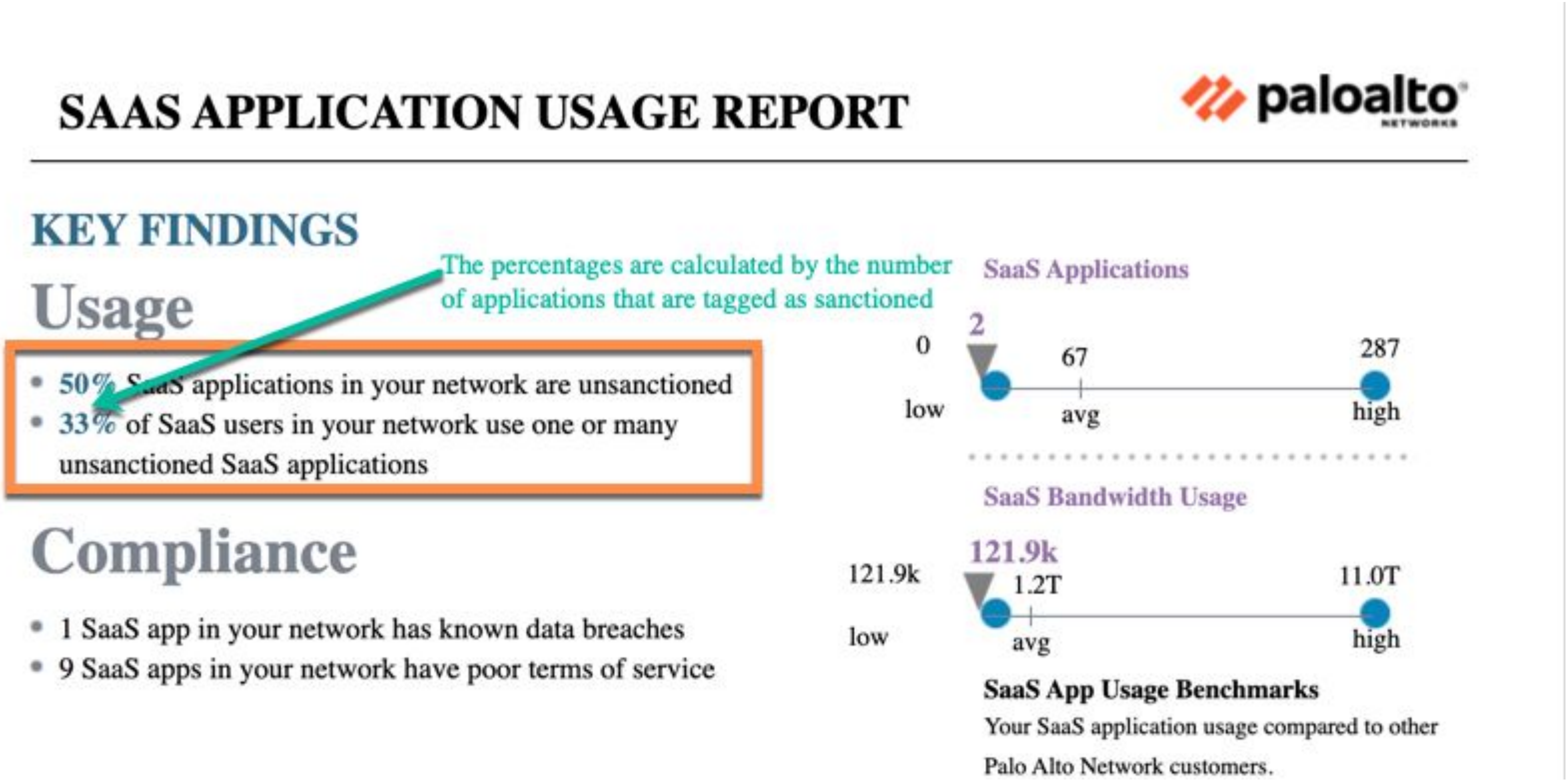
Tagging Sanctioned SaaS Applications

PANOS API

Zack Macharia | Systems Engineer

SaaS Report

Improve SaaS Usage Percentages by adding the “Sanctioned” Tag



SAAS APPLICATION USAGE REPORT

paloalto NETWORKS

KEY FINDINGS

The percentages are calculated by the number of applications that are tagged as sanctioned

Usage

- 50% SaaS applications in your network are unsanctioned
- 33% of SaaS users in your network use one or many unsanctioned SaaS applications

Compliance

- 1 SaaS app in your network has known data breaches
- 9 SaaS apps in your network have poor terms of service

SaaS App Usage Benchmarks

Your SaaS application usage compared to other Palo Alto Network customers.

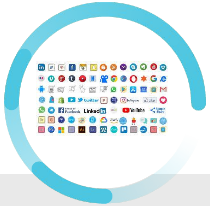
Sanctioned Tag Workflow

Run Daily Reports

Access the daily SaaS Application Usage Report

Download Report

Download the Report as a CSV/PDF for offline review



Review Apps

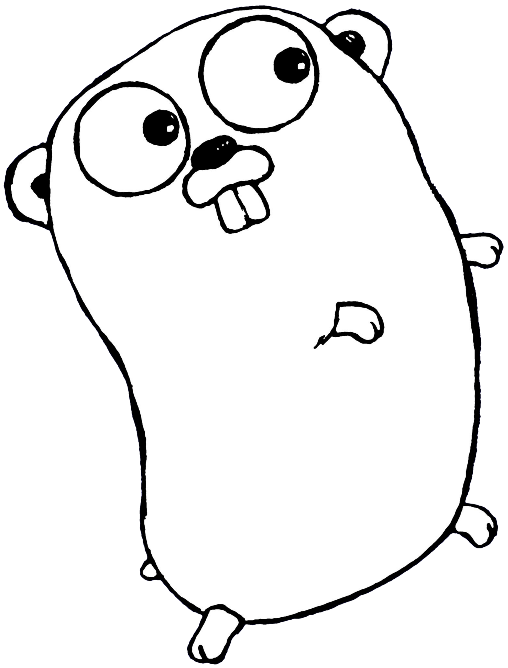
Review and Identify the applications approved for business use

Tag Applications

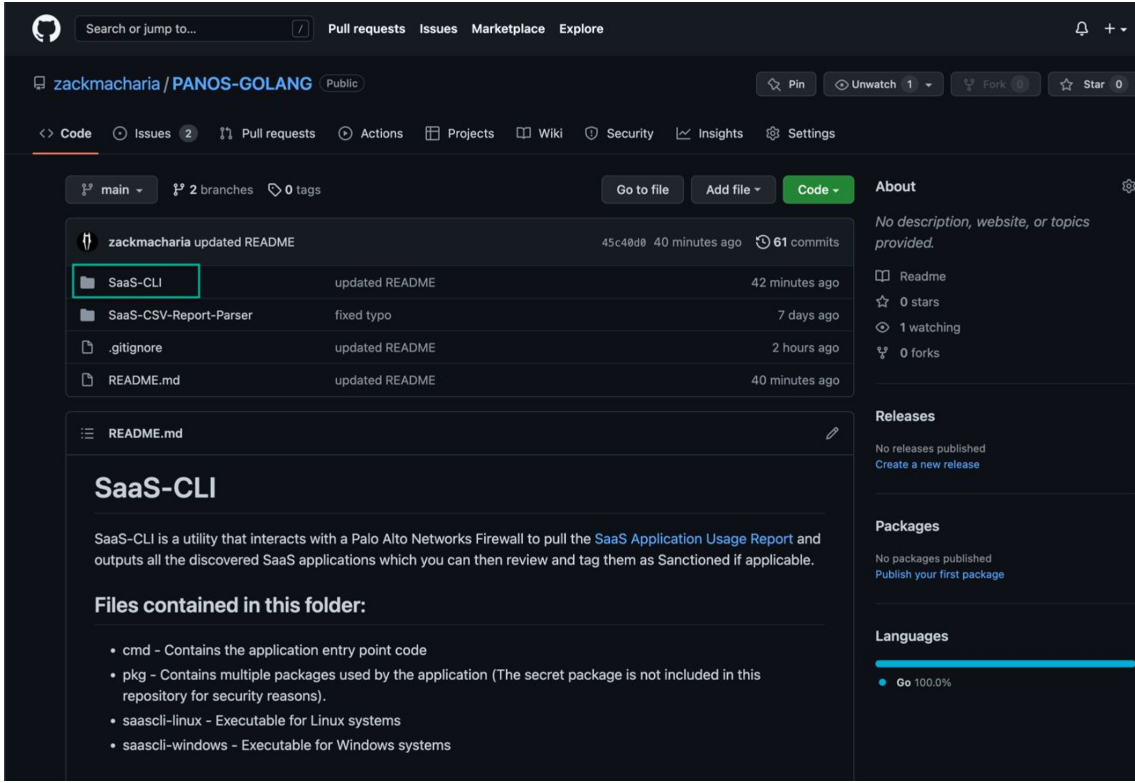
For the identified applications add the Sanctioned tag

SaaS-CLI Tool

CLI Based Application built in Go



Source code in GitHub



zackmacharia / PANOS-GOLANG Public

2 branches 0 tags

zackmacharia updated README 45c40d0 40 minutes ago 61 commits

SaaS-CLI	updated README	42 minutes ago
SaaS-CSV-Report-Parser	fixed typo	7 days ago
.gitignore	updated README	2 hours ago
README.md	updated README	40 minutes ago

README.md

SaaS-CLI

SaaS-CLI is a utility that interacts with a Palo Alto Networks Firewall to pull the SaaS Application Usage Report and outputs all the discovered SaaS applications which you can then review and tag them as Sanctioned if applicable.

Files contained in this folder:

- cmd - Contains the application entry point code
- pkg - Contains multiple packages used by the application (The secret package is not included in this repository for security reasons).
- saascli-linux - Executable for Linux systems
- saascli-windows - Executable for Windows systems

About

No description, website, or topics provided.

Readme
0 stars
1 watching
0 forks

Releases

No releases published
Create a new release

Packages

No packages published
Publish your first package

Languages

Go 100.0%

How does this tool work?

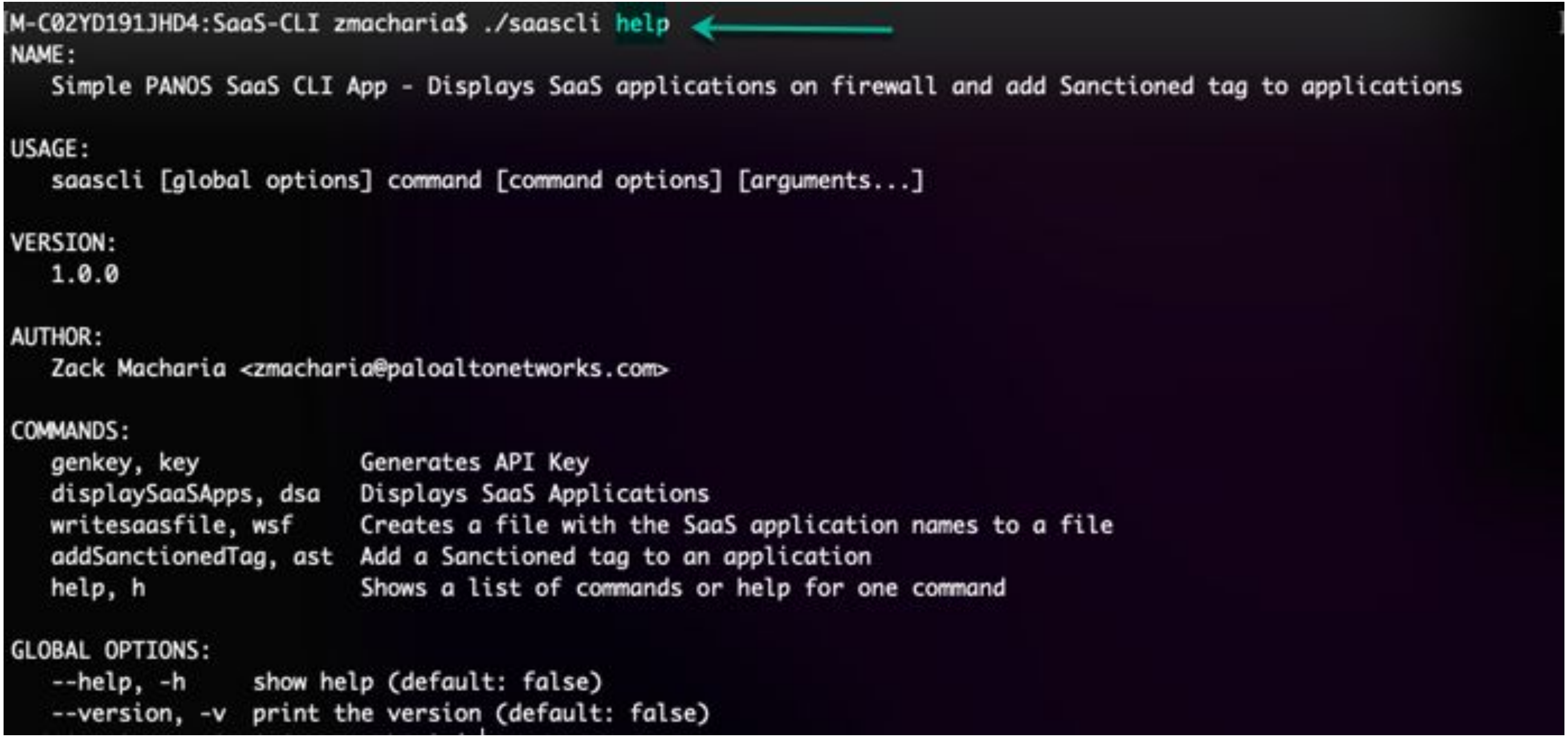
- Generate an API Key (Key will be encrypted and store as key.data file)
  - Used to authenticate to firewall

- Display the daily Saas App report on the terminal
  - Used to display applications on terminal/cmd screen

- Write the daily report on a text file for offline analysis
  - Writes the applications names to a text file

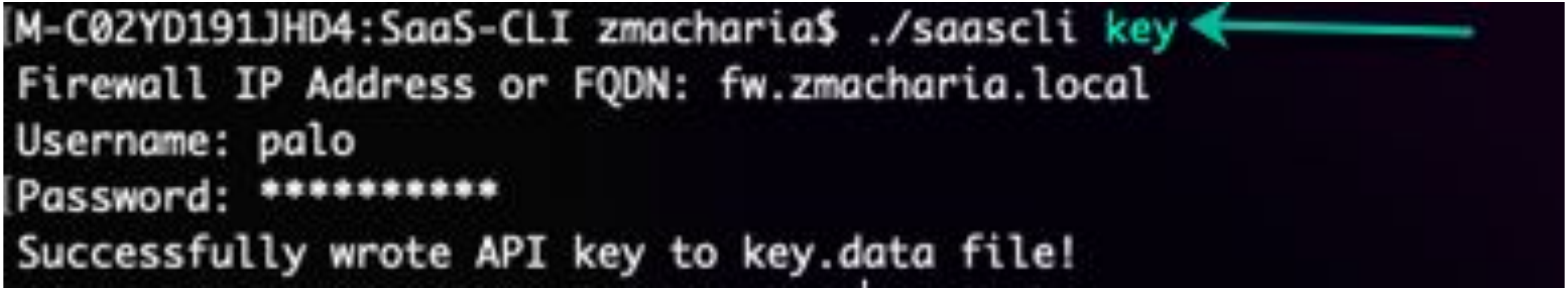
- Add the predefined “Sanctioned” tags to identified SaaS Applications

View all the commands using the “help” command



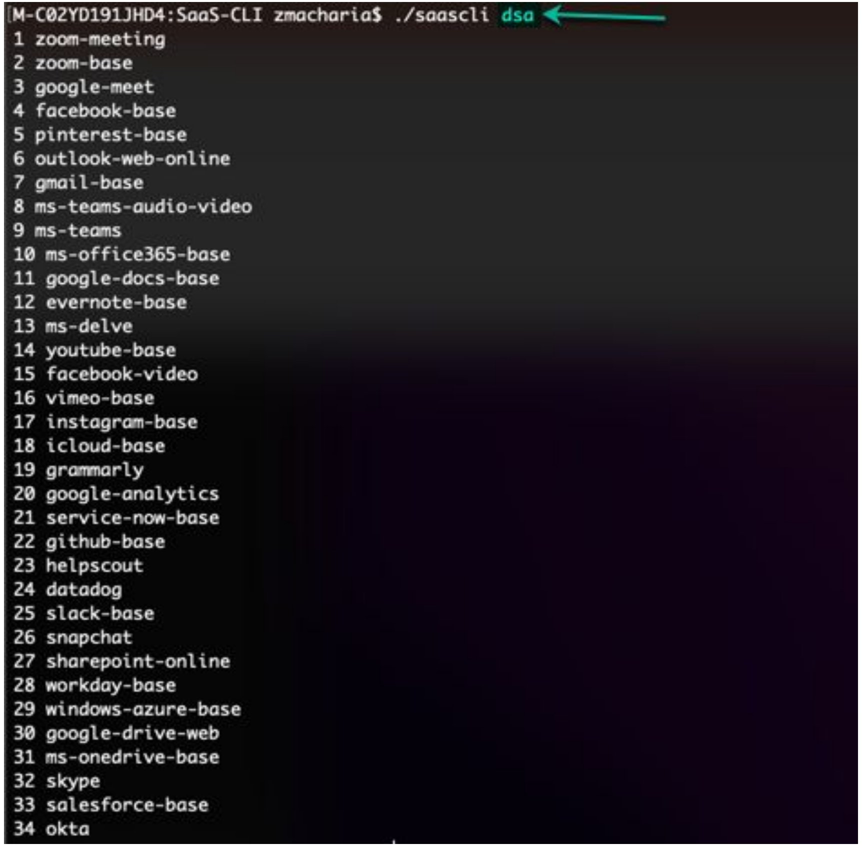
```
[M-C02YD191JHD4:SaaS-CLI zmacharia$ ./saascli help
NAME:
   Simple PANOS SaaS CLI App - Displays SaaS applications on firewall and add Sanctioned tag to applications

USAGE:
   saascli [global options] command [command options] [arguments...]

VERSION:
   1.0.0

AUTHOR:
   Zack Macharia <zmacharia@paloaltonetworks.com>

COMMANDS:
   genkey, key             Generates API Key
   displaySaaSApps, dsa    Displays SaaS Applications
   writesaasfile, wsf      Creates a file with the SaaS application names to a file
   addSanctionedTag, ast   Add a Sanctioned tag to an application
   help, h                 Shows a list of commands or help for one command

GLOBAL OPTIONS:
   --help, -h     show help (default: false)
   --version, -v  print the version (default: false)
```

Generate API KEY using the “key” command



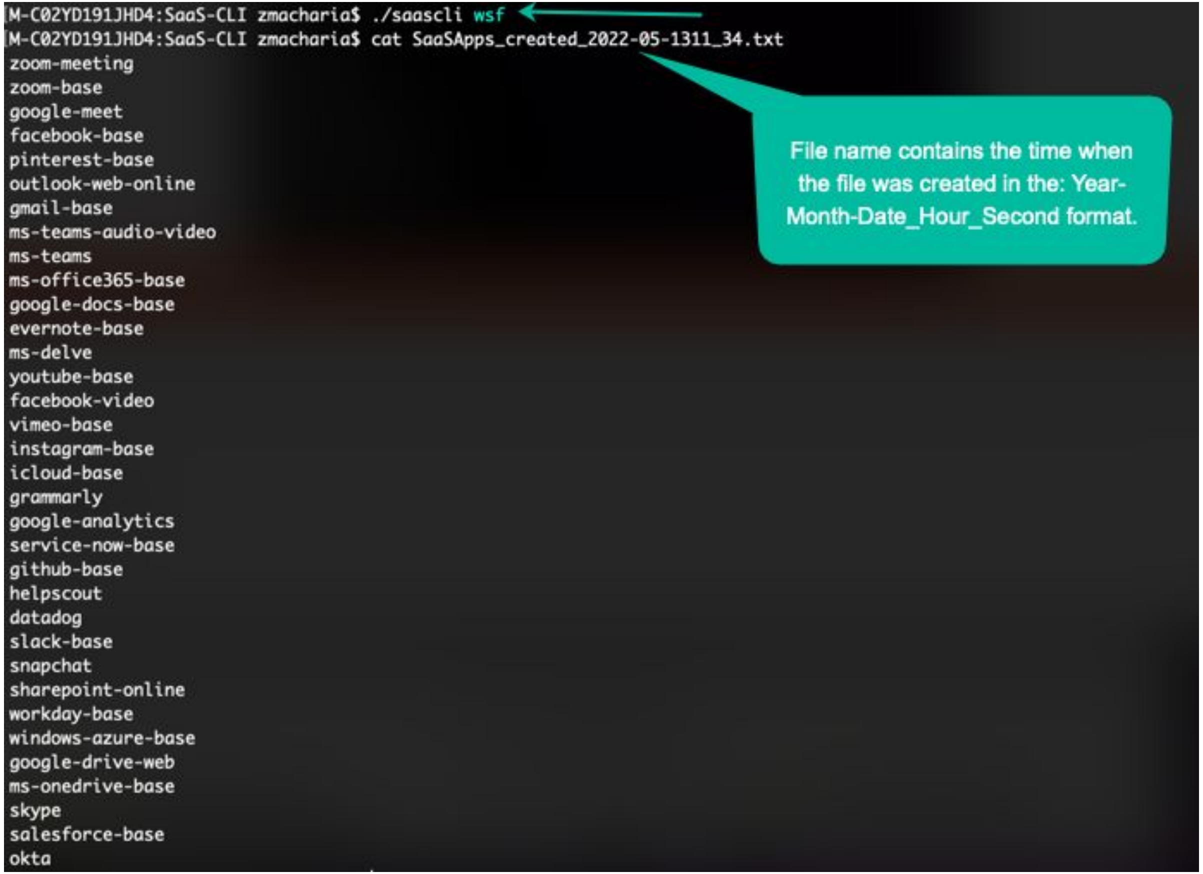
```
[M-C02YD191JHD4:SaaS-CLI zmacharia$ ./saascli key
Firewall IP Address or FQDN: fw.zmacharia.local
Username: palo
[Password: ***********
Successfully wrote API key to key.data file!
```

Displays SaaS Applications on terminal using the “dsa” command



```
[M-C02YD191JHD4:SaaS-CLI zmacharia$ ./saascli dsa
1 zoom-meeting
2 zoom-base
3 google-meet
4 facebook-base
5 pinterest-base
6 outlook-web-online
7 gmail-base
8 ms-teams-audio-video
9 ms-teams
10 ms-office365-base
11 google-docs-base
12 evernote-base
13 ms-delve
14 youtube-base
15 facebook-video
16 vimeo-base
17 instagram-base
18 icloud-base
19 grammarly
20 google-analytics
21 service-now-base
22 github-base
23 helpscout
24 datadog
25 slack-base
26 snapchat
27 sharepoint-online
28 workday-base
29 windows-azure-base
30 google-drive-web
31 ms-onedrive-base
32 skype
33 salesforce-base
34 okta
```

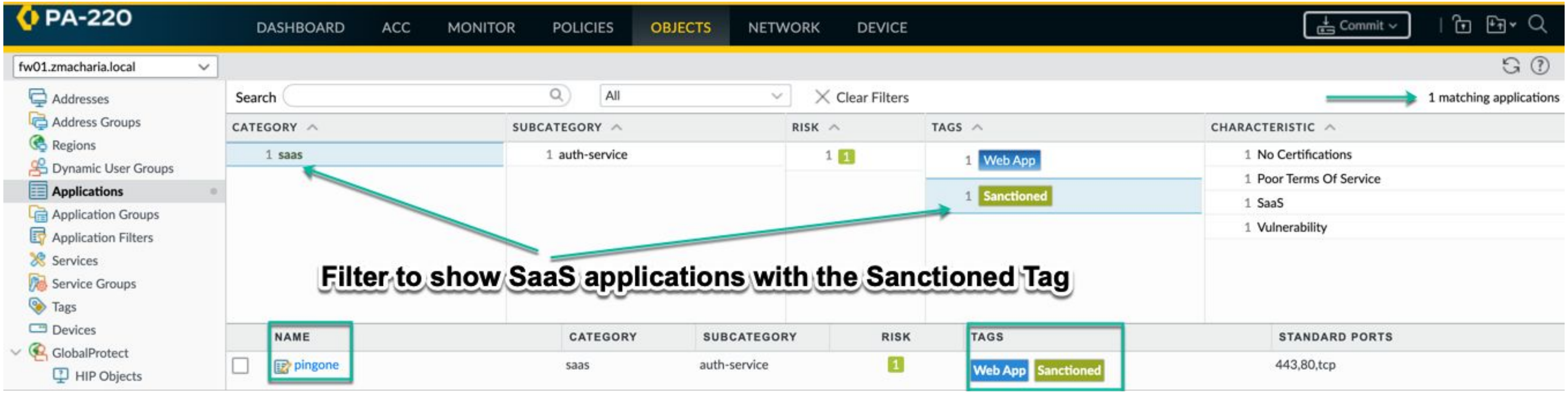
Create a file with SaaS Applications names using the “wsf” command



```
[M-C02YD191JHD4:SaaS-CLI zmacharia$ ./saascli wsf
[M-C02YD191JHD4:SaaS-CLI zmacharia$ cat SaaSApps_created_2022-05-1311_34.txt
zoom-meeting
zoom-base
google-meet
facebook-base
pinterest-base
outlook-web-online
gmail-base
ms-teams-audio-video
ms-teams
ms-office365-base
google-docs-base
evernote-base
ms-delve
youtube-base
facebook-video
vimeo-base
instagram-base
icloud-base
grammarly
google-analytics
service-now-base
github-base
helpscout
datadog
slack-base
snapchat
sharepoint-online
workday-base
windows-azure-base
google-drive-web
ms-onedrive-base
skype
salesforce-base
okta
```

File name contains the time when the file was created in the: Year-Month-Date_Hour_Second format.

Example showing one application (pingone) with the Sanctioned tag



1 matching applications

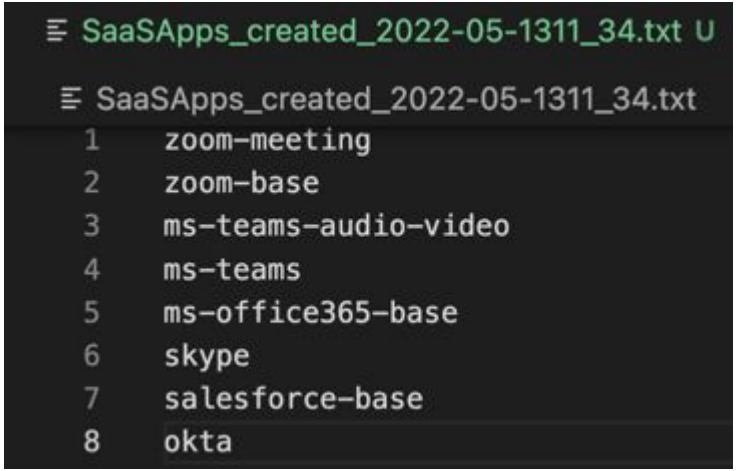
CATEGORY	SUBCATEGORY	RISK	TAGS	CHARACTERISTIC
1 saas	1 auth-service	1 1	1 Web App	1 No Certifications
			1 Sanctioned	1 Poor Terms Of Service
				1 SaaS
				1 Vulnerability

Filter to show SaaS applications with the Sanctioned Tag

	NAME	CATEGORY	SUBCATEGORY	RISK	TAGS	STANDARD PORTS
□	pingone	saas	auth-service	1	Web App Sanctioned	443,80,tcp

Example Edited Text

Example of business applications that need to bTe tagged as Sanctions from the previously generated file.

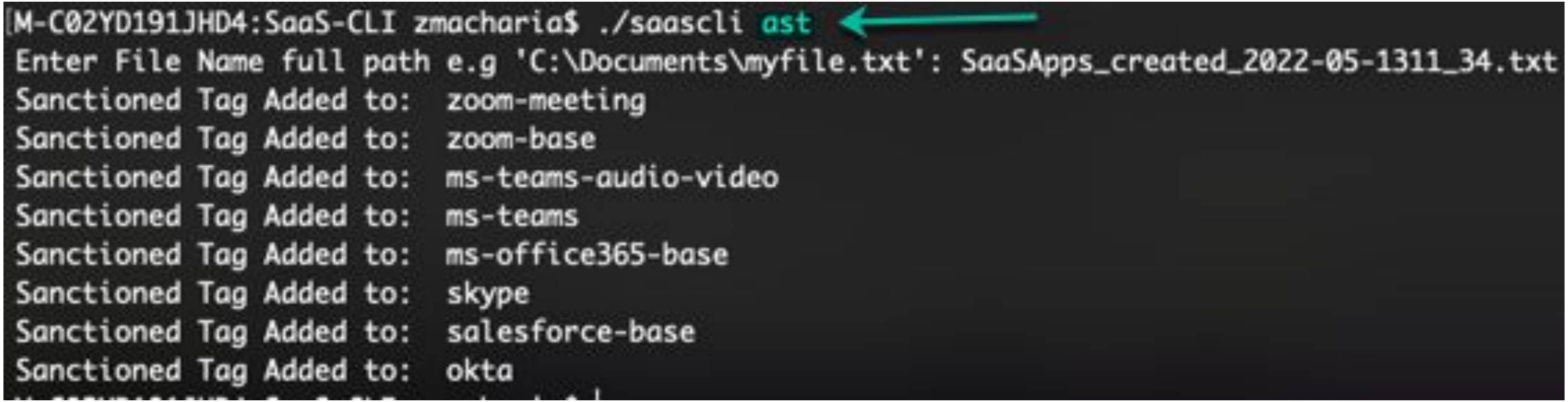


SaaSApps_created_2022-05-1311_34.txt

```
zoom-meeting
zoom-base
ms-teams-audio-video
ms-teams
ms-office365-base
skype
salesforce-base
okta
```

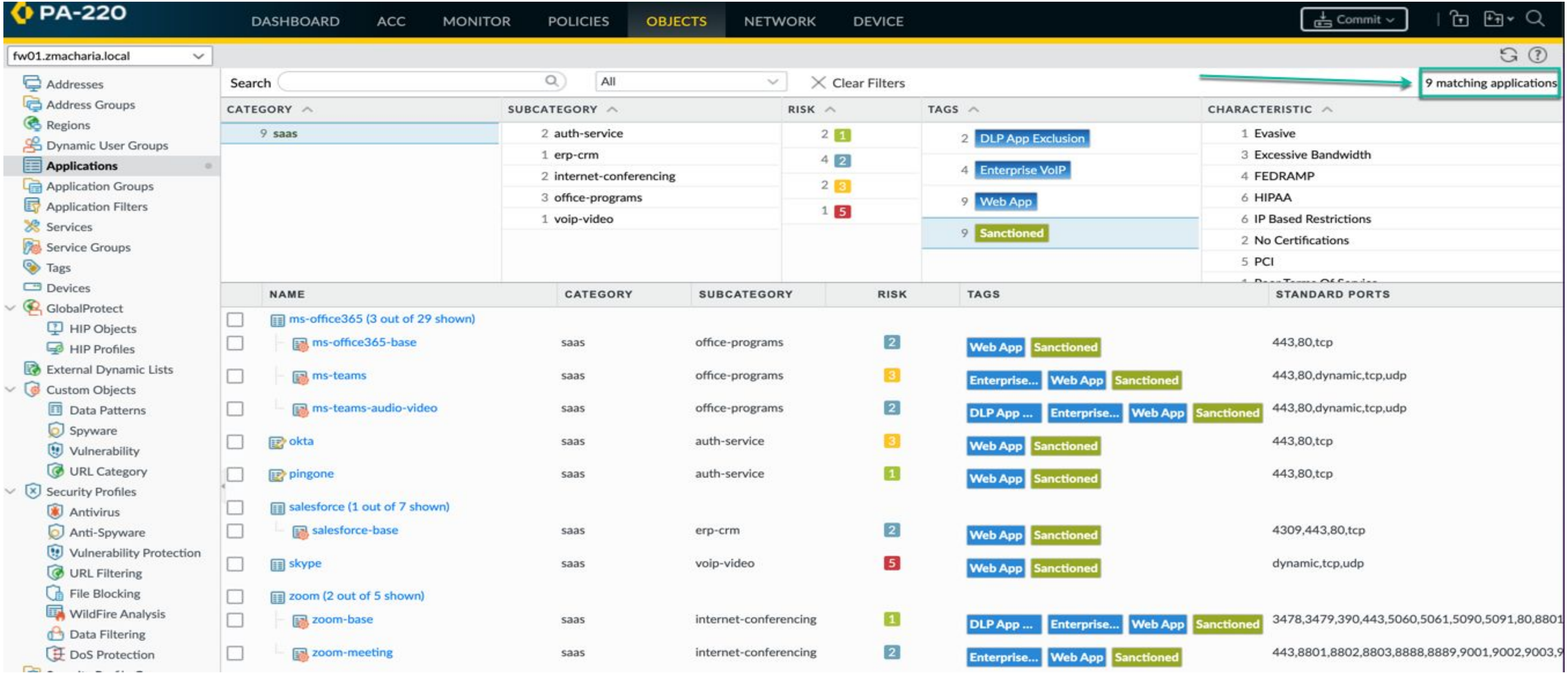
Add Sanctioned tag using the “ast” command

Note: In this example the **saascli** application and the edited text file are in the same folder location.



```
M-C02YD191JHD4:SaaS-CLI zmacharia$ ./saascli ast
Enter File Name full path e.g 'C:\Documents\myfile.txt': SaaSApps_created_2022-05-1311_34.txt
Sanctioned Tag Added to:  zoom-meeting
Sanctioned Tag Added to:  zoom-base
Sanctioned Tag Added to:  ms-teams-audio-video
Sanctioned Tag Added to:  ms-teams
Sanctioned Tag Added to:  ms-office365-base
Sanctioned Tag Added to:  skype
Sanctioned Tag Added to:  salesforce-base
Sanctioned Tag Added to:  okta
```

Example showing nine applications with the Sanctioned tag



9 matching applications

CATEGORY	SUBCATEGORY	RISK	TAGS	CHARACTERISTIC
9 saas	2 auth-service	2 1	2 DLP App Exclusion	1 Evasive
	1 erp-crm	4 2	4 Enterprise VoIP	3 Excessive Bandwidth
	2 internet-conferencing	2 3	9 Web App	4 FEDRAMP
	3 office-programs	1 5	9 Sanctioned	6 HIPAA
	1 voip-video			6 IP Based Restrictions
				2 No Certifications
				5 PCI

	NAME	CATEGORY	SUBCATEGORY	RISK	TAGS	STANDARD PORTS
□	ms-office365 (3 out of 29 shown)					
□	ms-office365-base	saas	office-programs	2	Web App Sanctioned	443,80,tcp
□	ms-teams	saas	office-programs	3	Enterprise... Web App Sanctioned	443,80,dynamic,tcp,udp
□	ms-teams-audio-video	saas	office-programs	2	DLP App ... Enterprise... Web App Sanctioned	443,80,dynamic,tcp,udp
□	okta	saas	auth-service	3	Web App Sanctioned	443,80,tcp
□	pingone	saas	auth-service	1	Web App Sanctioned	443,80,tcp
□	salesforce (1 out of 7 shown)					
□	salesforce-base	saas	erp-crm	2	Web App Sanctioned	4309,443,80,tcp
□	skype	saas	voip-video	5	Web App Sanctioned	dynamic,tcp,udp
□	zoom (2 out of 5 shown)					
□	zoom-base	saas	internet-conferencing	1	DLP App ... Enterprise... Web App Sanctioned	3478,3479,390,443,5060,5061,5090,5091,80,8801
□	zoom-meeting	saas	internet-conferencing	2	Enterprise... Web App Sanctioned	443,8801,8802,8803,8888,8889,9001,9002,9003,9