_cur
rent_installe

```
]
}
}
```

Output (XML)

```
<result>
  <metadata>

  <version>1</version>

  <result>1</result>

  <reason>OK</reason>

  <command>modsec_get_s
ettings</command>
  </metadata>
  <data>
    <settings>

    <directive>SecAuditEn
gine</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</settin
g_id>

    <url>

    https://github.com/Sp
iderLabs/ModSecurity/
wiki/Reference-Manual
#secauditengine

    </url>
```

d_exim_config	<name>Audit Log Level</name>
validate_current_dkims	<radio_options>
validate_current_ptrs	<name>Log all transactions.</name>
validate_current_spfs	<option>On</option>
validate_exim_configuration_syntax	</radio_options>
▼ Market	<radio_options>
disable_market_provider	<name>Do not log any transactions.</name>
enable_market_provider	<option>Off</option>
get_adjusted_market_providers_products	</radio_options>
get_market_providers_commission_config	<radio_options>
get_market_providers_list	<name>Only log noteworthy transactions.</name>
get_market_providers_product_metadata	<option>RelevantOnly</option>
get_market_providers_products	</radio_options>
set_market_product_attribute	</settings>
set_market_provider_commission_id	<settings>
▼ ModSecurity™	<name>Connections Engine</name>
modsec_admin_rule	<url>
modsec_admin_vendor	https://github.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#seconnengine
modsec_assemble_config_text	</url>
modsec_batch_settings	<setting_id>1</setting_id>
modsec_check_rule	<radio_options>
modsec_clone_rule	<option>On</option>
modsec_deploy_all_rule	<name>Process the

<code>_changes</code>	<code>rules.</name></code>
<code>modsec_deploy_rule_changes</code>	<code></radio_options></code>
<code>modsec_deploy_settings_changes</code>	<code><radio_options></code>
<code>modsec_disable_rule</code>	<code><name>Do not process the rules.</name></code>
<code>modsec_disable_vendor</code>	<code><option>Off</option></code>
<code>modsec_disable_vendor_configs</code>	<code></radio_options></code>
<code>modsec_disable_vendor_updates</code>	<code><radio_options></code>
<code>modsec_disable_all_rule_changes</code>	<code><name></code>
<code>modsec_disable_rule_changes</code>	<code>Process the rules in verbose mode, but do not execute disruptive actions.</code>
<code>modsec_edit_rule</code>	<code></name></code>
<code>modsec_enable_vendor</code>	<code><option>DetectionOnly</option></code>
<code>modsec_enable_vendor_configs</code>	<code></radio_options></code>
<code>modsec_enable_vendor_updates</code>	<code><directive>SecConnEngine</directive></code>
<code>modsec_get_config_text</code>	<code><description></code>
<code>modsec_get_configs</code>	<code> This</code>
<code>modsec_get_configs_with_changes_pending</code>	<code>setting controls the</code>
<code>modsec_get_log</code>	<code>behavior of the</code>
<code>modsec_get_rules</code>	<code>connections engine.</code>
<code>modsec_get_settings</code>	<code></description></code>
<code>modsec_get_vendors</code>	<code><missing>1</missing></code>
<code>modsec_is_installed</code>	<code><engine>1</engine></code>
<code>modsec_make_config_active</code>	<code><default>Off</default></code>
<code>modsec_make</code>	<code>></code>
	<code><type>radio</type></code>
	<code> <state/></code>
	<code> </settings></code>
	<code> <settings></code>
	<code></radio_options></code>

ke_config_in active	<option>On</option>
modsec_pre view_vendor	<name>Process the rules.</name>
modsec_re move_rule	</radio_options>
modsec_re move_settin g	<radio_options>
modsec_re move_vend or	<option>Off</option>
modsec_rep ort_rule	<name>Do not process the rules.</name>
modsec_set _config_text	</radio_options>
modsec_set _setting	<radio_options>
modsec_un disable_rule	<name>
modsec_up date_vendor	Process the rules in verbose mode, but do not execute disruptive actions.
▼ Packages	</name>
_getpkgexte nsionform	<option>DetectionOnly </option>
add_overrid e_features_f or_user	</radio_options>
addpkg	<setting_id>2</settin g_id>
addpkgext	<url>
changepack age	https://github.com/Sp iderLabs/ModSecurity/ wiki/Reference-Manual #secruleengine
create_featu relist	</url>
delete_featu relist	<name>Rules Engine</name>
delpkgext	<state/>
editpkg	<type>radio</type>
get_availabl e_applicatio ns	<engine>1</engine>
get_availabl e_featurelist s	<missing>1</missing>
get_feature_ metadata	
get_feature_ names	
get_featureli st_data	
get_featureli 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

php_ini_get

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

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

```
<setting_id>3</setting_id>
```

```
<radio_options>
```

_directives
php_ini_set
_content
php_ini_set
_directives
php_set_def
ault_accoun
ts_to_fpm
php_set_ha
ndler
php_set_old
_fpm_flag
php_set_ses
sion_save_p
ath
php_set_sys
tem_default
_version
php_set_vh
ost_versions
▼ Resellers
acccounts
get_public_c
ontact
getresellerip
s
listacls
listresellers
resellerstats
saveaclist
set_public_c
ontact
setacls
setresellerip
s
setresellerli
mits
setresellerm
ainip
setresellern
ameservers
setresellerp
ackagelimit
setupreselle
r
suspendres
eller
terminateres
eller
unsetuprese
ller

```
<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
```



```

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
    convertopen

```

```

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

```

sshtoputty
deletesshkey
y
fetch_security_advice
generatesshkeypair
importsshkey
y
listsshkeys
▼ Server
Administration
add_configclusterserver
configurebackgroundprocesskiller
configurereverse
cors_proxy_get
create_user_session
delete_configclusterserver
enable_monitor_all_enabled_services
get_all_contact_importances
get_application_list
get_application_contact_event_importance
get_application_contact_importance
get_available_profiles
get_current_profile
get_password_strength
get_remote_access_hash
get_service_config
get_service_

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.

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

set_applicati
on_contact_
event_imp
ortance

set_applicati
on_contact_
importance

set_primary_
_servernam
e

set_service_
config_key

set_tweake
stting

sethostname

setminimum
passwordstr
engths

start_profile_
_activation

system_nee
ds_reboot

systemloada
vg

update_conf
igclusterserv
er

update_cont
act_email

verify_aim_a
ccess

verify_icq_a
ccess

verify_oscar_
_access

verify_postu
rl_access

verify_pushb
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

```
<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  
#secprematchlimitrec  
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>
```

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_autos
 ssl_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	<i>array of hashes</i>	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	<i>integer</i>	The setting ID. The function returns this value in the settings array.	A positive integer.	0
name	<i>string</i>	The setting's name. The function returns this value in the settings array.	A valid string.	Audit logging level
default	<i>string</i>	The setting's default value. The function returns this value in the settings array.	A positive integer.	1500

set_autoss_provider
 start_autoss_l_check_for_all_users
 start_autoss_l_check_for_one_user

▼ Styles and Themes

generate_cp
 anel_plugin
 list_styles
 load_style
 remove_log
 o
 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	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.	<ul style="list-style-type: none"> 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.	<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	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

[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...](#)

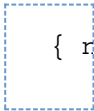
The function may specify one or more validators for a setting. The client should use these validators to perform front-end validation through the preferred implementation methods.

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.
------	---------------	--	-----------------	-----------------------