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

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

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

```
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/bin/whmapi1
```


```
{
   "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.com/SpiderLabs/ModSecurity/wiki/Reference-Manual#secauditengine",
            "setting_id":0,
            "name":"Audit Log Level",
            "state":"",
```


Function information

API Version: WHM API 1
Available in: WHM 11.46+
Methods: GET, POST
Required Parameters: (none)
Return Formats: JSON, XML

Important:

cPanel & WHM version 66 **deprecated** XML output.

About WHM API 1

WHM API 1 performs functions and accesses data in WHM.

Notes:

```
            "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",
            "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",
            "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
```


- Some functions and parameters may require that you authenticate as the root user.

convert_addon_fetch_domain_details

convert_addon_get_conversion_status

convert_addon_initiate_conversion

convert_addon_list_addon_domains

convert_addon_list_conversions

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_authn_linked_accounts

link_user_authn_provider

set_provider_client_configurations

set_provider_display_configurations

twofactorauth_disable_policy


```
behavior of the rules engine.",
            "type":"radio",
            "directive":"SecRuleEngine"
         },
         {
            "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
/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 Database."
         },
         {
            "validation":[
               {
                  "name":"startsWith",
                  "arg":"[|]"
               },
               "path"
            ],
            "missing":1,
            "state":"",
            "name":"Guardian Log",
            "setting_id":6,
            "url":"https://github.com/SpiderLabs
```


- You **must** use the appropriate WHM ports (2086 or 2087) to call WHM API functions.

Find a function

Related functions

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

backup_config_get

backup_config_set

backup_date_list

backup_destination_add

backup_destination_delete

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


```
/ModSecurity/wiki/Reference-Manual#secguardianlog",
            "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.",
            "type":"text",
            "directive":"SecGuardianLog"
         },
         {
            "description":"Specify 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
/ModSecurity/wiki/Reference-
Manual#secpcrematchlimitrecursion",
            "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
         }
      ]
   }
}
```

```
<result>
    <metadata>
        <version>1</version>
        <result>1</result>
```


- WHM API 1 Sections - ModSecurity — ModSecurity functions allow you to manage ModSecurity rules and vendors on your server.
- WHM API 1 Functions - modsec_add_rule — This function adds a new rule to a ModSecurity™ configuration staging file.
- WHM API 1 Functions - modsec_assemble_config_text — This function adds text to a ModSecurity™ configuration file.
- WHM API 1 Functions - modsec_add_vendor — This function adds a new ModSecurity™ vendor rule set to the server.
- WHM API 1 Functions - modsec_clone_rule — This function copies a ModSecurity™ rule with a new rule ID.

```
        <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/SpiderLabs/ModSecurity
/wiki/Reference-Manual#secconnengine
            </url>
            <setting_id>1</setting_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>SecConnEngine</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>
```

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

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

```
                <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>
            <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>
                <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</setting_id>
            <url>
                https://github.com/SpiderLabs/ModSecurity
/wiki/Reference-Manual#secgeolookupdb
            </url>
            <type>text</type>
            <state/>
            <validation>path</validation>
            <directive>SecGeoLookupDb</directive>
            <description>Specify a path for the
geolocation database.</description>
            <missing>1</missing>
        </settings>
```

start_background_mysql_upgrade

adddns

addzonerecord

addzonerecord (Reverse DNS)

create_parked_domain_for_user

dumpzone

editzonerecord

get_nameserver_config

getzonerecord

has_local_authority

killdns

listmxs

listzones

lookupnsip

lookupnsips

removezonerecord

resetzone

resolvedomainname

savemxs

setresolvers

update_nameservers_config

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

```
        <settings>
            <setting_id>5</setting_id>
            <url>
                https://github.com/SpiderLabs/ModSecurity
/wiki/Reference-Manual#secgsblookupdb
            </url>
            <name>Google Safe Browsing Database</name>
            <directive>SecGsbLookupDb</directive>
            <missing>1</missing>
            <description>
                Specify a path for the Google Safe
Browsing Database.
            </description>
            <state/>
            <type>text</type>
            <validation>path</validation>
        </settings>
        <settings>
            <state/>
            <type>text</type>
            <validation>
                <arg>[|]</arg>
                <name>startsWith</name>
            </validation>
            <validation>path</validation>
            <directive>SecGuardianLog</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/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.
            </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>
```

ea4_tomcat85_list

ea4_tomcat85_rem

cpgreylist_is_server_netblock_trusted

cpgreylist_list_entries_for_common_mail_provider

cpgreylist_load_common_mail_providers_config

cpgreylist_save_common_mail_providers_config

cpgreylist_status

cpgreylist_trust_entries_for_common_mail_provider

cpgreylist_untrust_entries_for_common_mail_provider

create_cpgreylist_trusted_host

delete_cpgreylist_trusted_host

disable_cpgreylist

enable_cpgreylist

load_cpgreylist_config

read_cpgreylist_deferred_entries

read_cpgreylist_trusted_host

save_cpgreylist_config

batch

cpanel

create_integration_group

create_integration_link

```
            <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</setting_id>
            <url>
                https://github.com/SpiderLabs/ModSecurity
/wiki/Reference-Manual#secpcrematchlimitrecursion
            </url>
            <directive>SecPcreMatchLimitRecursion<
/directive>
            <description>
                Define the match limit recursion of the
Perl Compatible Regular Expressions library.
            </description>
            <default>1500</default>
            <missing>1</missing>
            <type>number</type>
            <state/>
            <validation>positiveInteger</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.	`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.	`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

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`
`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.	`{ name: 'startsWith', arg: '[Ee]xample' }` **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

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

modsec_disable_rule

modsec_disable_vendor

modsec_disable_vendor_configs

modsec_disable_vendor_updates

modsec_discard_all_rule_changes

modsec_discard_rule_changes

modsec_edit_rule

modsec_enable_vendor

modsec_enable_vendor_configs

modsec_enable_vendor_updates

modsec_get_config_text

modsec_get_configs

modsec_get_configs_with_changes_pending

modsec_get_log

modsec_get_rules

modsec_get_settings

modsec_get_vendors

modsec_is_installed

modsec_make_config_active

modsec_make_config_inactive

modsec_preview_vendor

modsec_remove_rule

modsec_remove_setting

modsec_remove_vendor

modsec_report_rule

modsec_set_config_text

modsec_set_setting

modsec_undisable_rule

modsec_update_vendor

_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_featurelists

get_users_features_settings

getfeaturelist

getpkginfo

killpkg

listpkgs

manage_features

matchpkgs

read_featurelist

remove_override_features_for_user

update_featurelist

verify_user_has_feature

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_vhosts_by_version

php_get_vhost_versions

php_ini_get_content

php_ini_get_directives

php_ini_set_content

php_ini_set_directives

php_fpm_config_get

php_fpm_config_set

php_set_default_accounts_to_fpm

php_set_handler

php_set_old_fpm_flag

php_set_session_save_path

php_set_system_default_version

php_set_vhost_versions

acctcounts

get_public_contact

getresellerips

listacls

listresellers

resellerstats

saveacllist

set_public_contact

setacls

setresellerips

setresellerlimits

setresellermainip

setresellernameservers

setresellerpackagelimit

setupreseller

suspendreseller

terminatereseller

unsetupreseller

unsuspendreseller

delete_rpm_version

edit_rpm_version

get_rpm_version_data

install_rpm_plugin

list_rpms

package_manager_fixcache

package_manager_get_build_log

package_manager_get_package_info

package_manager_is_performing_actions

package_manager_list_packages

package_manager_resolve_actions

package_manager_submit_actions

package_manager_upgrade

uninstall_rpm_plugin

delete_hook

edit_hook

list_hooks

reorder_hooks

accesshash

authorizesshkey

check_remote_ssh_connection

convertopensshtoputty

deletesshkey

fetch_security_advice

generatesshkeypair

importsshkey

listsshkeys

add_configclusterserver

configurebackgroundprocesskiller

configureservice

cors_proxy_get

create_user_session

delete_configclusterserver

enable_monitor_all_enabled_services

get_all_contact_importances

get_appconfig_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_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

servicestatus

set_application_contact_event_importance

set_application_contact_importance

set_primary_servername

set_service_config_key

set_tweaksetting

sethostname

setminimumpasswordstrengths

start_profile_activation

system_needs_reboot

systemloadavg

update_configclusterserver

update_contact_email

verify_aim_access

verify_icq_access

verify_oscar_access

verify_posturl_access

verify_pushbullet_access

delete_ssl_vhost

disable_autossl

fetch_service_ssl_components

fetch_ssl_certificates_for_fqdns

fetch_ssl_vhosts

fetch_vhost_ssl_components

fetchcrtinfo

fetchsslinfo

generatessl

get_autossl_check_schedule

get_autossl_log

get_autossl_logs_catalog

get_autossl_metadata

get_autossl_pending_queue

get_autossl_pending_queue_for_domain

get_autossl_pending_queue_for_user

get_autossl_problems_for_domain

get_autossl_problems_for_user

get_autossl_providers

get_best_ssl_domain_for_service

install_service_ssl_certificate

installssl

listcrts

rebuildinstalledssldb

rebuilduserssldb

reset_autossl_provider

reset_service_ssl_certificate

set_autossl_metadata

set_autossl_metadata_key

set_autossl_provider

start_autossl_check_for_all_users

start_autossl_check_for_one_user

generate_cpanel_plugin

list_styles

load_style

remove_logo

remove_style

save_style

set_default

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

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

accept_eula

get_available_tiers

get_current_lts_expiration_status

get_lts_wexpire

getlongtermsupport

installed_versions

set_cpanel_updates

set_tier

update_upda
teconf

version