**pcopy.py**

Security Solutions Architecture

Current version 1.2

Updated December 4, 20

Tested with Phantom 4.9.35731

|  |  |  |
| --- | --- | --- |
| logo_splunk_white_rgb | Splunk, Inc. 270 Brannan Street, 1st Floor San Francisco, CA 94107 | +1.415.568.4200(Main)  +1.415.869.3906 (Fax) [www.splunk.com](http://www.splunk.com) |

**Table of Contents**

Overview 3

Configuration 3

Certificate verification 3

Output directory 3

Configuration items 3

Syntax 4

Get configuration 4

Put configuration 4

Limitations 4

Not implemented 4

Update behavior 4

# Overview

The pcopy.py script can be used to backup configuration and apply configuration to a Phantom instance. It does this over the REST interface and requires HTTPS access to the Phantom instance.

# Configuration

Configuration for the script is done directly in the Python file. The user editable variables are at the top as follows.

## Certificate verification

VERIFY\_CERT = False

This takes a value of True or False and is used to decide whether to verify the certificates provided by Phantom for the secure session.

## Output directory

OUTPUT\_DIR = "ph\_config"

This directory will be created with the get command and will be read from for the put command.

## Configuration items

ITEMS = {

"system\_settings": {

"mobile": True,

"clickable\_urls": True,

"multi\_tenant": True,

"whitelist": True,

"indicators": True,

"audit\_trail\_settings": True,

"auth\_settings": True

},

"role": True,

"cef": True,

"container\_status": True,

"severity": True,

"labels": True,

"custom\_fields": True,

"tags": True,

"container\_pin\_settings": True

}

Any item set to True in the list will be pulled down with the get command and applied with the put command.

# Syntax

## Get configuration

./pcopy put [hostname/ipaddress]

Use the hostname or IP address of your Phantom instance as the second argument. Any items marked True in the configuration will be queried over REST and the resulting JSON will be put in the output directory specified.

You will be prompted for the username and password to authenticate with.

## Put configuration

./pcopy get [hostname/ipaddress]

Use the hostname or IP address of your Phantom instance as the second argument. Any items marked True will have their configuration read from the output directory, cleaned up to repost Phantom, and then applied to the Phantom instance via a POST.

You will be prompted for the username and password to authenticate with.

# Limitations

## Not implemented

* License
* System settings (not features)
* Users
* Response
* Resolution
* Workbooks
* Assets
* Playbook repos
* Apps
* Custom lists
* Tags (only get is implemented)

## Update behavior

**Custom fields** are added all at once and will replace whatever exists in Phantom.

**System settings features** will update the True/False setting on any specified features.

**Roles** will fail if the named role already exists. The role will not be updated, and this error can be ignored.

An unsuccessful status code of 400 was returned for https://192.168.7.204/rest/role.

b'{"failed": true, "message": "Role with this name (test) already exists."}'

**CEF fields** will fail if the named field already exists. The field will not be updated, and this error can be ignored.

An unsuccessful status code of 400 was returned for https://192.168.7.204/rest/cef.

b'{"failed": true, "message": "duplicate key value violates unique constraint \\"cef\_name\_key\\"\\nDETAIL: Key (name)=(test) already exists.\\n"}'

**Container status** will fail if the name4d field already exists. The field will not be updated, and this error can be ignored.

An unsuccessful status code of 400 was returned for https://192.168.7.204/rest/container\_status.

b'{"failed": true, "message": "There were validation errors. {\'name\': [\'Container status with this Name already exists.\']}", "errors": {"name": ["Container status with this Name already exists."]}}'

**Severities** will fail if the named field already exists. The field will not be updated, and this error can be ignored. The High, Medium, and Low severities will not be updated.

An unsuccessful status code of 400 was returned for https://192.168.7.204/rest/severity.

b'{"failed": true, "message": "There were validation errors. {\'name\': [\'Severity with this Name already exists.\']}", "errors": {"name": ["Severity with this Name already exists."]}}'

**Tags** need to be added by hand. Only the get action works. The put action lists the tags and tells you to do it by hand.

**Container pin settings (HUD cards)** are just added to the existing collection. If the card already exists another copy is added.