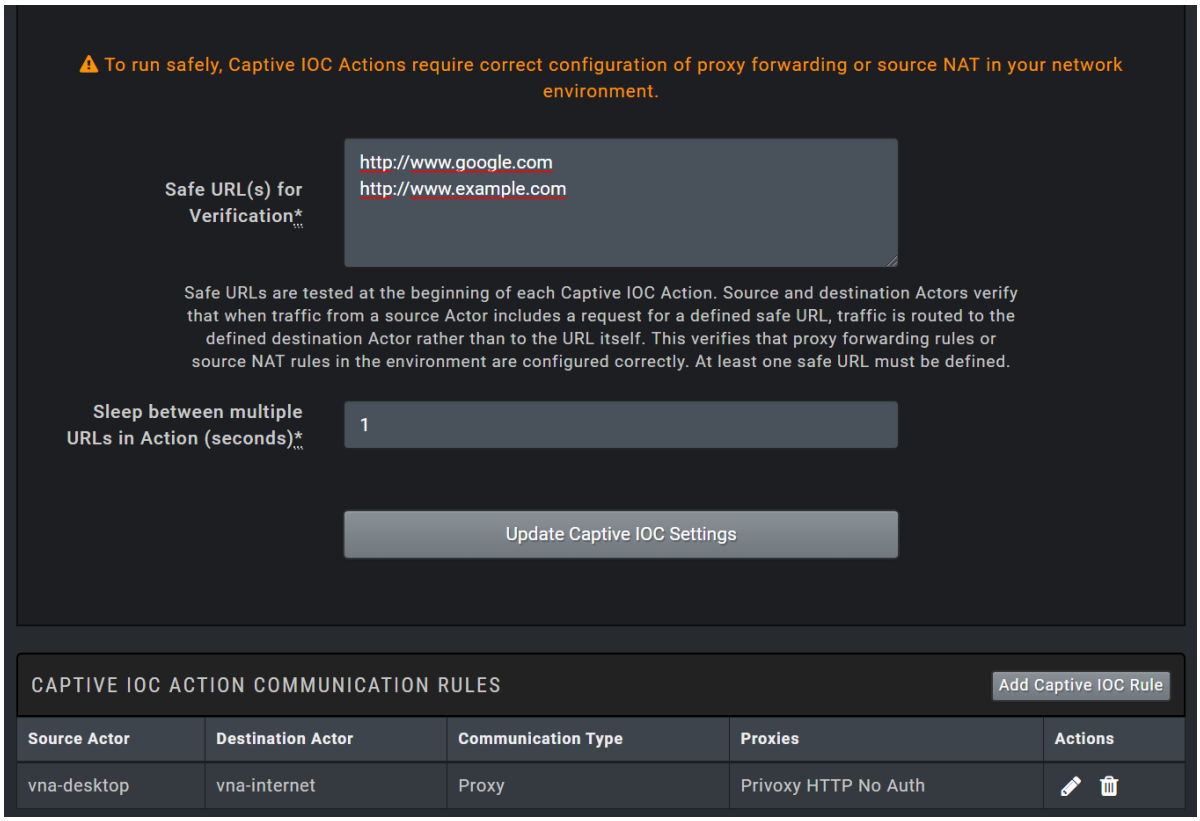
CAPTIVE IOC ACTIONS SETTINGS

One of the features included with the TAAM license is the ability to Run Captive IOC (Indicators of Compromise) Actions. These Actions allow for the safe evaluation of defensive performance related to blocking communication with publicly routable destination addresses for a Threat Actor.

You can create URL-based and PCAP-based Actions, as well as run any PCAP Action that includes HTTP traffic as a Captive IOC Action. Before running these Actions, you must first configure the Captive IOC Action Settings and enable Actors to run them.

To run Captive IOC Actions, you must first configure safe URLs and communications rules. This is completed on the Captive IOC Actions settings page

Your license must include the Threat Actor Assurance Module to use Captive IOC Actions.



Captive IOC Settings page

To configure safe URLs for Captive IOC Actions

Before you can run Captive IOC Actions, you must configure at least one safe URL. A safe URL allows you to verify traffic gets to the Actor when Actions are run. This helps you to verify that proxy forwarding rules or source NAT rules are configured correctly in your environment.

1. Go to **Settings > Director Settings**. The Systems Settings page opens.
2. Select **Captive IOC Actions**.

3. Enter one safe URL per line in the Safe URLs for Verification field.

   You must enter at least one safe URL and you must include the entire URL (http/https, the domain, and any path/arguments if desired).

4. Enter sleep time (in seconds) for the Action to wait between checking each safe URL.
5. Click **Update Captive IOC Settings**.

To configure Captive IOC Action Communication Rules

Communication rules define how communication between two Actors will occur when running Captive IOC Actions.

1. Go to **Settings > Director Settings**. The Systems Settings page opens.
2. Select **Captive IOC Actions**.
3. Click **Add Captive IOC Rule**.
4. Select a **Source Actor**.

   Source and destination Actors must have the **Captive IOC Enabled** parameter set to Yes. You can set this parameter on the Actor in **Environment > Actors**. For more information, see the Actors section in the Admin Guide.

5. Select a **Destination Actor**.
6. Select one of the following communication types.
   If you select one of the proxy types, you are prompted to select a proxy to use. The list of available proxies match what is listed in the Proxy Definitions table on the **Proxy Rules** Settings page. Access this by going to **Settings > Director Settings**. The Systems Settings page opens. Then click **Proxy Rules**.
   - Source NAT (no Proxy)
   - Proxy Definition & Source NAT
   - Proxy Forwarding
7. Click **Submit** to save your communication rule.