» checkpoint_management_access_rule

This resource allows you to add/update/delete Check Point Access Rule.

» Example Usage

```
resource "checkpoint_management_access_rule" "rule1" {
  layer = "Network"
  position = {top = "top"}
  name = "test1"
}

resource "checkpoint_management_access_rule" "rule2" {
  layer = "Network"
  position = {below = checkpoint_management_access_rule.rule1.name}
  name = "test2"
  enabled = true
}

resource "checkpoint_management_access_rule" "rule3" {
  layer = "Network"
  position = {below = checkpoint_management_access_rule.rule2.name}
  name = "test3"
  action = "Accept"
  action_settings = {
    enable_identity_captive_portal = true
  }
  source = ["DMZNet", "DMZZone", "WirelessZone"]
  enabled = true
  destination = ["InternalNet", "CPDShield"]
  destination_negate = true
}

resource "checkpoint_management_access_rule" "rule4" {
  layer = "Network"
  position = {below = checkpoint_management_access_rule.rule3.name}
  name = "test4"
  track = {
    type = "Log"
  }
  enabled = false
}

resource "checkpoint_management_access_rule" "rule5" {
```

```
  layer = "Network"
  position = {below = checkpoint_management_access_rule.rule4.name}
  name = "test5"
  action = "Accept"
}

resource "checkpoint_management_access_rule" "rule6" {
  layer = "Network"
  position = {below = checkpoint_management_access_rule.rule5.name}
  name = "test6"
}
```

» Argument Reference

The following arguments are supported:

- `layer` - (Required) Layer that the rule belongs to identified by the name or UID.
- `position` - (Required) Position in the rulebase. Position blocks are documented below.
- `name` - (Required) Rule name.
- `action` - (Optional) \"Accept\", \"Drop\", \"Ask\", \"Inform\", \"Reject\", \"User Auth\", \"Client Auth\", \"Apply Layer\".
- `action_settings` - (Optional) Action settings. Action settings blocks are documented below.
- `content` - (Optional) List of processed file types that this rule applies on.
- `content_direction` - (Optional) On which direction the file types processing is applied.
- `content_negate` - (Optional) True if negate is set for data.
- `custom_fields` - (Optional) Custom fields. Custom fields blocks are documented below.
- `destination` - (Optional) Collection of Network objects identified by the name or UID.
- `destination_negate` - (Optional) True if negate is set for destination.
- `enabled` - (Optional) Enable/Disable the rule.
- `inline_layer` - (Optional) Inline Layer identified by the name or UID. Relevant only if \"Action\" was set to \"Apply Layer\".
- `install_on` - (Optional) Which Gateways identified by the name or UID to install the policy on.
- `service` - (Optional) Collection of Network objects identified by the name or UID.
- `service_negate` - (Optional) True if negate is set for service.
- `source` - (Optional) Collection of Network objects identified by the name or UID.
- `source_negate` - (Optional) True if negate is set for source.

- `time` - (Optional) List of time objects. For example: \"Weekend\", \"Off-Work\", \"Every-Day\".
- `track` - (Optional) Track Settings. Track Settings blocks are documented below.
- `user_check` - (Optional) User check settings. User check settings blocks are documented below.
- `vpn` - (Optional) Communities or Directional.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `comments` - (Optional) Comments string.

`position` supports the following:

- `top` - (Optional) Add rule at the top of the rulebase.
- `above` - (Optional) Add rule above specific section/rule identified by uid or name.
- `below` - (Optional) Add rule below specific section/rule identified by uid or name.
- `bottom` - (Optional) Add rule at the bottom of the rulebase.

`action_settings` supports the following:

- `enable_identity_captive_portal` - (Optional) N/A.
- `limit` - (Optional) N/A.

`custom_fields` supports the following:

- `field_1` - (Optional) First custom field.
- `field_2` - (Optional) Second custom field.
- `field_3` - (Optional) Third custom field.

`track` supports the following:

- `accounting` - (Optional) Turns accounting for track on and off.
- `alert` - (Optional) Type of alert for the track.
- `enable_firewall_session` - (Optional) Determine whether to generate session log to firewall only connections.
- `per_connection` - (Optional) Determines whether to perform the log per connection.
- `per_session` - (Optional) Determines whether to perform the log per session.
- `type` - (Optional) \"Log\", \"Extended Log\", \"Detailed Log\", \"None\".

`user_check` supports the following:

- `confirm` - (Optional) N/A.
- `custom_frequency` - (Optional) N/A. Custom Frequency blocks are documented below.

- `frequency` - (Optional) N/A.
- `interaction` - (Optional) N/A.

`custom_frequency` supports the following:

- `every` - (Optional) N/A.
- `unit` - (Optional) N/A.

» checkpoint_management_address_range

This resource allows you to add/update/delete Check Point Address Range.

» Example Usage

```
resource "checkpoint_management_address_range" "example" {
  name = "New Address Range 1"
  ipv4_address_first = "192.0.2.1"
  ipv4_address_last = "192.0.2.10"
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `ipv4_address_first` - (Optional) First IPv4 address in the range.
- `ipv6_address_first` - (Optional) First IPv6 address in the range.
- `ipv4_address_last` - (Optional) Last IPv4 address in the range.
- `ipv6_address_last` - (Optional) Last IPv6 address in the range.
- `nat_settings` - (Optional) NAT settings. NAT settings blocks are documented below.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.
- `groups` - (Optional) Collection of group identifiers.
- `tags` - (Optional) Collection of tag identifiers.

`nat_settings` supports the following:

- `auto_rule` - (Optional) Whether to add automatic address translation rules.
- `ipv4_address` - (Optional) IPv4 address.

- `ipv6_address` - (Optional) IPv6 address.
- `hide_behind` - (Optional) Hide behind method. This parameter is not required in case \"method\" parameter is \"static\".
- `install_on` - (Optional) Which gateway should apply the NAT translation.
- `method` - (Optional) NAT translation method.

» checkpoint_management_group

This resource allows you to add/update/delete Check Point Group.

» Example Usage

```
resource "checkpoint_management_group" "example" {
  name = "New Group 4"
  members = [ "New Host 1", "My Test Host 3" ]
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `members` - (Optional) Collection of Network objects identified by the name or UID.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.
- `groups` - (Optional) Collection of group identifiers.
- `tags` - (Optional) Collection of tag identifiers.

» checkpoint_management_host

This resource allows you to add/update/delete Check Point Host.

» Example Usage

```
resource "checkpoint_management_host" "example" {
  name = "New Host 1"
  ipv4_address = "192.0.2.1"
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `ipv4_address` - (Optional) IPv4 address.
- `ipv6_address` - (Optional) IPv6 address.
- `interfaces` - (Optional) Host interfaces. Host interfaces blocks are documented below.
- `nat_settings` - (Optional) NAT settings. NAT settings blocks are documented below.
- `host_servers` - (Optional) Servers Configuration. Servers Configuration blocks are documented below.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.
- `groups` - (Optional) Collection of group identifiers.
- `tags` - (Optional) Collection of tag identifiers.

`interfaces` supports the following:

- `name` - (Required) Object name. Should be unique in the domain.
- `subnet4` - (Optional) IPv4 network address.
- `subnet6` - (Optional) IPv6 network address.
- `mask_length4` - (Optional) IPv4 network mask length.
- `mask_length6` - (Optional) IPv6 network mask length.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.

`nat_settings` supports the following:

- `auto_rule` - (Optional) Whether to add automatic address translation rules.

- `ipv4_address` - (Optional) IPv4 address.
- `ipv6_address` - (Optional) IPv6 address.
- `hide_behind` - (Optional) Hide behind method. This parameter is not required in case \"method\" parameter is \"static\".
- `install_on` - (Optional) Which gateway should apply the NAT translation.
- `method` - (Optional) NAT translation method.

`host_servers` supports the following:

- `dns_server` - (Optional) Gets True if this server is a DNS Server.
- `mail_server` - (Optional) Gets True if this server is a Mail Server.
- `web_server` - (Optional) Gets True if this server is a Web Server.
- `web_server_config` - (Optional) Web Server configuration. Web Server configuration blocks are documented below.

`web_server_config` supports the following:

- `additional_ports` - (Optional) Server additional ports.
- `application_engines` - (Optional) Application engines of this web server.
- `listen_standard_port` - (Optional) "Whether server listens to standard port.
- `operating_system` - (Optional) Operating System.
- `protected_by` - (Optional) Network object which protects this server identified by the name or UID.

» checkpoint_management_network

This resource allows you to add/update/delete Check Point Network Object.

» Example Usage

```
resource "checkpoint_management_network" "example" {
  name = "New Network 1"
  subnet4 = "192.0.2.0"
  mask_length4 = 32
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `subnet4` - (Optional) IPv4 network address.
- `subnet6` - (Optional) IPv6 network address..

- `mask_length4` - (Optional) IPv4 network mask length.
- `mask_length6` - (Optional) IPv6 network mask length.
- `nat_settings` - (Optional) NAT settings. NAT settings blocks are documented below.
- `tags` - (Optional) Collection of tag identifiers.
- `groups` - (Optional) Collection of group identifiers.
- `broadcast` - (Optional) "Allow broadcast address inclusion.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `comments` - (Optional) Comments string.

`nat_settings` supports the following:

- `auto_rule` - (Optional) Whether to add automatic address translation rules.
- `ipv4_address` - (Optional) IPv4 address.
- `ipv6_address` - (Optional) IPv6 address.
- `hide_behind` - (Optional) Hide behind method. This parameter is not required in case \"method\" parameter is \"static\".
- `install_on` - (Optional) Which gateway should apply the NAT translation.
- `method` - (Optional) NAT translation method.

» checkpoint_management_package

This resource allows you to add/update/delete Check Point Package Object.

» Example Usage

```
resource "checkpoint_management_network" "example" {
  name = "New_Standard_Package_1"
  comments = "My Comments"
  color = "green"
  threat_prevention = false
  access = true
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `access` - (Optional) True - enables, False - disables access & NAT policies, empty - nothing is changed.
- `desktop_security` - (Optional) True - enables, False - disables Desktop security policy, empty - nothing is changed.
- `qos` - (Optional) True - enables, False - disables QoS policy, empty - nothing is changed.
- `qos_policy_type` - (Optional) QoS policy type.
- `threat_prevention` - (Optional) True - enables, False - disables Threat policy, empty - nothing is changed.
- `vpn_traditional_mode` - (Optional) True - enables, False - disables VPN traditional mode, empty - nothing is changed.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `comments` - (Optional) Comments string.
- `tags` - (Optional) Collection of tag identifiers.

» checkpoint_management_service_group

This resource allows you to add/update/delete Check Point Service Group.

» Example Usage

```
resource "checkpoint_management_service_group" "example" {
  name = "New Service Group 1"
  members = [ "https", "bootp", "nisplus", "HP-OpCdistm" ]
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `members` - (Optional) Collection of Network objects identified by the name or UID.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.

- `comments` - (Optional) Comments string.
- `groups` - (Optional) Collection of group identifiers.
- `tags` - (Optional) Collection of tag identifiers.

» checkpoint_management_service_tcp

This resource allows you to add/update/delete Check Point Service Tcp.

» Example Usage

```
resource "checkpoint_management_service_tcp" "example" {
  name = "New_TCP_Service_1"
  port = 5669
  keep_connections_open_after_policy_installation = false
  session_timeout = 0
  match_for_any = true
  sync_connections_on_cluster = true
  aggressive_aging = {
    enable = true
    timeout = 360
    use_default_timeout = false
  }
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `port` - (Optional) The number of the port used to provide this service. To specify a port range, place a hyphen between the lowest and highest port numbers, for example 44-55.
- `aggressive_aging` - (Optional) Sets short (aggressive) timeouts for idle connections. Aggressive Aging blocks are documented below.
- `keep_connections_open_after_policy_installation` - (Optional) Keep connections open after policy has been installed even if they are not allowed under the new policy. This overrides the settings in the Connection Persistence page. If you change this property, the change will not affect open connections, but only future connections.
- `match_by_protocol_signature` - (Optional) A value of true enables matching by the selected protocol's signature - the signature identifies the protocol as genuine. Select this option to limit the port to the specified

protocol. If the selected protocol does not support matching by signature, this field cannot be set to true.

- `match_for_any` - (Optional) Indicates whether this service is used when 'Any' is set as the rule's service and there are several service objects with the same source port and protocol.
- `override_default_settings` - (Optional) Indicates whether this service is a Data Domain service which has been overridden.
- `protocol` - (Optional) Select the protocol type associated with the service, and by implication, the management server (if any) that enforces Content Security and Authentication for the service. Selecting a Protocol Type invokes the specific protocol handlers for each protocol type, thus enabling higher level of security by parsing the protocol, and higher level of connectivity by tracking dynamic actions (such as opening of ports).
- `session_timeout` - (Optional) Time (in seconds) before the session times out.
- `source_port` - (Optional) Port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected during packet inspection. Otherwise, the source port is not inspected.
- `sync_connections_on_cluster` - (Optional)Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster.
- `use_default_session_timeout` - (Optional) Use default virtual session timeout.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.
- `groups` - (Optional) Collection of group identifiers.
- `tags` - (Optional) Collection of tag identifiers.

`aggressive_aging` supports the following:

- `default_timeout` - (Optional) Default aggressive aging timeout in seconds.
- `enable` - (Optional) N/A
- `timeout` - (Optional) Aggressive aging timeout in seconds.
- `use_default_timeout` - (Optional) N/A.

» checkpoint_management_service_udp

This resource allows you to add/update/delete Check Point Service Udp.

» Example Usage

```
resource "checkpoint_management_service_udp" "example" {
  name = "New_UDP_Service_1"
  port = 5669
  keep_connections_open_after_policy_installation = false
  session_timeout = 0
  match_for_any = true
  sync_connections_on_cluster = true
  aggressive_aging = {
    enable = true
    timeout = 360
    use_default_timeout = false
  }
  accept_replies = false
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `accept_replies` - (Optional) N/A.
- `aggressive_aging` - (Optional) Sets short (aggressive) timeouts for idle connections. Aggressive Aging blocks are documented below.
- `keep_connections_open_after_policy_installation` - (Optional) Keep connections open after policy has been installed even if they are not allowed under the new policy. This overrides the settings in the Connection Persistence page. If you change this property, the change will not affect open connections, but only future connections.
- `match_by_protocol_signature` - (Optional) A value of true enables matching by the selected protocol's signature - the signature identifies the protocol as genuine. Select this option to limit the port to the specified protocol. If the selected protocol does not support matching by signature, this field cannot be set to true.
- `match_for_any` - (Optional) Indicates whether this service is used when 'Any' is set as the rule's service and there are several service objects with the same source port and protocol.
- `override_default_settings` - (Optional) Indicates whether this service is a Data Domain service which has been overridden.
- `port` - (Optional) The number of the port used to provide this service. To specify a port range, place a hyphen between the lowest and highest port numbers, for example 44-55.
- `protocol` - (Optional) Select the protocol type associated with the service, and by implication, the management server (if any) that enforces

Content Security and Authentication for the service. Selecting a Protocol Type invokes the specific protocol handlers for each protocol type, thus enabling higher level of security by parsing the protocol, and higher level of connectivity by tracking dynamic actions (such as opening of ports).

- `session_timeout` - (Optional) Time (in seconds) before the session times out.
- `source_port` - (Optional) Port number for the client side service. If specified, only those Source port Numbers will be Accepted, Dropped, or Rejected during packet inspection. Otherwise, the source port is not inspected.
- `sync_connections_on_cluster` - (Optional)Enables state-synchronized High Availability or Load Sharing on a ClusterXL or OPSEC-certified cluster.
- `use_default_session_timeout` - (Optional) Use default virtual session timeout.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.
- `groups` - (Optional) Collection of group identifiers.
- `tags` - (Optional) Collection of tag identifiers.

`aggressive_aging` supports the following:

- `default_timeout` - (Optional) Default aggressive aging timeout in seconds.
- `enable` - (Optional) N/A
- `timeout` - (Optional) Aggressive aging timeout in seconds.
- `use_default_timeout` - (Optional) N/A.

» checkpoint_management_threat_indicator

This resource allows you to add/update/delete Check Point Threat Indicator.

» Example Usage

```
resource "checkpoint_management_threat_indicator" "example" {
    name = "My_Indicator"
    observables {
      name = "My_Observable"
      mail_to = "someone@somewhere.com"
      confidence = "medium"
```

```
      severity = "low"
      product = "AV"
    }
    action = "ask"
    profile_overrides {
      profile = "My_Profile"
      action = "detect"
    }
    ignore_warnings = true
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Object name. Should be unique in the domain.
- `observables` - (Optional) The indicator's observables. Indicator's observables blocks are documented below.
- `action` - (Optional) The indicator's action.
- `profile_overrides` - (Optional) Profiles in which to override the indicator's default action. Profile Overrides blocks are documented below.
- `ignore_warnings` - (Optional) Apply changes ignoring warnings.
- `ignore_errors` - (Optional) Apply changes ignoring errors. You won't be able to publish such a changes. If ignore-warnings flag was omitted - warnings will also be ignored.
- `color` - (Optional) Color of the object. Should be one of existing colors.
- `comments` - (Optional) Comments string.
- `tags` - (Optional) Collection of tag identifiers.

`observables` supports the following:

- `name` - (Required) Object name. Should be unique in the domain.
- `md5` - (Optional) A valid MD5 sequence.
- `url` - (Optional) A valid URL.
- `ip_address` - (Optional) A valid IP-Address.
- `ip_address_first` - (Optional) A valid IP-Address, the beginning of the range. If you configure this parameter with a value, you must also configure the value of the 'ip-address-last' parameter.
- `ip_address_last` - (Optional) A valid IP-Address, the end of the range. If you configure this parameter with a value, you must also configure the value of the 'ip-address-first' parameter.
- `domain` - (Optional) The name of a domain.
- `mail_to` - (Optional) A valid E-Mail address, recipient filed.
- `mail_from` - (Optional) A valid E-Mail address, sender field.
- `mail_cc` - (Optional) A valid E-Mail address, cc field.
- `mail_reply_to` - (Optional) A valid E-Mail address, reply-to field.

- `mail_subject` - (Optional) Subject of E-Mail.
- `confidence` - (Optional) The confidence level the indicator has that a real threat has been uncovered.
- `product` - (Optional) The software blade that processes the observable: AV - AntiVirus, AB - AntiBot.
- `severity` - (Optional) The severity level of the threat.

`profile_overrides` supports the following:

- `action` - (Optional) The indicator's action in this profile.
- `profile` - (Optional) The profile in which to override the indicator's action.

» checkpoint_management_publish

Publish Changes.

» Example Usage

```
resource "checkpoint_management_publish" "example" { }
```

» Argument Reference

The following arguments are supported:

- `uid` - (Optional) Session unique identifier. Specify it to publish a different session than the one you currently use.

» How To Use

Make sure this command resource will be executed by terraform when you meant it will run.

» checkpoint_management_install_policy

Install the published policy.

» Example Usage

```
resource "checkpoint_management_install_policy" "example" {
  policy_package = "standard"
  targets = ["corporate-gateway"]
}
```

» Argument Reference

The following arguments are supported:

- `policy_package` - (Required) The name of the Policy Package to be installed.
- `targets` - (Required) On what targets to execute this command. Targets may be identified by their name, or object unique identifier.
- `access` - (Optional) Set to be true in order to install the Access Control policy. By default, the value is true if Access Control policy is enabled on the input policy package, otherwise false.
- `desktop_security` - (Optional) Set to be true in order to install the Desktop Security policy. By default, the value is true if desktop security policy is enabled on the input policy package, otherwise false.
- `qos` - (Optional) Set to be true in order to install the QoS policy. By default, the value is true if Quality-of-Service policy is enabled on the input policy package, otherwise false.
- `threat_prevention` - (Optional) Set to be true in order to install the Threat Prevention policy. By default, the value is true if Threat Prevention policy is enabled on the input policy package, otherwise false.
- `install_on_all_cluster_members_or_fail` - (Optional) Relevant for the gateway clusters. If true, the policy is installed on all the cluster members. If the installation on a cluster member fails, don't install on that cluster.
- `prepare_only` - (Optional) If true, prepares the policy for the installation, but doesn't install it on an installation target.
- `revision` - (Optional) The UID of the revision of the policy to install.

» How To Use

Make sure this command will be executed in the right execution order. note: terraform execution is not sequential.

» checkpoint_management_login

Log in to the server with username and password.

» Example Usage

```
resource "checkpoint_management_login" "example" {
  user = "aa"
  password = "aaaa"
}
```

» Argument Reference

The following arguments are supported:

- `user` - (Required) Session unique identifier. Specify it to publish a different session than the one you currently use.
- `password` - (Required) Administrator password.
- `continue_last_session` - (Optional) When 'continue-last-session' is set to 'True', the new session would continue where the last session was stopped. This option is available when the administrator has only one session that can be continued. If there is more than one session, see 'switch-session' API.
- `domain` - (Optional) Use domain to login to specific domain. Domain can be identified by name or UID.
- `enter_last_published_session` - (Optional) Login to the last published session. Such login is done with the Read Only permissions.
- `read_only` - (Optional) Login with Read Only permissions. This parameter is not considered in case continue-last-session is true.
- `session_comments` - (Optional) Session comments.
- `session_description` - (Optional) Session description.
- `session_name` - (Optional) Session unique name.
- `session_timeout` - (Optional) Session expiration timeout in seconds. Default 600 seconds.

» How To Use

Make sure this command will be executed in the right execution order. note: terraform execution is not sequential.

» checkpoint_management_logout

Log out from the current session. After logging out the session id is not valid any more.

» Example Usage

```
resource "checkpoint_management_logout" "example" {}
```

» Argument Reference

There are no arguments in this command.

» How To Use

Make sure this command will be executed in the right execution order. note: terraform execution is not sequential.

» checkpoint_management_run_ips_update

Runs IPS database update. If "package-path" is not provided server will try to get the latest package from the User Center.

» Example Usage

```
resource "checkpoint_management_run_ips_update" "example" {}
```

» Argument Reference

The following arguments are supported:

- `package_path` - (Optional) Offline update package path.

» How To Use

Make sure this command will be executed in the right execution order. note: terraform execution is not sequential.

» checkpoint_hostname

This resource allows you to set the hostname of a Check Point machine.

» Example Usage

```
resource "checkpoint_hostname" "hostname" {
      name = "terrahost"
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) New hostname to change.

» checkpoint_put_file

This resource allows you to add a new file to a Check Point machine.

» Example Usage

```
resource "checkpoint_put_file" "put_file1" {
      file_name = "/path/to/file1/terrafile1.txt"
      text_content = "It's a terrafile!"
      override = true
}

resource "checkpoint_put_file" "put_file1" {
      file_name = "/path/to/file2/terrafile2.txt"
      text_content = "It's a terrafile!"
}
```

» Argument Reference

The following arguments are supported:

- `file_name` - (Required) Filename include the desired path. The file will be created in the user home directory if the full path wasn't provided.
- `text_content` - (Required) Content to add to the new file.
- `override` - (Optional) If the file already exists, indicates whether to overwrite it.

» checkpoint_physical_interface

This resource allows you to set a Physical interface.

» Example Usage

```
resource "checkpoint_physical_interface" "physical_interface1" {
      name = "eth1"
      enabled = "true"
      ipv4_address = "20.30.1.10"
      ipv4_mask_length = 24
}

resource "checkpoint_physical_interface" "physical_interface2" {
      name = "eth2"
      enabled = "true"
      speed = "100M"
      duplex = "full"
}

resource "checkpoint_physical_interface" "physical_interface3" {
      name = "eth3"
      monitor_mode = "true"
      enabled = "true"
      ipv4_address = "1.2.3.4"
      ipv4_mask_length = 24
}
```

» Argument Reference

The following arguments are supported:

- `name` - (Required) Interface name.
- `enabled` - (Optional) Interface state.
- `ipv4_address` - (Optional) IPv4 address to set for the interface.
- `ipv4_mask_length` - (Optional) Interface IPv4 address mask length.
- `ipv6_address` - (Optional) IPv6 address to set for the interface.
- `ipv6_mask_length` - (Optional) Interface IPv6 address mask length.
- `ipv6_autoconfig` - (Optional) Configure IPv6 auto-configuration true/false.
- `mac_addr` - (Optional) Configure hardware address.
- `mtu` - (Optional) Interface Mtu.
- `rx_ringsize` - (Optional) Set receive buffer size for the interface.
- `tx_ringsize` - (Optional) Set transmit buffer size for the interface.

- `monitor_mode` - (Optional) Set monitor mode for the interface true/false.
- `auto_negotiation` - (Optional) Configure auto-negotiation. Activating Auto-Negotiation will skip the speed and duplex configuration.
- `duplex` - (Optional) duplex for the interface. Duplex is not relevant when 'auto_negotiation' is enabled.
- `speed` - (Optional) Interface link speed. Speed is not relevant when 'auto_negotiation' is enabled.
- `comments` - (Optional) interface Comments.