

Samurai

Library version: RENAT 0.1.8g
Library scope: test suite
Named arguments: supported

Introduction

A library provides functions to control Samurai application

The library utilize *Selenium2Library* and adds more functions to control Samurai application easily. Without other further mentions, all of the concepts of `user`, `user group` are Samurai concepts.

By default, RENAT will try to connect to all Samurai nodes defined in active `local.yaml` at the beginning of the test and disconnect from them at the end of the test automatically. Usually user does not need to use `Connect All` and `Close` explicitly.

Currently, this module supposed that Samurai is used in Japanese locale. When Samurai module has error, it tried to make the last snapshot in `result/selenium-screenshot-x.png`. Checking this capture will help to understand the reason of the error.

Some keywords of *Samurai* is using `xpath` to identify elements. See *Selenium2Library* for more details about xpath.

See *WebApp* for common keywords of web applications.

Selenium2Library keywords still could be used together within this library. See *Selenium2Library* for more details.

Shortcuts

Add Policy · **Add Policy Group** · **Add User** · **Capture Screenshot** · **Change Policy View Group** · **Click All Elements** · **Close** · **Close All** · **Connect** · **Connect All** · **Delete Policy** · **Delete Policy Group** · **Delete User** · **Edit Policy** · **Left Menu** · **Login** · **Logout** · **Make Item Map** · **Reset Capture Counter** · **Select Items In Table** · **Set Capture Counter** · **Set Capture Format** · **Show Policy Basic** · **Show Policy Mitigation** · **Show Policy Mo** · **Show Policy Monitor** · **Start Mitigation** · **Stop Mitigation** · **Switch**

Keywords

Keyword	Arguments	Documentation																																																																																																																
Add Policy	**policy	Adds a new Samurai policy																																																																																																																
		<code>policy</code> is a map containing the below information to create the new policy.																																																																																																																
		<table><tr><th>key</th><th>meaning</th><th>mandatory</th><th>sample</th></tr><tr><td>name</td><td>name of the policy</td><td>yes</td><td><code>test001</code></td></tr><tr><td>basic_alias</td><td>alias name of the policy</td><td></td><td><code>test001</code></td></tr><tr><td>basic_port_id</td><td>another alias</td><td></td><td></td></tr><tr><td>basic_facing</td><td>customer or backbone</td><td></td><td><code>customer</code></td></tr><tr><td>basic_intf_list</td><td>list of router and interface pair, separated by comma</td><td>yes</td><td><code>10.128.18.31:xe-0/0/0.1</code></td></tr><tr><td>basic_cidr_list</td><td>list of CIDR separate by comma</td><td></td><td></td></tr><tr><td>basic_option_filter</td><td>optinal filter</td><td></td><td></td></tr><tr><td>basic_direction</td><td>direction of the traffic (incoming or outgoing)</td><td></td><td><code>Incoming</code></td></tr><tr><td>traffic_enabled</td><td>Enable traffic monitoring or not</td><td>yes</td><td><code>\${True}</code> or <code>\${False}</code></td></tr><tr><td>detection_enabled</td><td>Enable detection or not</td><td>yes</td><td><code>\${True}</code> or <code>\${False}</code></td></tr><tr><td>mitigation_zone_name</td><td>Name of the zone for mitigation</td><td></td><td><code>zone001</code></td></tr><tr><td>mitigation_zone_prefix</td><td>Prefixes that could mitigate</td><td></td><td><code>1.1.1.1/32</code></td></tr><tr><td>mitigation_thr_bps</td><td>Upper limit (bps)</td><td></td><td><code>800,000,000</code></td></tr><tr><td>mitigation_thr_pps</td><td>Upper limit (pps)</td><td></td><td><code>54,000,000</code></td></tr><tr><td>mitigation_mo_enabled</td><td>Using Arbor TMS MO or not</td><td>yes</td><td><code>\${True}</code> or <code>\${False}</code></td></tr><tr><td>mitigation_device_list</td><td>Devices used for TMS, separated by comma</td><td></td><td><code>ArborSP-A</code></td></tr><tr><td>mitigation_mo_name</td><td>MO name, separated by comma</td><td></td><td><code>OCN12(ALU)_LOOSE</code></td></tr><tr><td>mitigation_comm_list</td><td>commna separated peer/community list</td><td>yes</td><td><code>1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777</code></td></tr><tr><td>nw_monitor_gre1</td><td>1st GRE address for NW monitor</td><td></td><td><code>210.0.1.1</code></td></tr><tr><td>nw_monitor_gre2</td><td>2nd GRE address for NW monitor</td><td></td><td><code>210.0.1.1</code></td></tr><tr><td>nw_monitor_ce1</td><td>1st CE address for NW monitor</td><td></td><td><code>210.0.1.2</code></td></tr><tr><td>nw_monitor_ce2</td><td>2nd CE address for NW monitor</td><td></td><td><code>210.0.1.2</code></td></tr><tr><td>nw_monitor_pe1</td><td>1st PE for NW monitor (list)</td><td></td><td><code>edge01hige-MX2020-15(118.23.176.244)</code></td></tr><tr><td>nw_monitor_pe2</td><td>2nd PE for NW monitor (list)</td><td></td><td><code>edge01hige-MX2020-15(118.23.176.244)</code></td></tr><tr><td>event_name</td><td>name of the message event to make</td><td></td><td><code>info1</code></td></tr><tr><td>event_addr</td><td>address to send the events</td><td></td><td><code>user@mail.com</code></td></tr><tr><td>view_group</td><td>user group that could view this policy, separated by comma</td><td>yes</td><td><code>SuperGroup,test_group_007</code></td></tr></table>	key	meaning	mandatory	sample	name	name of the policy	yes	<code>test001</code>	basic_alias	alias name of the policy		<code>test001</code>	basic_port_id	another alias			basic_facing	customer or backbone		<code>customer</code>	basic_intf_list	list of router and interface pair, separated by comma	yes	<code>10.128.18.31:xe-0/0/0.1</code>	basic_cidr_list	list of CIDR separate by comma			basic_option_filter	optinal filter			basic_direction	direction of the traffic (incoming or outgoing)		<code>Incoming</code>	traffic_enabled	Enable traffic monitoring or not	yes	<code>\${True}</code> or <code>\${False}</code>	detection_enabled	Enable detection or not	yes	<code>\${True}</code> or <code>\${False}</code>	mitigation_zone_name	Name of the zone for mitigation		<code>zone001</code>	mitigation_zone_prefix	Prefixes that could mitigate		<code>1.1.1.1/32</code>	mitigation_thr_bps	Upper limit (bps)		<code>800,000,000</code>	mitigation_thr_pps	Upper limit (pps)		<code>54,000,000</code>	mitigation_mo_enabled	Using Arbor TMS MO or not	yes	<code>\${True}</code> or <code>\${False}</code>	mitigation_device_list	Devices used for TMS, separated by comma		<code>ArborSP-A</code>	mitigation_mo_name	MO name, separated by comma		<code>OCN12(ALU)_LOOSE</code>	mitigation_comm_list	commna separated peer/community list	yes	<code>1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777</code>	nw_monitor_gre1	1st GRE address for NW monitor		<code>210.0.1.1</code>	nw_monitor_gre2	2nd GRE address for NW monitor		<code>210.0.1.1</code>	nw_monitor_ce1	1st CE address for NW monitor		<code>210.0.1.2</code>	nw_monitor_ce2	2nd CE address for NW monitor		<code>210.0.1.2</code>	nw_monitor_pe1	1st PE for NW monitor (list)		<code>edge01hige-MX2020-15(118.23.176.244)</code>	nw_monitor_pe2	2nd PE for NW monitor (list)		<code>edge01hige-MX2020-15(118.23.176.244)</code>	event_name	name of the message event to make		<code>info1</code>	event_addr	address to send the events		<code>user@mail.com</code>	view_group	user group that could view this policy, separated by comma	yes	<code>SuperGroup,test_group_007</code>
		key	meaning	mandatory	sample																																																																																																													
		name	name of the policy	yes	<code>test001</code>																																																																																																													
		basic_alias	alias name of the policy		<code>test001</code>																																																																																																													
		basic_port_id	another alias																																																																																																															
		basic_facing	customer or backbone		<code>customer</code>																																																																																																													
		basic_intf_list	list of router and interface pair, separated by comma	yes	<code>10.128.18.31:xe-0/0/0.1</code>																																																																																																													
		basic_cidr_list	list of CIDR separate by comma																																																																																																															
		basic_option_filter	optinal filter																																																																																																															
		basic_direction	direction of the traffic (incoming or outgoing)		<code>Incoming</code>																																																																																																													
		traffic_enabled	Enable traffic monitoring or not	yes	<code>\${True}</code> or <code>\${False}</code>																																																																																																													
		detection_enabled	Enable detection or not	yes	<code>\${True}</code> or <code>\${False}</code>																																																																																																													
		mitigation_zone_name	Name of the zone for mitigation		<code>zone001</code>																																																																																																													
		mitigation_zone_prefix	Prefixes that could mitigate		<code>1.1.1.1/32</code>																																																																																																													
		mitigation_thr_bps	Upper limit (bps)		<code>800,000,000</code>																																																																																																													
		mitigation_thr_pps	Upper limit (pps)		<code>54,000,000</code>																																																																																																													
		mitigation_mo_enabled	Using Arbor TMS MO or not	yes	<code>\${True}</code> or <code>\${False}</code>																																																																																																													
		mitigation_device_list	Devices used for TMS, separated by comma		<code>ArborSP-A</code>																																																																																																													
		mitigation_mo_name	MO name, separated by comma		<code>OCN12(ALU)_LOOSE</code>																																																																																																													
		mitigation_comm_list	commna separated peer/community list	yes	<code>1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777</code>																																																																																																													
		nw_monitor_gre1	1st GRE address for NW monitor		<code>210.0.1.1</code>																																																																																																													
		nw_monitor_gre2	2nd GRE address for NW monitor		<code>210.0.1.1</code>																																																																																																													
		nw_monitor_ce1	1st CE address for NW monitor		<code>210.0.1.2</code>																																																																																																													
		nw_monitor_ce2	2nd CE address for NW monitor		<code>210.0.1.2</code>																																																																																																													
		nw_monitor_pe1	1st PE for NW monitor (list)		<code>edge01hige-MX2020-15(118.23.176.244)</code>																																																																																																													
nw_monitor_pe2	2nd PE for NW monitor (list)		<code>edge01hige-MX2020-15(118.23.176.244)</code>																																																																																																															
event_name	name of the message event to make		<code>info1</code>																																																																																																															
event_addr	address to send the events		<code>user@mail.com</code>																																																																																																															
view_group	user group that could view this policy, separated by comma	yes	<code>SuperGroup,test_group_007</code>																																																																																																															
		Example:																																																																																																																
		<table><tr><td>Samurai.<i>Switch</i></td><td>samurai-1</td><td></td></tr><tr><td>Samurai.<i>Add Policy</i></td><td>name=\${POLICY_NAME}</td><td>basic_alias=\${POLICY_NAME}</td></tr><tr><td>...</td><td>basic_facing=customer</td><td>basic_intf_list=10.128.18.31:xe-0/0/0.1</td></tr><tr><td>...</td><td>basic_cidr_list=1.1.1.0/24</td><td>basic_direction=incoming</td></tr><tr><td>...</td><td>traffic_enabled=\${TRUE}</td><td></td></tr><tr><td>...</td><td>detection_enabled=\${TRUE}</td><td></td></tr></table>	Samurai. <i>Switch</i>	samurai-1		Samurai. <i>Add Policy</i>	name=\${POLICY_NAME}	basic_alias=\${POLICY_NAME}	...	basic_facing=customer	basic_intf_list=10.128.18.31:xe-0/0/0.1	...	basic_cidr_list=1.1.1.0/24	basic_direction=incoming	...	traffic_enabled=\${TRUE}		...	detection_enabled=\${TRUE}																																																																																															
Samurai. <i>Switch</i>	samurai-1																																																																																																																	
Samurai. <i>Add Policy</i>	name=\${POLICY_NAME}	basic_alias=\${POLICY_NAME}																																																																																																																
...	basic_facing=customer	basic_intf_list=10.128.18.31:xe-0/0/0.1																																																																																																																
...	basic_cidr_list=1.1.1.0/24	basic_direction=incoming																																																																																																																
...	traffic_enabled=\${TRUE}																																																																																																																	
...	detection_enabled=\${TRUE}																																																																																																																	

		<table><tr><td>...</td><td>mitigation_zone_name=test_zone001</td><td>mitigation_zone_prefix=1.1.1.1/32</td></tr><tr><td>...</td><td>mitigation_device_list=ArborSP-A,ArborSP-B</td><td></td></tr><tr><td>...</td><td>mitigation_mo_enabled=\${TRUE}</td><td></td></tr><tr><td>...</td><td>mitigation_mo_name=N000000012_LOOSE</td><td></td></tr><tr><td>...</td><td>mitigation_comm_list=1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777</td><td></td></tr><tr><td>...</td><td>event_name=test</td><td>event_addr=user@mail.com</td></tr><tr><td>...</td><td>view_group=SuperGroup</td><td></td></tr></table>	...	mitigation_zone_name=test_zone001	mitigation_zone_prefix=1.1.1.1/32	...	mitigation_device_list=ArborSP-A,ArborSP-B		...	mitigation_mo_enabled=\${TRUE}		...	mitigation_mo_name=N000000012_LOOSE		...	mitigation_comm_list=1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777		...	event_name=test	event_addr=user@mail.com	...	view_group=SuperGroup	
...	mitigation_zone_name=test_zone001	mitigation_zone_prefix=1.1.1.1/32																					
...	mitigation_device_list=ArborSP-A,ArborSP-B																						
...	mitigation_mo_enabled=\${TRUE}																						
...	mitigation_mo_name=N000000012_LOOSE																						
...	mitigation_comm_list=1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777																						
...	event_name=test	event_addr=user@mail.com																					
...	view_group=SuperGroup																						
Add Policy Group	group_name, policy_list=*, limit_bps=4000000000, limit_pps=2700000	<p>Add a new policy group</p> <p>group_name is the name of the new group. policy_list is a comma separated of existed policy that should be bound to this policy. An asterisk for this parameter (*) means <i>all of the existed policy</i>. limit_bps and limit_pps are the mitigation capacity threshold of this group.</p>																					
Add User	group, **user_info	<p>Adds user to the current group user_info is a dictionary contains user information that has following keys: name, password, privilege and policy</p> <p>privilege is existed privilege that has been created (e.g: system_admin.</p> <p>policy could be * for all current policies or a list of policy names that are binded to this user.</p> <p>group is the user group. Dot(.) means current group</p> <p>Examples:</p> <table><tr><td>Samurai.Add User</td><td>OCNDDoS</td><td>name=user000</td><td>password=Test12345678</td></tr><tr><td>...</td><td>privilege=system_admin</td><td>policy=*</td><td></td></tr><tr><td>Samurai.Add User</td><td>OCNDDoS</td><td>username=user001</td><td>password=Test12345678</td></tr><tr><td>...</td><td>privilege=system_admin</td><td>policy=OCN11,OCN12</td><td></td></tr></table>	Samurai. Add User	OCNDDoS	name=user000	password=Test12345678	...	privilege=system_admin	policy=*		Samurai. Add User	OCNDDoS	username=user001	password=Test12345678	...	privilege=system_admin	policy=OCN11,OCN12						
Samurai. Add User	OCNDDoS	name=user000	password=Test12345678																				
...	privilege=system_admin	policy=*																					
Samurai. Add User	OCNDDoS	username=user001	password=Test12345678																				
...	privilege=system_admin	policy=OCN11,OCN12																					
Capture Screenshot	filename=None, extra=	<p>Captures the current screen to file</p> <p>Using the internal counter for filename if filename is not specified. In this case, the filename is defined by a pre-set format. Set Capture Format could be used to change the current format.</p> <p>An extra information will be add to the filename if extra is defined</p> <p>Examples:</p> <table><tr><td>Samurai.Capture Screenshot</td><td></td><td># samurai_0000000001.png</td></tr><tr><td>Samurai.Capture Screenshot</td><td>extra=_list</td><td># samurai_0000000002_list.png</td></tr><tr><td>Arbor.Capture Screenshot</td><td></td><td># arbor_0000000001.png</td></tr><tr><td>Arbor.Capture Screenshot</td><td>extra=_xxx</td><td># arbor_0000000001_xxx.png</td></tr><tr><td>Samurai.Capture Screenshot</td><td>file_name=1111.png</td><td># 1111.png</td></tr></table>	Samurai. Capture Screenshot		# samurai_0000000001.png	Samurai. Capture Screenshot	extra=_list	# samurai_0000000002_list.png	Arbor. Capture Screenshot		# arbor_0000000001.png	Arbor. Capture Screenshot	extra=_xxx	# arbor_0000000001_xxx.png	Samurai. Capture Screenshot	file_name=1111.png	# 1111.png						
Samurai. Capture Screenshot		# samurai_0000000001.png																					
Samurai. Capture Screenshot	extra=_list	# samurai_0000000002_list.png																					
Arbor. Capture Screenshot		# arbor_0000000001.png																					
Arbor. Capture Screenshot	extra=_xxx	# arbor_0000000001_xxx.png																					
Samurai. Capture Screenshot	file_name=1111.png	# 1111.png																					
Change Policy View Group	name, *group_name	<p>Changes the groups that could see this policy</p> <p>name is the policy name. group_name is a list of policies</p> <p>Example:</p> <table><tr><td>Samurai.Change Policy View Group</td><td>super_admin</td><td>test_group001</td></tr></table>	Samurai. Change Policy View Group	super_admin	test_group001																		
Samurai. Change Policy View Group	super_admin	test_group001																					
Click All Elements	xpath	<p>Click all element in current page defined by xpath</p> <p>Returns the number of elements that have been clicked</p>																					
Close		Closes the current active browser																					
Close All		Closes all current opened applications																					
Connect	app, name	<p>Opens a web browser and connects to application and assigns a name.</p> <p>If not defined in local.yaml those following key will have default values:</p> <table><tr><td>browser</td><td>firefox</td><td>optional</td></tr><tr><td>login_url</td><td>/</td><td>optiona</td></tr><tr><td>proxy:</td><td></td><td>optional</td></tr><tr><td>http: 10.128.8.210:8080</td><td>optional</td><td></td></tr><tr><td>ssl: 10.128.8.210:8080</td><td>optional</td><td></td></tr><tr><td>socks: 10.128.8.210:8080</td><td>optional</td><td></td></tr><tr><td>profile_dir</td><td>./config/samurai.profile</td><td>optional</td></tr></table>	browser	firefox	optional	login_url	/	optiona	proxy:		optional	http: 10.128.8.210:8080	optional		ssl: 10.128.8.210:8080	optional		socks: 10.128.8.210:8080	optional		profile_dir	./config/samurai.profile	optional
browser	firefox	optional																					
login_url	/	optiona																					
proxy:		optional																					
http: 10.128.8.210:8080	optional																						
ssl: 10.128.8.210:8080	optional																						
socks: 10.128.8.210:8080	optional																						
profile_dir	./config/samurai.profile	optional																					
Connect All		<p>Connects to all applications defined in local.yaml</p> <p>The name of the connection will be the same of the webapp name</p>																					
Delete Policy	*policy_names	<p>Deletes poilcies by their names</p> <p>Returned the number of deleted users</p> <p>Notes: If the policy does not exists, the system will not report any error.</p> <p>Examples:</p> <table><tr><td>Samurai.Delete Policy</td><td>test001</td><td>test002</td></tr></table>	Samurai. Delete Policy	test001	test002																		
Samurai. Delete Policy	test001	test002																					
Delete Policy Group	*group_list	<p>Deletes policy groups</p> <p>Returns the number of deleted policy groups Example:</p> <table><tr><td>Samurai.Delete Policy Group</td><td>test_group001</td><td>test_group002</td></tr></table>	Samurai. Delete Policy Group	test_group001	test_group002																		
Samurai. Delete Policy Group	test_group001	test_group002																					
Delete User	group, *user_list	<p>Deletes user from the user group</p> <p>group is the user group. And . means current group Returns the number of deleted users</p> <p>Examples:</p> <table><tr><td>Samurai.Delete User</td><td>SuperGroup</td><td>user001</td><td>user002</td></tr><tr><td>Samurai.Delete User</td><td>.</td><td>user002</td><td></td></tr></table>	Samurai. Delete User	SuperGroup	user001	user002	Samurai. Delete User	.	user002														
Samurai. Delete User	SuperGroup	user001	user002																				
Samurai. Delete User	.	user002																					

Edit Policy	<i>**policy</i>	Edits a Samurai policy policy contains information about the policy. See Add Policy for more details about policy format							
Left Menu	<i>menu</i>	Chooses the left panel menu by its displayed name Return a list of 1st meaningful column Example: <table><tr><td>Samurai.Left Menu</td><td>Traffic</td></tr><tr><td>Samurai.Left Menu</td><td>Detection</td></tr><tr><td>Samurai.Left Menu</td><td>ポリシー管理</td></tr></table>	Samurai. Left Menu	Traffic	Samurai. Left Menu	Detection	Samurai. Left Menu	ポリシー管理	
Samurai. Left Menu	Traffic								
Samurai. Left Menu	Detection								
Samurai. Left Menu	ポリシー管理								
Login		Logs-in into the application User and password is set by the template and authentication methods in the master files							
Logout		Logs-out the current application, the browser remains							
Make Item Map	<i>xpath</i>	Makes a item/webelement defined <i>xpath</i> The map is a dictionary from <i>item</i> to the <i>WebElement</i> Items name found by <i>xpath</i> are used as keys							
Reset Capture Counter		Resets the counter of the screen capture							
Select Items In Table	<i>xpath, xpath2, *item_list</i>	Checks items in Samurai table by <i>xpath</i> <i>xpath</i> points to the column that used as key and <i>xpath2</i> is the relative <i>xpath</i> contains the checkbox column. <i>item_list</i> is a list of item that need to check. Item in the list could be a regular expression with the format <code>reg=<regular expression</code> . The keyword is called with assuming that the table is already visible. Returns the tuple of all items and selected items Note: Non-width-space (\u200b) will be take care by the keyword. Note: if the first <i>item_list</i> is * then the keyword will try to click a link named <code>すべてを選択</code> .							
Set Capture Counter	<i>value=0</i>	Sets the counter of the screen capture to <i>value</i>							
Set Capture Format	<i>format</i>	Sets the format for the screen capture file The format does not include the default prefix <code>.png</code> The default format is <code><mod>_%010d</code> . <i>mod</i> could be <code>samurai</code> or <code>arbor</code> See https://docs.python.org/2/library/string.html#format-specification-mini-language for more details about the format string. Examples: <table><tr><td>Samurai.Set Capture Format</td><td><code>\${case}_%010d</code></td><td># <code>\${case}</code> is a predefined variable</td></tr></table>	Samurai. Set Capture Format	<code>\${case}_%010d</code>	# <code>\${case}</code> is a predefined variable				
Samurai. Set Capture Format	<code>\${case}_%010d</code>	# <code>\${case}</code> is a predefined variable							
Show Policy Basic	<i>policy_name</i>	Makes the virtual browser show basic setting of the policy <i>name</i> . A following Samurai. Capture Screenshot is necessary to capture the result.							
Show Policy Mitigation	<i>policy_name</i>	Make the virtual browser show the mitigation setting of a policy A following Samurai. Capture Screenshot is necessary to capture the result.							
Show Policy Mo	<i>policy_name</i>	Make the virtual browser show the MO setting of a policy Automatically expand the MO section of other devices if necessary. A following Samurai. Capture Screenshot is necessary to capture the result.							
Show Policy Monitor	<i>policy_name</i>	Make a virtual browser show the mitigation setting of a policy A following Samurai. Capture Screenshot is necessary to capture the result.							
Start Mitigation	<i>policy, prefix, comment=mitigation started by RENAT, device=None, force=False</i>	Starts a mitigation with specific <i>prefix</i> <i>device</i> is used for matching real device name configured by Samurai If <i>force</i> is <code>TRUE</code> then the keyword will fail if selected device does not contain <i>device</i> Returns mitigation <i>id</i> and selected <i>arbor device</i> Example: <table><tr><td><code>\${id}</code></td><td><code>\${device}=</code></td><td>Samurai.Start Mitigation</td><td><code>211.1.12.1/32</code></td><td>mitigation by RENAT</td><td>SP-A</td><td><code>\${TRUE}</code></td></tr></table>	<code>\${id}</code>	<code>\${device}=</code>	Samurai. Start Mitigation	<code>211.1.12.1/32</code>	mitigation by RENAT	SP-A	<code>\${TRUE}</code>
<code>\${id}</code>	<code>\${device}=</code>	Samurai. Start Mitigation	<code>211.1.12.1/32</code>	mitigation by RENAT	SP-A	<code>\${TRUE}</code>			
Stop Mitigation	<i>id</i>	Stops a mitigation by its ID Example: <table><tr><td>Samurai.Stop Mitigation</td><td><code>700</code></td></tr></table>	Samurai. Stop Mitigation	<code>700</code>					
Samurai. Stop Mitigation	<code>700</code>								
Switch	<i>name</i>	Switches the current browser to <i>name</i>							

