

# WHM API 1 Functions - set\_cphulk\_config\_key

## Guide to WHM API 1

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

- 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

## Description

This function sets cPHulk's configuration settings.

## Examples

### JSON API

```
https://hostname.example.com:2087/cpsess#####/json-api/set_cphulk_config_key?api.version=1&key=block_brute_force_with_firewall&value=0
```

### XML API

```
https://hostname.example.com:2087/cpsess#####/xml-api/set_cphulk_config_key?api.version=1&key=block_brute_force_with_firewall&value=0
```

### Command Line

```
whmapil set_cphulk_config_key key=block_brute_force_with_firewall value=0
```

### Output (JSON)

```
{  "data": {    "cphulk_config": {      "block_brute_force_with_firewall": 0,      "block_excessive_brute_force_with_firewall": 1,      "brute_force_period_m
```

## Function information

About WHM API 1 WHM API 1 performs functions and accesses data in WHM.

### Notes:

- Sc
- Yc
- mt
- us
- 20
- 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\_my.cnf\_for\_cpuser  
limitbw  
list\_users  
listaccts  
listlockedaccounts  
listsuspended  
modifyacct  
myprivs  
passwd  
quota\_enabled  
removeacct  
set\_digest\_auth  
showbw  
suspendacct  
unsuspendacct  
untrack\_acct

```
ins":5,  
"brute_force_period_sec":300,  
"can_temp_ban_firewall":1,  
"command_to_run_on_brute_force":"","  
"command_to_run_on_excessive_brute_force":"","  
"country_blacklist":"PK,BR",  
"country_whitelist":"US,AU",  
"ip_based_protection":0,  
"ip_brute_force_period_mins":15,  
"ip_brute_force_period_sec":900,  
"is_enabled":1,  
"lookback_period_min":360,  
"lookback_time":21600,  
"mark_as_brute":30,  
"max_failures":15,  
"max_failures_byip":5,  
"notify_on_brute":0,  
"notify_on_root_login":0,  
"notify_on_root_login_for_known_netblock":0,
```

## Find a function

- WHM API 1 Functions - cphulk\_status — This function returns the status of the cPhulk service.

- \_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

```

"username_based_protection":0,

"username_based_protection_for_root":0,

"username_based_protection_local_origin":0
  }
},
  "metadata":{
    "reason":"OK",

"command":"set_cphulk_config_key",
    "result":1,

```

- WHM API 1 Functions - create\_cphulk\_record — This function adds a new record or records to cPHulk's white list or black list.
- WHM API 1 Functions - delete\_cphulk\_record — This function deletes a record or records from cPHulk's white list or black list.

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

```
"version":1
}
```

Output (XML)

```
<result>
  <data>
    <cphulk_config>

    <block_brute_force_with_firewall>0</block_brute_force_with_firewall>

    <block_excessive_brute_force_with_firewall>1</block_excessive_brute_force_with_firewall>

    <brute_force_period_mins>5</brute_force_period_mins>

    <brute_force_period_sec>300</brute_force_period_sec>

    <can_temp_ban_firewall>1</can_temp_ban_firewall>

    <command_to_run_on_brute_force></command_to_run_on_brute_force>

    <command_to_run_on_excessive_brute_force></command_to_run_on_excessive_brute_force>

    <country_blacklist>PK,BR</country_blacklist>

    <country_whitelist>US,AU</country_whitelist>

    <ip_based_protection>
```

- WHM API 1 Functions - disable\_cphulk - This function disables the cPHulk service.

backup_destination_get	0</ip_based_protection>
backup_destination_list	<ip_brute_force_period_mins>15</ip_brute_force_period_mins>
backup_destination_set	
backup_destination_validate	<ip_brute_force_period_sec>900</ip_brute_force_period_sec>
backup_get_transport_status	<is_enabled>1</is_enabled>
backup_list_transported	
backup_set_list	<lookback_period_min>360</lookback_period_min>
backup_set_list_combined	
backup_skip_users_all	<lookback_time>21600</lookback_time>
backup_skip_users_all_status	<mark_as_brute>30</mark_as_brute>
backup_user_list	<max_failures>15</max_failures>
convert_and_migrate_from_legacy_config	
get_users_with_backup_metadata	<max_failures_byip>5</max_failures_byip>
list_cparchive_files	<notify_on_brute>0</notify_on_brute>
start_background_package	<notify_on_root_login>0</notify_on_root_login>
toggle_user_backup_status	<notify_on_root_login_for_known_netblock>0</notify_on_root_login_for_known_netblock>
▼ cPHulk	
cphulk_statuses	
create_cphulk_record	<username_based_protection>0</username_based_protection>
delete_cphulk_record	
disable_cphulk	<username_based_protection_for_root>0</username_based_protection_for_root>
enable_cphulk	
flush_cphulk_login_history	<username_based_protection_local_origin>0<

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\_activated

```
/username_based_protection_local_origin>  
</cphulk_config>  
</data>  
<metadata>  
<reason>OK</reason>  
  
<command>set_cphulk_config_key</command>  
<result>1</result>
```

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

addns

addzonerecord

addzonerecord (Reverse DNS)

dumpzone

editzonerecord

get\_nameserver\_config

getzonerecord

has\_local\_authority

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

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

## Parameters

- Notes:**
- You **must** set at least one key and value pair.
  - You can only enter one key and value pair per call.

Parameter	Type	Description	Possible values	Example
block_brute_force_with_firewall	<i>Boolean</i>	Whether to use cPanel & WHM's firewall to block brute force attacks.  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>1 — Use the firewall.</li> <li>0 — Do <b>not</b> use the firewall.</li> </ul>	0
block_excessive_brute_force_with_firewall	<i>Boolean</i>	Whether to use cPanel & WHM's firewall to block excessive brute force attacks.  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>1 — Use the firewall.</li> <li>0 — Do <b>not</b> use the firewall.</li> </ul>	0
brute_force_period_mins	<i>integer</i>	The number of minutes over which cPHulk measures all login attempts to a specific user's account.  This parameter defaults to 5.	A valid integer.	5

killdns	brute_force_ period_sec	<i>integer</i>	The number of seconds over which cPHulk measures all login attempts to a specific user's account.	A valid integer.	300
listmxs					
listzones					
lookupnsip					
lookupnsips					
removezone					
record					
resetzone					
resolvedom					
ainname					
savemxs					
setresolvers					
update_nam					
eservers_co					
nfig					
<ul style="list-style-type: none"> <li>▼ EasyApache <ul style="list-style-type: none"> <li>ea4_get_cur rently_install ed_packages</li> <li>ea4_get_ea _pkgs_state</li> <li>ea4_list_pro files</li> <li>ea4_metainf o</li> <li>ea4_migrati on</li> <li>ea4_pre_mi grate_check</li> <li>ea4_recom mendations</li> <li>ea4_save_p rofile</li> <li>ea4_tomcat 85_add</li> <li>ea4_tomcat 85_list</li> <li>ea4_tomcat 85_rem</li> </ul> </li> <li>▼ Greylisting <ul style="list-style-type: none"> <li>cpgreylist_is _server_net block_truste d</li> <li>cpgreylist_li st_entries_f or_common _mail_provid er</li> <li>cpgreylist_lo ad_common _mail_provid</li> </ul> </li> </ul>	command_to_r un_on_brute_ force	<i>string</i>	The command to run when an IP address triggers brute force protection.	<ul style="list-style-type: none"> <li>• A valid command.</li> <li>• An empty string.</li> </ul>	" "
			<p style="text-align: center;"><b>Note</b> : For a list of commands, read the <i>Command variables</i> section of our cPHulk Brute Force Protection documentation.</p>		
			This parameter defaults to an empty string.		

<p>ers_config</p> <p>cpgreylist_s ave_commo n_mail_provi ders_config</p> <p>cpgreylist_st atus</p> <p>cpgreylist_tr ust_entries_ for_common _mail_provid er</p> <p>cpgreylist_u ntrust_entrie s_for_comm on_mail_pro vider</p> <p>create_cpgr eylist_truste d_host</p> <p>delete_cpgr eylist_truste d_host</p> <p>disable_cpgr eylist</p> <p>enable_cpgr eylist</p> <p>load_cpgreyl ist_config</p> <p>read_cpgrey list_deferred _entries</p>	<p>command_to_r un_on_excess ive_brute_fo rce</p> <p><i>string</i></p>	<p>The command to run when the system blocks an IP address blocked for a one day period.</p> <div data-bbox="732 296 873 1024" style="border: 1px solid orange; padding: 5px;"> <p><b>Note</b> : For a list of commands, read the <i>Command variables</i> section of our cPHulk Brute Force Protection documentation.</p> </div> <p>This parameter defaults to an empty string.</p>	<ul style="list-style-type: none"> <li>• A valid command.</li> <li>• An empty string.</li> </ul>	<p>" "</p>
<p>read_cpgrey list_trusted_ host</p> <p>save_cpgrey list_config</p> <p>▼ Integration</p> <p>batch</p> <p>cpanel</p> <p>create_integ ration_group</p> <p>create_integ ration_link</p> <p>get_integrati on_link_user_ _config</p> <p>list_integrati on_groups</p> <p>list_integrati on_links</p> <p>remove_inte gration_grou p</p> <p>remove_inte</p>	<p>country_blac klist</p> <p><i>string</i></p>	<p>The countries to blacklist.</p> <div data-bbox="732 1199 873 1965" style="border: 1px solid orange; padding: 5px;"> <p><b>Notes:</b></p> </div>	<ul style="list-style-type: none"> <li>• A comma-separated list of valid ISO 3166-1 alpha-2 country codes.</li> <li>• An empty string.</li> </ul>	<p>PK, BR</p>

gration\_link

update\_inte  
gration\_link  
\_token

▼ IP Addresses

addips

delip

get\_public\_i  
p

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\_pub  
lic\_ip

setsiteip

▼ Mail

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

• This value overwrites the current default blacklist.

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

• E  
n  
t  
e  
r  
a  
c  
c  
o  
m  
m  
a  
-  
s  
e  
p  
a  
r  
a  
t  
e  
d  
l  
i  
s  
t  
o  
e  
n  
t  
e  
r  
m  
o  
r  
e  
t  
h  
a  
n  
o  
n  
e  
v  
a  
l  
u  
e  
.

validate\_current\_installed\_exim\_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

• Formalists of countries, run the WHM API 1 function on get - countries with this known - ip - ranges.

modsec_deploy_all_rule_changes			This parameter defaults to an empty string.		
modsec_deploy_rule_changes	country_whitelist	string	The countries to whitelist.	<ul style="list-style-type: none"> <li>A comma-separated list of valid ISO 3166-1 alpha-2 country codes.</li> <li>An empty string.</li> </ul>	US, AU
modsec_deploy_settings_changes			<p><b>Note:</b></p> <ul style="list-style-type: none"> <li>This is a valid overview of the current whitelist.</li> </ul>		
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\_uninstall\_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

• E  
n  
t  
e  
r  
a  
c  
o  
m  
m  
a  
-  
s  
e  
p  
a  
r  
a  
t  
e  
d  
l  
i  
s  
t  
o  
e  
n  
t  
e  
r  
m  
o  
r  
e  
t  
h  
a  
n  
o  
n  
e  
v  
a  
l  
u  
e  
.

sts  
get\_users\_f  
eatures\_sett  
ings  
getfeaturelis  
t  
getpkginfo  
killpkg  
listpkgs  
manage\_fea  
tures  
matchpkgs  
read\_feature  
list  
remove\_ove  
rride\_feature  
s\_for\_user  
update\_feat  
urelist  
verify\_user\_  
has\_feature

▼ PHP

convert\_all\_  
domains\_to\_  
\_fpm  
get\_fpm\_co  
unt\_and\_util  
ization  
is\_conversio  
n\_in\_progre  
ss  
php\_get\_def  
ault\_accoun  
ts\_to\_fpm  
php\_get\_ha  
ndlers  
php\_get\_im  
pacted\_dom  
ains  
php\_get\_ins  
talled\_versio  
ns  
php\_get\_old  
\_fpm\_flag  
php\_get\_sys  
tem\_default  
\_version  
php\_get\_vh  
osts\_by\_ver  
sion  
php\_get\_vh  
ost\_versions  
php\_ini\_get  
\_content

• F  
o  
r  
a  
l  
i  
s  
t  
o  
f  
c  
o  
u  
n  
t  
r  
i  
e  
s  
,  
r  
u  
n  
t  
h  
e  
W  
H  
M  
A  
P  
I  
f  
u  
n  
c  
t  
i  
o  
n  
g  
e  
t  
\_  
c  
o  
u  
n  
t  
r  
i  
e  
s  
\_  
w  
i  
t  
h  
\_  
k  
n  
o  
w  
n  
\_  
i  
p  
\_  
r  
a  
n  
g  
e  
s  
.

php_ini_get_directives			This parameter defaults to an empty string.		
php_ini_set_content	ip_based_protection	Boolean	Whether to enable IP address-based protection on all requests.	<ul style="list-style-type: none"> <li>• 1 — Enable IP-based protection.</li> <li>• 0 — Disable IP-based protection.</li> </ul>	1
php_ini_set_directives					
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_whoost_versions					
<a href="#">▼ Resellers</a> acccounts get_public_contact getresellers listacks listresellers resellerstats saveacllist set_public_contact setacks setresellers setresellerlimits setresellermainip setresellerameservers setresellerpackagelimit setupreseller suspendreseller terminatereseller unsetuprese			<p><b>Note</b> : If you set the ip_based_protection parameter to 0, you <b>can not</b> use the following parameters:</p> <ul style="list-style-type: none"> <li>• block -brute -force -receive -with -html -firewall ll</li> </ul>		

ller

unsuspendr  
eseller

▼ 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

▼ Script Hooks

delete\_hook

edit\_hook

list\_hooks

reorder\_hoo  
ks

▼ Security

accesshash

authorizessh  
key

check\_remo  
te\_ssh\_conn  
ection

• b  
l  
o  
c  
k  
-  
e  
x  
c  
e  
s  
s  
i  
v  
e  
-  
b  
r  
u  
t  
e  
-  
f  
o  
r  
c  
e  
-  
w  
i  
t  
h  
-  
f  
i  
r  
e  
w  
a  
l  
l  
l  
• i  
p  
-  
b  
r  
u  
t  
e  
-  
f  
o  
r  
c  
e  
-  
p  
e  
r  
i  
o  
d  
-  
m  
i  
n  
s

convertopen  
 sshotputty  
 deletesshkey  
 fetch\_security\_advice  
 generatesshkeypair  
 importsshkey  
 listsshkeys  
 Server  
 Administration  
 add\_configclusterserver  
 configurebackgroundprocesskiller  
 configureservervice  
 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\_has  
 get\_service\_config

		<ul style="list-style-type: none"> <li>ip_brute_force_period_secs</li> </ul>		
		This parameter defaults to 1.		
ip_brute_force_period_mins	integer	<p>The number of minutes in which cPHulk measures an attacker's login attempts.</p> <p>The parameter defaults to 15.</p>	A valid integer.	15
ip_brute_force_period_secs	integer	<p>The number of seconds in which cPHulk measures an attacker's login attempts.</p> <p>The parameter defaults to the ip_brute_force_period_mins parameter's value multiplied by 60.</p>	A valid integer.	900
is_enabled	Boolean	<p>Whether to enable the cPHulk service.</p> <p>This parameter defaults to 1.</p>	<ul style="list-style-type: none"> <li>1 — Enable.</li> <li>0 — Disable.</li> </ul>	1
lookback_period_min	integer	<p>The number of minutes over which cPHulk counts failed logins against a user.</p> <p>This parameter defaults to 360.</p>	A valid integer.	360

get_service_config_key	lookback_time	integer	The number of seconds over which cPHulk counts failed logins against a user.  The parameter defaults to the lookback_period_min parameter's value multiplied by 60.	A valid integer.	21600
get_tcp4_sockets	mark_as_brute	integer	The maximum number of failures from a specific IP address before cPHulk blocks that address for a two-week period.  This parameter defaults to 30.	A valid integer.	30
get_tcp6_sockets					
get_tweaksetting	max_failures	integer	The maximum number of failures that cPHulk allows per account within the defined time range.  This parameter defaults to 30.	A valid integer.	30
get_udp4_sockets					
get_udp6_sockets	max_failures_byip	integer	The maximum number of failures from a specific IP address before cPHulk locks out that address.  This parameter defaults to 5.	A valid integer.	5
get_update_availability					
get_users_links	notify_on_brute	Boolean	Whether cPHulk will send a notification when it detects a brute force attack.  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>• 1 — Send the notification.</li> <li>• 0 — Do <b>not</b> send the notification.</li> </ul>	0
getdiskusage					
gethostname	notify_on_root_login	Boolean	Whether cPHulk will send a notification when the root user successfully logs in from an IP address that is not on the whitelist.  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>• 1 — Send the notification.</li> <li>• 0 — Do <b>not</b> send the notification.</li> </ul>	0
is_role_enabled					
list_configclusterservers					
loadavg					
nvget					
nvset					
personalization_get					
personalization_set					
purchase_license					
reboot					
remove_in_progress_exim_configedit					
restartservice					
restore_config_from_file					
restore_config_from_upload					
run_cpkeyctl					
send_test_posturl					
send_test_pushbullet_note					
servicestatus					

s

set\_application\_contact\_event\_importance

set\_application\_contact\_importance

set\_primary\_servername

set\_service\_config\_key

set\_tweaking

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

▼ SSL

disable\_autossll

fetch\_service\_ssl\_components

fetch\_ssl\_certificates\_for\_fqdns

fetch\_ssl\_hosts

fetch\_vhost\_ssl\_components

notify_on_root_login_for_known_netblock	<i>Boolean</i>	Whether cPHulk sends a notification upon successful root login when the IP address is not on the whitelist, but from a known netblock  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>1 — Send the notification.</li> <li>0 — Do <b>not</b> send the notification.</li> </ul>	0
username_based_protection	<i>Boolean</i>	Whether to enable username-based protection on all requests.  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>1 — Enable.</li> <li>0 — Disable.</li> </ul>	0
username_based_protection_for_root	<i>Boolean</i>	Whether to allow username-based protection to lock out the root user.  This parameter defaults to 0.	<ul style="list-style-type: none"> <li>1 — Allow.</li> <li>0 — Do <b>not</b> allow.</li> </ul>	0
username_based_protection_local_origin	<i>Boolean</i>	Whether to enable username-based protection <b>only</b> on requests that originate from a local IP address.  This parameter defaults to 1.	<ul style="list-style-type: none"> <li>1 — Enable.</li> <li>0 — Disable.</li> </ul>	1

## Returns

Return	Type	Description	Possible values	Example
--------	------	-------------	-----------------	---------

<p>fetchcrtinfo</p> <p>fetchsslinfo</p> <p>generatessl</p> <p>get_autossl_check_schedule</p> <p>get_autossl_log</p> <p>get_autossl_logs_catalog</p> <p>get_autossl_metadata</p> <p>get_autossl_pending_queue</p> <p>get_autossl_pending_queue_for_domain</p> <p>get_autossl_pending_queue_for_user</p> <p>get_autossl_problems_for_domain</p> <p>get_autossl_problems_for_user</p> <p>get_autossl_providers</p> <p>get_best_ssl_domain_for_service</p> <p>install_service_ssl_certificate</p> <p>installssl</p> <p>listcrt</p> <p>rebuildinstallssl</p> <p>rebuilduserssl</p> <p>reset_autossl_provider</p> <p>reset_service_ssl_certificate</p> <p>set_autossl_metadata</p> <p>set_autossl_metadata_key</p>	<p>cphulk_config</p> <p><i>hash</i></p>	<p>A hash of cPHulk configuration settings.</p>	<p>This hash contains the block_brute_force_with_firewall, block_excessive_brute_force_with_firewall, brute_force_period_mins, brute_force_period_sec, can_temp_ban_firewall, command_to_run_on_brute_force, command_to_run_on_excessive_brute_force, country_blacklist, country_witelist, ip_based_protection, ip_brute_force_period_mins, ip_brute_force_period_sec, is_enabled, lookback_period_min, lookback_time, mark_as_brute, max_failures, max_failures_by_ip, notify_on_brute, notify_on_root_login, notify_on_root_login_for_known_netblock, username_based_protection, username_based_protection_for_root, and username_based_protection_local_origin returns.</p>	
<p>block_brute_force_with_firewall</p>	<p><i>Boolean</i></p>	<p>Whether to use cPanel &amp; WHM's firewall to block brute force attacks.</p> <p>The function returns this value in the <code>cphulk_config_hash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Use the firewall.</li> <li>• 0 — Do not use the firewall.</li> </ul>	<p>0</p>

- set\_autoss\_provider
- start\_autossil\_check\_for\_all\_users
- start\_autossil\_check\_for\_one\_user
- generate\_cpanel\_plugin
    - list\_styles
    - load\_style
    - remove\_log
    - remove\_style
    - save\_style
    - set\_default
- ticket\_create\_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

block_excessive_brute_force_with_firewall	<i>Boolean</i>	<p>Whether to use cPanel &amp; WHM's firewall to block excessive brute force attacks.</p> <p>The function returns this value in the <code>cpanel_confighash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Use the firewall.</li> <li>• 0 — Do <b>not</b> use the firewall.</li> </ul>	0
brute_force_period_mins	<i>integer</i>	<p>The number of minutes over which cPHulk measures all login attempts to a specific user's account.</p> <p>The function returns this value in the <code>cpanel_confighash</code>.</p>	A valid integer.	5
brute_force_period_sec	<i>integer</i>	<p>The number of seconds over which cPHulk measures all login attempts to a specific user's account.</p> <p>The function returns this value in the <code>cpanel_confighash</code>.</p>	A valid integer.	300
can_temp_ban_firewall	<i>Boolean</i>	<p>Whether the system firewall can apply temporary IP address bans.</p> <p>The function returns this value in the <code>cpanel_confighash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Can temporarily apply IP address bans.</li> <li>• 0 — <b>Cannot</b> temporarily apply IP address bans.</li> </ul> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p style="text-align: center;"><b>Note</b> :</p> </div>	1

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\_lts\_expiration\_status  
get\_lts\_expire  
getlongterm support  
installed\_versions  
set\_cpanel\_updates

If this return's value is 0, then the ip\_base\_protect ion parameter is **not** available, which means that you cannot use the following parameters:

- block\_rute\_force\_with\_firewall

set\_tier  
update\_upd  
ateconf  
version

- b  
l  
o  
c  
k  
-  
e  
x  
c  
e  
s  
s  
i  
v  
e  
-  
b  
r  
u  
t  
e  
-  
f  
o  
r  
c  
e  
-  
w  
i  
t  
h  
-  
f  
i  
r  
e  
w  
a  
l  
l
- i  
p  
-  
b  
r  
u  
t  
e  
-  
f  
o  
r  
c  
e  
-  
p  
e  
r  
i  
o  
d  
-  
m  
i  
n  
s

			<ul style="list-style-type: none"> <li>ip-brute-force-period-sec</li> </ul>	
command_to_run_on_brute_force	string	<p>The command to run when an IP address triggers brute force protection.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>A valid command.</li> <li>An empty string.</li> </ul>	""
command_to_run_on_excessive_brute_force	string	<p>The command to run when the system blocks an IP address blocked for a one day period.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>A valid command.</li> <li>An empty string.</li> </ul>	""
country_blacklist	string	<p>The countries to blacklist.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>A comma-separated list of valid ISO 3166-1 alpha-2 country codes.</li> <li>An empty string.</li> </ul>	PK, BR
country_whitelist	string	<p>The countries to whitelist.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>A comma-separated list of valid ISO 3166-1 alpha-2 country codes.</li> <li>An empty string.</li> </ul>	US, AU

ip_based_protection	<i>Boolean</i>	<p>Whether IP address-based protection on all requests is enabled.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Enabled.</li> <li>• 0 — Disabled.</li> </ul>	1
ip_brute_force_period_mins	<i>integer</i>	<p>The number of minutes in which cPHulk measures an attacker's login attempts.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	15
ip_brute_force_period_secs	<i>integer</i>	<p>The number of seconds in which cPHulk measures an attacker's login attempts.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	900
is_enabled	<i>Boolean</i>	<p>Whether the cPHulk service is enabled.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Enabled.</li> <li>• 0 — Disabled.</li> </ul>	1
lookback_period_min	<i>integer</i>	<p>The number of minutes over which cPHulk counts failed logins against a user.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	360
lookback_time	<i>integer</i>	<p>The number of seconds over which cPHulk counts failed logins against a user.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	21600

mark_as_brute	<i>integer</i>	<p>The maximum number of failures from a specific IP address before cPHulk blocks that address for a two-week period.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	30
max_failures	<i>integer</i>	<p>The maximum number of failures that cPHulk allows per account within the defined time range.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	30
max_failures_byip	<i>integer</i>	<p>The maximum number of failures from a specific IP address before cPHulk locks out that address.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	A valid integer.	5
notify_on_brute	<i>Boolean</i>	<p>Whether cPHulk will send a notification when it detects a brute force attack.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Send the notification .</li> <li>• 0 — Do <b>not</b> send the notification .</li> </ul>	0
notify_on_root_login	<i>Boolean</i>	<p>Whether cPHulk will send a notification when the root user successfully logs in from an IP address that is not on the whitelist.</p> <p>The function returns this value in the <code>cphulk_confighash</code>.</p>	<ul style="list-style-type: none"> <li>• 1 — Send the notification .</li> <li>• 0 — Do <b>not</b> send the notification .</li> </ul>	0

notify_on_root_login_for_known_netblock	<i>Boolean</i>	Whether cPHulk sends a notification upon successful root login when the IP address is not on the whitelist, but from a known netblock  The function returns this value in the <code>cphulk_confighash</code> .	<ul style="list-style-type: none"> <li>• 1 — Send the notification.</li> <li>• 0 — Do <b>not</b> send the notification.</li> </ul>	0
username_based_protection	<i>Boolean</i>	Whether username-based protection on all requests is enabled.  The function returns this value in the <code>cphulk_confighash</code> .	<ul style="list-style-type: none"> <li>• 1 — Enabled.</li> <li>• 0 — Disabled.</li> </ul>	0
username_based_protection_for_root	<i>Boolean</i>	Whether username-based protection can lock out the root user.  The function returns this value in the <code>cphulk_confighash</code> .	<ul style="list-style-type: none"> <li>• 1 — Allowed.</li> <li>• 0 — <b>Not</b> allowed.</li> </ul>	0
username_based_protection_local_origin	<i>Boolean</i>	Whether username-based protection <b>only</b> on requests that originate from a local IP address.  The function returns this value in the <code>cphulk_confighash</code> .	<ul style="list-style-type: none"> <li>• 1 — Enabled.</li> <li>• 0 — Disabled.</li> </ul>	1