





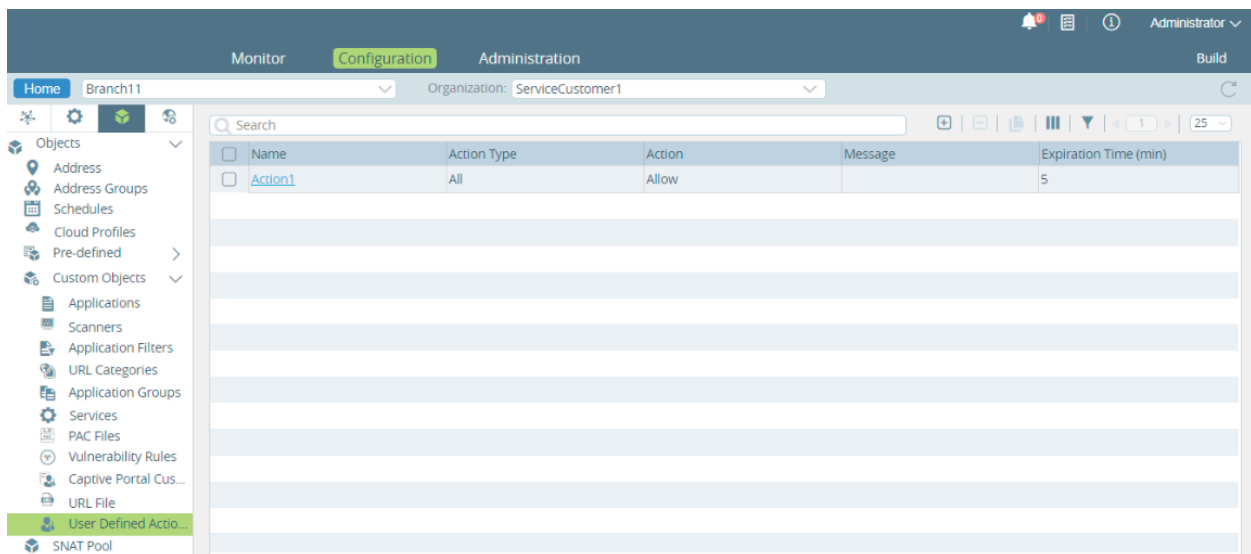
Configure User-Defined Actions

 For supported software information, click [here](#).

For URL filtering, you can select a user-defined action as the action to take when a filter matches.

To configure user-defined actions:

1. In Director view:
 - a. Select the Configuration tab in the top menu bar.
 - b. Select Templates > Device Templates in the horizontal menu bar.
 - c. Select an organization in the left menu bar.
 - d. Select a template in the main pane. The view changes to Appliance view.
2. Select the Configuration tab in the top menu bar.
3. Select Objects & Connectors  > Objects  > Custom Objects  > User-Defined Actions  in the left menu bar. The User-Defined Actions dashboard displays.



4. Click the  Add icon to add an action. In the Add Action popup window, enter information for the following fields.

Add Action

Name*

Description

Tags

Action Type*

IPREP

Action*

sink-hole

Expiration Time (min)

Override PIN

Redirection URL

☐ decrypt-bypass

☐ Log

Message

sink-hole Params

Domain Name

TTL

IP Addresses

☐ IP Addresses


OK

Cancel

Field	Description
Name	Enter a name for the action.
Description	Enter a text description for the action.
Tags	Enter a keyword or phrase that allows you to filter the action. This is useful when you have many action and want to view those that are tagged with a particular keyword.
Action Type	<p>Select the type of action to which to apply the action when the page is redirected. The action type options represent the module for which the user-defined action was configured. For example, if you select URLF, the action can be used only in URL filtering profiles.</p> <ul style="list-style-type: none"> ◦ All—Apply to all action types. ◦ CASB—(For Releases 22.1.3 and later.) Apply to CASB profiles. ◦ Decrypt—Apply for decryption. ◦ DNS—Apply for DNS traffic. ◦ IPS—Apply for intrusion detection and prevention profiles. ◦ IPREP—Apply for IP reputation profiles. ◦ URLF—Apply for URL filtering profiles.
Action	<p>Select the action to take when the user is redirected to a captive portal. Note that not all actions are available for all action types.</p> <ul style="list-style-type: none"> ◦ Allow—Allow the URL without generating an entry in the log. ◦ Ask—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation by clicking OK (for HTTP and HTTPS). ◦ Block—Block the URL and generate an entry in the URL filtering log. No response page is displayed, and the user cannot continue with the website. ◦ Custom Redirection—The browser redirects the user to the URL configured in the Redirection URL field. Session information such as the URL

	<p>requested by the user, the IP address of the HTTP/HTTPS request, and the URL filtering profile to process are included in the redirected URL to the web server that hosts the redirected URL page. After the redirection occurs, the external web server, not the VOS device, handles the captive portal functionality. You can customize the session information parameters that are passed to the web server.</p> <ul style="list-style-type: none"> ◦ Drop Packet—The browser waits for a response from the server and then drops the packets. It is not possible to determine whether the packet was dropped because of a delayed response from the server or because a firewall blocked access to the website. ◦ Drop Session—The browser waits for a response from the server and drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website. ◦ Inform—The browser presents an information page that prompts the user to continue after clicking OK (for HTTP and HTTPS). ◦ Justify—The browser presents an information page that allows the user to either cancel the operation by clicking Cancel or continue with the operation after entering a justification message and clicking OK (for HTTP and HTTPS). ◦ Override—The browser prompts the user to enter a PIN (4 to 6 digits). This action generates an entry in the URL filtering log. ◦ Reset Client—The host responds by sending a TCP Reset packet to the client, and the browser displays an error message indicating that the connection has been reset. It is not possible to determine whether the web server reset the connection or the firewall reset the session. ◦ Reset Client and Server—The host responds by sending a TCP Reset packet back to the client and server. The browser displays an error message indicating that the connection was reset. It is not possible to determine whether the web server reset the connection or the firewall reset the session. ◦ Reset Server—The host responds by sending a TCP Reset packet to the server. The browser waits for a response from the server and then
--	---

	<p>drops the session. It is not possible to determine whether the session was dropped because of a delayed response from the server or because a firewall blocked access to the website.</p> <ul style="list-style-type: none"> ◦ Sinkhole—(For Releases 22.1.3 and later.) Return a false IP address to the URL, thus blocking a DNS sinkhole. A DNS sinkhole spoofs DNS servers to prevent the resolution of the hostnames associated with URLs. This action can help you identify infected hosts in a network if a firewall is unable to find the original source IP address of DNS request sender. Sinkhole malware DNS queries create responses to the client host queries directed at malicious domains and try to connect to a sinkhole IP address instead of connecting to malicious domains. You can check the traffic logs to identify infected hosts. You can apply the sinkhole to the following action types: <ul style="list-style-type: none"> ▪ All ▪ DNS ▪ IPREP ▪ URLF
Log	Click to log captive portal actions. If you do not enable logging, the custom message that you enter in the Message field is not displayed in the log displayed in Versa Analytics.
Expiration Time	<p>Enter how often to redirect a user to the URL, in minutes. When a user first enters a URL and is redirected to a captive portal page, the VOS device creates a cache entry, which expires after a global expiration time. While the cache entry is active, the device does not enforce the captive portal action, and users can view the webpage at the initial URL and at all URLs that belong to the same URL category, without seeing the captive portal page, with one exception. If the action is Block, all URLs are redirected to the Block page, regardless of the expiration time</p> <p><i>Range:</i> 1 through 65535 minutes</p> <p><i>Default:</i> 1 minute</p>

Override PIN	For the Override action, enter the PIN value, which is a 4-, 5-, or 6-digit number
Redirection URL	For the Custom Redirection action, enter the URL to which to redirect the user.
Decrypt Bypass	Click to disable SSL encryption for matching traffic, to allow you to define websites that are not subject to decryption.
Message	Enter a message to display on the captive portal page.
Sinkhole Parameters (Group of Fields)	(For Releases 22.1.3 and later.)
◦ Domain Name	Enter the domain name in which the LDAP server resides.
◦ IP Address	Click the  Add icon to enter one or more IP addresses.
◦ TTL	Enter the time-to-live (TTL) value, in seconds. <i>Range:</i> 1 through 65535 seconds <i>Default:</i> 30 seconds

4. Click OK.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 22.1.3 supports the sinkhole action and the CASB action type.

Additional Information

[Configure Persistent Actions](#)

[Configure URL Filtering](#)