Palo Alto Networks® Wildfire connector v1.0.0

About the connector

The Palo Alto Networks® Wildfire Malware sandbox provides a service that analyzes file samples and URLs and provides the reputation of submitted entities.

This document provides information about the PaloAlto Wildfire connector, which facilitates automated interactions, with a Palo Alto Networks® Wildfire server using CyOPs™ playbooks. Add the PaloAlto Wildfire connector as a step in CyOPs™ playbooks and perform automated operations, such as submitting files or URLs to the Palo Alto Networks® Wildfire server for analyzes and retrieving reports from the Palo Alto Networks® Wildfire server for previously submitted files or URLs.

Version information

Connector Version: 1.0.0

Compatibility with CyOPs™ Versions: 4.9.0.0-708 and later

Compatibility with PaloAlto Wildfire Sandbox Versions: 6 and later

Installing the connector

For the procedure to install a connector, click here.

Prerequisites to configuring the connector

- You must have the IP address or the Server URL of Palo Alto Networks® Wildfire sandbox server to which you will connect and perform the automated operations and the API Key to access that server.
- To access the CyOPs™ UI, ensure that port 443 is open through the firewall for the CyOPs™ instance.

Configuring the connector

For the procedure to configure a connector, click here.

Configuration parameters

In CyOPs™, on the Connectors page, select the **PaloAlto Wildfire** connector and click **Configure** to configure the following parameters:

Parameter	Description
Server	IP address or Server URL of the Palo Alto Networks® Wildfire sandbox server to which you will connect and perform the automated operations.
API Key	API key that is configured for your account to access the Palo Alto Networks® Wildfire sandbox server.

Actions supported by the connector

The following automated operations can be included in playbooks and you can also use the annotations to access operations from CyOPs™ release 4.10.0 onwards:

Function	Description	Annotation and Category
Submit File	Submits files from the CyOPs™ `Attachment` Module to the Wildfire sandbox server for analyzes.	submit_file Investigation
Submit URL	Submits a URL to the Wildfire sandbox server for analyzes.	submit_url Investigation
Get Report	Retrieves a report from the Wildfire sandbox server for the files or URLs you have submitted. Reports are retrieved based on the hash value of the file or URL that you specify. You can use this report to determine the reputation of the URL or file.	get_report Investigation

operation: Submit File

Input parameters

Note: To use this operation, you must submit files for analyzes to the Wildfire sandbox from the CyOPs™ 'Attachments' module only.

You can upload the following supported file types to the Wildfire sandbox for analysis:

- Doc
- Exe
- JS

- PDF
- PPT
- PS1
- RAR
- VBS
- XLS
- Zip

Parameter	Description
File to detonate	CyOPs™ file IRI value of the file that you want to submit to the Wildfire sandbox server for analyzes. The file IRI is used to access the file in the *Attachments* module of CyOPs™. In the playbook, the value of the **File to detonate** field defaults to *{{vars.file_iri}}*.

Output

The JSON output contains the retrieved details of the submitted file, including the sha256 value of the submitted file. You can use this sha256 value to retrieve scan reports from the Palo Alto Networks® Wildfire server for this submitted file.

Following image displays a sample output:

operation: Submit URL

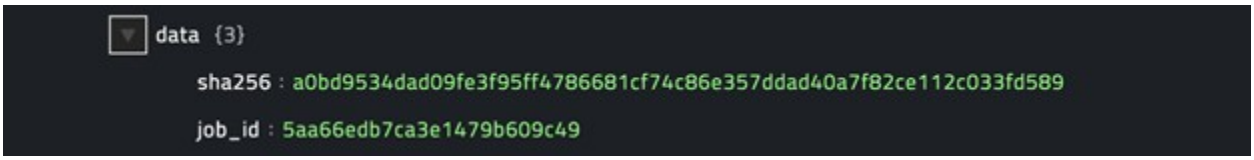
Input parameters

Parameter	Description
URL to detonate	URL that you want to submit to the Wildfire sandbox server for analyzes.

Output

The JSON output contains the retrieved details of the submitted URL, including the sha256 value of the submitted URL. You can use this sha256 value to retrieve scan reports from the Palo Alto Networks® Wildfire server for this submitted URL.

Following image displays a sample output:



operation: Get Report

Input parameters

Parameter	Description
HashValue(sha256)	Hash value (sha256only) of a previously submitted file or URL for which you want to retrieve the analysis report from the Palo Alto Networks® Wildfire server.

Output

The JSON output contains the retrieved analysis report from the Palo Alto Networks® Wildfire sandbox server for a previously submitted file or URL based on the Hash value you have specified. You can use the report details to determine the reputation of the previously submitted files or URLs. The report details also include other details such as network pcap, signatures, and targets, of the previously submitted file or URL.

Following image displays a sample output that contains the sha256 value, score, and category of the previously submitted file or URL:

Included playbooks

The *Sample - PaloAlto Wildfire - 1.0.0* playbook collection comes bundled with the PaloAlto Wildfire connector. This playbook contains steps using which you can perform all supported actions. You can see the bundled playbooks in the **Automation** > **Playbooks** section in CyOPs™ after importing the PaloAlto Wildfire connector.

- Get Report from Wildfire
- Submit File to Wildfire
- Submit URL to Wildfire

Note: If you are planning to use any of the sample playbooks in your environment, ensure that you clone those playbooks and move them to a different collection, since the sample playbook collection gets deleted during connector upgrade and delete.