# Configure Persistent Actions

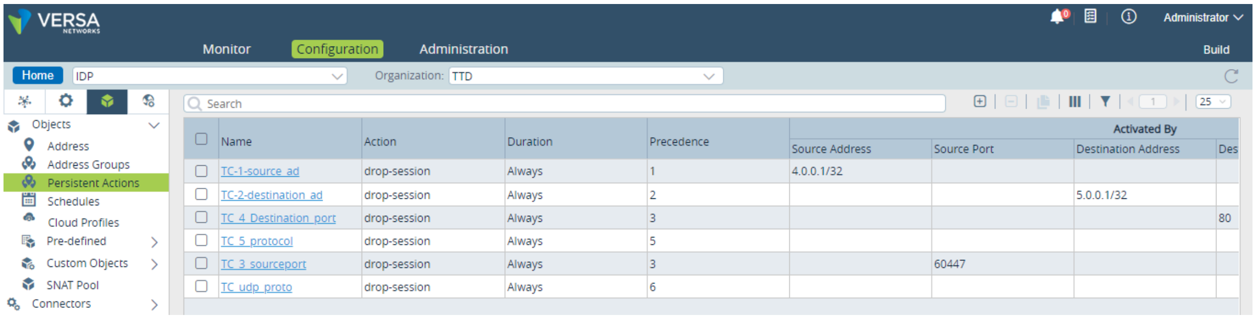
*For supported software information, click here.*

Persistent actions are actions that apply to both current and future sessions. There are two types of persistent actions:

- Activate by security module—You can configure any combination of source IP address, source port number, destination IP address, destination port number, and protocol, and then refer that persistent action object in the IPS profile. If the persistent action associated with the IPS profile is not activated, that persistent action applies only to the current session. To have the action be considered for future session, you must activate the persistent action. One dynamic instance is generated by using the five tuple extracted from current session. If any future session matches this instance, the configured action is taken. If one dynamic entry is generated, a unique integer identifier is created and attached to the entry. You can later activate or deactivate actions by using this identifier.
- Activate by request command—You can configure the actual value of the source IP address, source port, destination IP address, destination port, and protocol. You must then activate persistent action after you compete the configuration. If any future session matches this instance, the configured action is taken

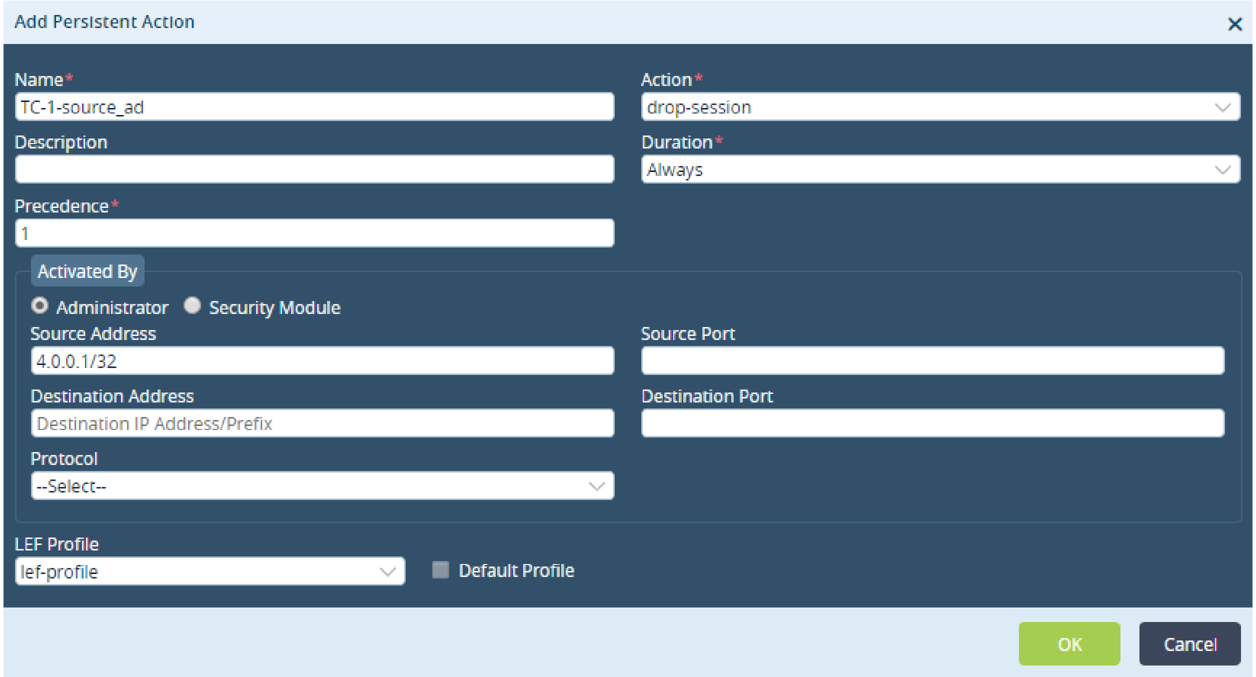
To configure persistent actions:

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 > Persistent Actions in the left menu bar. The main pane displays the persistent actions that are already configured.



| □ | Name | Action | Duration | Precedence | Activated By | | | |
|---|---|---|---|---|---|---|---|---|
| | | | | | Source Address | Source Port | Destination Address | Des |
| □ | TC-1-source ad | drop-session | Always | 1 | 4.0.0.1/32 | | | |
| □ | TC-2-destination ad | drop-session | Always | 2 | | | 5.0.0.1/32 | |
| □ | TC 4 Destination port | drop-session | Always | 3 | | | | 80 |
| □ | TC 5 protocol | drop-session | Always | 5 | | | | |
| □ | TC 3 sourceport | drop-session | Always | 3 | | 60447 | | |
| □ | TC udp proto | drop-session | Always | 6 | | | | |

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



Add Persistent Action ✕

Name*: TC-1-source_ad

Action*: drop-session

Description:

Duration*: Always

Precedence*: 1

Activated By

● Administrator ○ Security Module

Source Address: 4.0.0.1/32

Source Port:

Destination Address: Destination IP Address/Prefix

Destination Port:

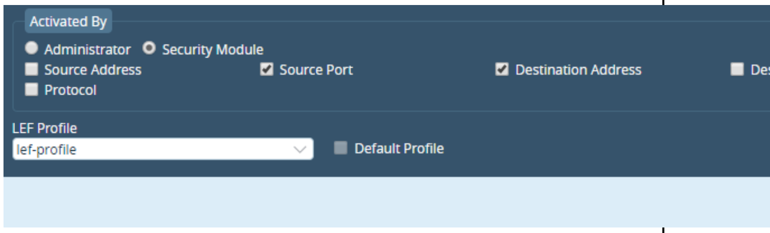
Protocol: --Select--

LEF Profile: lef-profile

□ Default Profile

| Field | Description |
|---|---|
| Name | Enter a name for the persistent action. |
| Description | Enter a text description for the persistent action. |
| Action | Select the action to perform for sessions that match the security profile associated with the persistent action:<br>◦ Allow—Allow the session without generating an entry in the log.<br>◦ 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).<br>◦ Block—Block the session and generate an entry in the log. No response page is displayed, and the user cannot continue with the session.<br>◦ Custom Redirection—The browser redirects the user to the configured URL. Session information such as the URL 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.<br>◦ 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.<br>◦ 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.<br>◦ 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.<br>◦ Inform—The browser presents an information page that prompts the user to continue after clicking OK (for HTTP and HTTPS).<br>◦ 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).<br>◦ Override—The browser prompts the user to enter a PIN (4 to 6 digits). This action generates an entry in the URL filtering log.<br>◦ 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.<br>◦ 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.<br>◦ 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 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. |
| Duration | Select the duration for the persistent action:<br>◦ Always<br>◦ Minute—If you select this option, enter a value. |
| Precedence | Enter a precedence value.<br>*Range:* 0 through 255 |

| | |
|---|---|
| | *Default:* None |
| Activated By | Select the user who is noted as having activated the persistent action:<br>- Administrator<br>- Security Module |
| Activated By Administrator | If you select Activated By Administrator, enter information for the following fields. |
| - Source Address | Enter the source IP address to associate with the persistent action. |
| - Source Port | Enter the source port number to associate with the persistent action. |
| - Destination Address | Enter the destination IP address to associate with the persistent action. |
| - Destination Port | Enter the destination port number to associate with the persistent action. |
| - Protocol | Select the protocol to associate with the persistent action:<br>- TCP<br>- UDP |
| - LEF Profile | Select the LEF profile to associate with the persistent action. |
| - Default Profile | Click to mark this as the default profile. |
| Activated By Security Module | If you select Activated By Security Module, enter information for the following fields.<br><br>Activated By<br>○ Administrator ● Security Module<br>□ Source Address ☑ Source Port ☑ Destination Address □ Des<br>□ Protocol<br>LEF Profile<br>lef-profile<br>□ Default Profile |

| | |
|---|---|
| ◦ Source Address | Click to associate the source IP address with the persistent action. |
| ◦ Source Port | Click to associate the source port number with the persistent action. |
| ◦ Destination Address | Click to associate the destination IP address with the persistent action. |
| ◦ Destination Port | Click to associate the destination port number with the persistent action. |
| ◦ Protocol | Click to associate the protocol to associate with the persistent action |
| ◦ LEF Profile | Select the LEF profile to associate with the persistent action. |
| ◦ Default Profile | Click to mark this as the default profile. |

4. Click OK.

## Supported Software Information

Releases 20.2 and later support all content described in this article.

## Additional Information

Configure User-Defined Actions