

Samurai

Library version: RENAT 0.1.13
Library scope: test suite
Named arguments: supported

Introduction

A library provides functions to control Samurai application

The library utilize *SeleniumLibrary* and adds more functions to control Samurai application easily. Without other furthur mentions, all of the concepts of `user`, `user group` are Samurai concepts. By default, RENAT will try to connec 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.

Currently the module support Samurai 09/14/16

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 and how to configure the `local.yaml` file.

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** · **Close Window** · **Connect** · **Connect All** · **Delete Policy** · **Delete Policy Group** · **Delete User** · **Edit Mitigation Controller** · **Edit Policy** · **Get Mitigation List** · **Get Verbose** · **Left Menu** · **Login** · **Logout** · **Make Item Map** · **Mark Element** · **Open Ff With Profile** · **Reconnect** · **Reset Capture Counter** · **Select Items In Table** · **Select Window** · **Set Ajax Wait** · **Set Capture Counter** · **Set Capture Format** · **Set Verbose** · **Show Detail Mitigation** · **Show Policy Basic** · **Show Policy Detection** · **Show Policy Display** · **Show Policy Mitigation** · **Show Policy Mo** · **Show Policy Monitor** · **Show Policy Notify** · **Show Policy Nw Monitor** · **Show Policy Traffic** · **Start Mitigation** · **Stop Mitigation** · **Switch** · **Update Mitigation Controller Info** · **Verbose Capture** · **Wait Until Element Changes**

Keywords

Keyword	Arguments	Documentation				
Add Policy	**policy	Adds a new Samurai policy				
		policy is a map containing the below information to create the new policy.				
		key	meaning	mandatory	sample	
		name	name of the policy	yes	test001	
		basic_alias	alias name of the policy		test001	
		basic_port_id	another alias			
		basic_facing	customer or backbone		customer	
		basic_intf_list	list of router and interface pair, separated by comma	yes	10.128.18.31:xe-0/0/0.1	
		basic_cidr_list	list of CIDR separate by comma			
		basic_option_filter	optinal filter			
		basic_direction	direction of the traffic (incoming or outgoing)		incoming	
		traffic_enabled	Enable traffic monitoring or not	yes	\${TRUE} or \${FALSE}	
		detection_enabled	Enable detection or not	yes	\${TRUE} or \${FALSE}	
		detection_direction	change detect direction fo all attack type	incomming,outgoing,'both both:check		
		mitigation_enabled	Enable Mitigation or not	yes	\${TRUE} or \${FALSE}	
		mitigation_zone_name	Name of the zone for mitigation		zone001	
		mitigation_zone_prefix	Prefixes that could mitigate		1.1.1.1/32	
		mitigation_thr_bps	Upper limit (bps)		800,000,000	
		mitigation_thr_pps	Upper limit (pps)		54,000,000	
		mitigation_auto_enabled	Enable automitigation or not		\${TRUE} or \${FALSE}	
		mitigation_auto_level	Automitigation level		0:overLow 1:overMedium 2:High	
		mitigation_auto_time	Automitigation detect attack time (min)		default is 15	
		mitigation_mo_enabled	Using Arbor TMS MO or not	yes	\${TRUE} or \${FALSE}	
		mitigation_auto_stop_enabled	Enable		\${TRUE} or \${FALSE}	

		mitigation_auto_stop_enabled	enable automitigation stop or not		$\$(TRUE) \text{ or } \$(FALSE)$
		mitigation_auto_stop_level	Automitigation level		0:overLow 2:High
		mitigation_auto_stop_time	Automitigation stop detect attack time (min)		default is 15
		mitigation_device_list	Devices used for TMS, separated by comma		ArborSP-A
		mitigation_mo_name	MO name, separated by comma		OCN12(ALU)_LOOSE
		mitigation_comm_list	commna separated peer/community list		1.10(180.0.1.10)/2914:666,1.11(180.0.1.11)/2914:777
		nw_monitor_gre1	1st GRE address for NW monitor		210.0.1.1
		nw_monitor_gre2	2nd GRE address for NW monitor		210.0.1.1
		nw_monitor_ce1	1st CE address for NW monitor		210.0.1.2
		nw_monitor_ce2	2nd CE address for NW monitor		210.0.1.2
		nw_monitor_pe1	1st PE for NW monitor (list)		edge01hige-MX2020-15(118.23.176.244)
		nw_monitor_pe2	2nd PE for NW monitor (list)		edge01hige-MX2020-15(118.23.176.244)
		event_name	name of the message event to make		info1
		event_addr	address to send the events		user@mail.com
		view_group	user group that could view this policy, separated by comma	yes	SuperGroup,test_group_007

Example:

Samurai. Switch	samurai-1	
Samurai. Add Policy	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}	
...	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	Add a new policy group 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 all of the existed policy. limit_bps and limit_pps are the mitigation capacity threshold of this group.																
Add User	group, **user_info	Adds user to the current group user_info is a dictionary contains user information that has following keys: name, password, privilege and policy privilege is existed privilege that has been created (e.g: system_admin. policy could be * for all current policies or a list of policy names that are binded to this user. group is the user group. Dot(.) means current group Examples: <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=	Captures the current screen to file 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. An extra information will be add to the filename if extra is defined Examples: <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></td><td># arbor_0000000001</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		# arbor_0000000001				
Samurai.Capture Screenshot		# samurai_0000000001.png																
Samurai.Capture Screenshot	extra=_list	# samurai_0000000002_list.png																
Arbor.Capture Screenshot		# arbor_0000000001.png																
Arbor.Capture Screenshot		# arbor_0000000001																

		<div>Samurai.Capture Screenshot filename=1111.png # 1111.png</div>																		
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> <div>Samurai.Change Policy View Group super_admin test_group001</div>																		
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		Close the web application																		
Close All		Closes all current opened applications																		
Close Window		Closes the current window																		
Connect	app, name	<p>Opens a web browser and connects to application and assigns a name .</p> <ul style="list-style-type: none">app is the name of the application (e.ge. samurai-1)name is the name of the browser <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></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	
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																			
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> <div>Samurai.Delete Policy test001 test002</div>																		
Delete Policy Group	*group_list	<p>Deletes policy groups</p> <p>See Select Items In Table for more detail about how to choose group_list</p> <p>Returns the number of deleted policy groups Example:</p> <div>Samurai.Delete Policy Group test_group001 test_group002</div>																		
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 Mitigation Controller	controller, **config	<p>Change the setting of the mitigation control</p> <ul style="list-style-type: none">control: name of the mitigation controllerconfig: configuration need to be changed. Currently only tms_group is configurable with the following format: groupname1:action1,groupname2:action2. groupname is currently set TMS group name and action could be click,check or uncheck. <p>Example:</p> <div>Samurai.Edit Mitigation Controller controller=vSP-A tms_group=Logical0_SOCN_IPv4:uncheck</div>																		
Edit Policy	**policy	<p>Edits a Samurai policy</p> <p>policy contains information about the policy. See Add Policy for more details about policy format</p>																		
Get Mitigation List	status=実行中	<p>Gets current mitigation list</p> <p>Return current active mitgation name, ID and the number of them</p> <p>Example:</p> <div>\$(MITI) \$(IDS) \$(NUM)= Samurai.Get Mitigation List</div>																		
Get Verbose		Get current verbose mode																		
Left Menu	menu, locator=None, ignore_first_element=True	<p>Chooses the left panel menu by its displayed name</p> <p>When locator is not null, the keyword will return a list of text attribute of all elements specified by the locator. locator could be a xpath or a predefined string.</p> <p>locator predefined strings are: MITIGATE_REALTIME, MITIGATE_LIST, DETECT_LIST</p> <p>For example, a xpath //div[@id='infoareain2']/*//td[1]/a means the list of link of all elements in a 1st column of a table insides a div with id infoareain2.</p> <p>Examples:</p> <table><tr><td>Samurai.Left Menu</td><td>Traffic</td><td></td><td></td></tr><tr><td>Samurai.Left Menu</td><td>Detection</td><td></td><td></td></tr><tr><td>Samurai.Left Menu</td><td>ポリシー管理</td><td></td><td></td></tr><tr><td>@{LIST}=</td><td>Samurai.Left Menu</td><td>Active Mitigation</td><td>//div[@id='infoareain2']/*//td[1]/a</td></tr></table>	Samurai. Left Menu	Traffic			Samurai. Left Menu	Detection			Samurai. Left Menu	ポリシー管理			@{LIST}=	Samurai. Left Menu	Active Mitigation	//div[@id='infoareain2']/*//td[1]/a		
Samurai. Left Menu	Traffic																			
Samurai. Left Menu	Detection																			
Samurai. Left Menu	ポリシー管理																			
@{LIST}=	Samurai. Left Menu	Active Mitigation	//div[@id='infoareain2']/*//td[1]/a																	
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
Mark Element	<i>xpath</i>	Marking an element to check its status later
Open Ff With Profile	<i>app, name</i>	
Reconnect		Reconnects to the server
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 target column. <i>item_list</i> is a list of item and its action that need to check. Item in the list could be a regular expression with the format <i>re: <regular expression> action</i> . The default action for the item could be <i>click`'(default)`,check</i> or <i>uncheck</i> 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 <i>*</i> then the keyword will try to click a link named <i>すべてを選択</i> .
Select Window	<i>title</i>	Selects a window by its title
Set Ajax Wait	<i>wait_time=2s</i>	Set the ajax wait time
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 <i>.png</i> The default format is <i><mod>_%010d</i> . <i>mod</i> could be <i>samurai</i> or <i>arbor</i> See https://docs.python.org/2/library/string.html#format-specification-mini-language for more details about the format string. Examples: <div>Samurai.<i>Set Capture Format</i> \${case}_%010d # \${case} is a predefined variable</div>
Set Verbose	<i>verbose=False</i>	Set current verbose mode to <i>verbose</i>
Show Detail Mitigation	<i>id</i>	Shows detail information of a mitigation
Show Policy Basic	<i>policy_name</i>	Makes the virtual browser show basic setting of the policy <i>name</i> . A following Samurai. <i>Capture Screenshot</i> is necessary to capture the result.
Show Policy Detection	<i>policy_name</i>	Shows the detection pannel of <i>policy_name</i> policy
Show Policy Display	<i>policy_name</i>	Make a virtual browser show the display setting of a policy Notes: Depending on the setting of the policy, MO panel may not be existed. In this case, if <i>strict</i> is <i>True</i> , then the keyword will fail.
Show Policy Mitigation	<i>policy_name</i>	Make the virtual browser show the mitigation setting of a policy
Show Policy Mo	<i>policy_name, strict=False</i>	Make the virtual browser show the MO setting of a policy Automatically expand the MO section of other devices. Notes: Depending on the setting of the policy, MO panel may not be existed. In this case, if <i>strict</i> is <i>True</i> , then the keyword will fail.
Show Policy Monitor	<i>policy_name</i>	
Show Policy Notify	<i>policy_name</i>	Make a virtual browser show the mitigation setting of a policy
Show Policy Nw Monitor	<i>policy_name, strict=False</i>	Make a virtual browser show the NW monitor setting of a policy Notes: Depending on the setting of the policy, MO panel may not be existed. In this case, if <i>strict</i> is <i>True</i> , then the keyword will fail.
Show Policy Traffic	<i>policy_name</i>	Makes the virtual browser show the traffic setting of the policy <i>name</i> . A following Samurai. <i>Capture Screenshot</i> 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 <i>TRUE</i> then the keyword will fail if selected device does not contain <i>device</i> Returns mitigation <i>id</i> and selected <i>arbor</i> device Example: <div>\${id} \${device}= Samurai.<i>Start Mitigation</i> 211.1.12.1/32 mitigation by RENAT SP-A \${TRUE}</div>
Stop Mitigation	<i>id, raise_error=True</i>	Stops a mitigation by its ID The keyword will raise an error if <i>raise_error</i> is <i>True</i> . Otherwise it will ignore any errors. Example: <div>Samurai.<i>Stop Mitigation</i> 700</div>
Switch	<i>name</i>	Switches the current browser to <i>name</i>
Update	<i>controller wait=10s</i>	Updates information of <i>controller</i>

Update Mitigation Controller Info	<i>controller, wait=10s</i>	Updates information of controller
Verbose Capture	<i>*args, **kwargs</i>	Capture screenshot if verbose mode is <code>True</code> otherwise do nothing
Wait Until Element Changes	<i>interval=5s, timeout=180s, error_on_timeout=False</i>	Wait until the marked element has been changed

Altogether 48 keywords.

Generated by [Libdoc](#) on 2019-02-23 16:37:04.

