AppGate SDP Basic Training Extra Labs

Lefteris Chairetakis

Zahir Alli

October 2019

Singapore

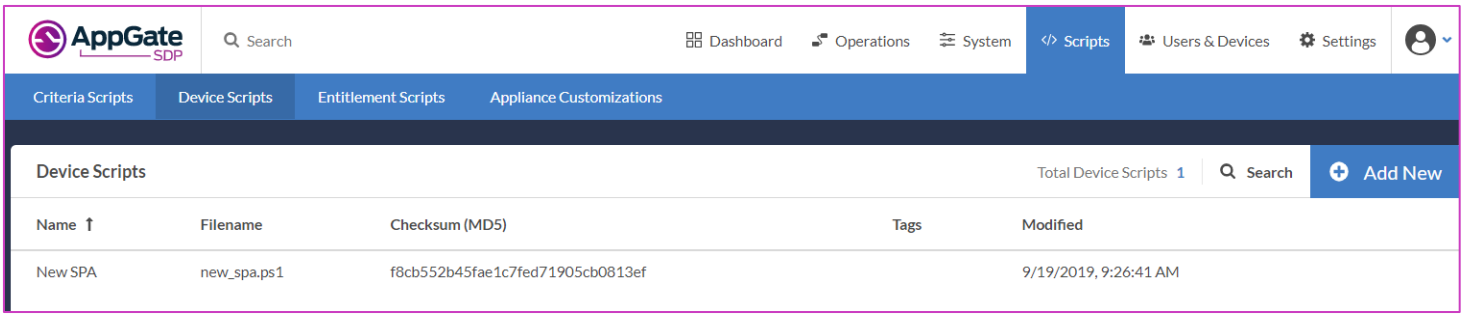
Table of Contents

Lab 1. Publishing a new SPA via device script 3
Lab 2. Using Ringfence rules to block specific packets 5
Lab 3. Access to distribution server is not working! 5

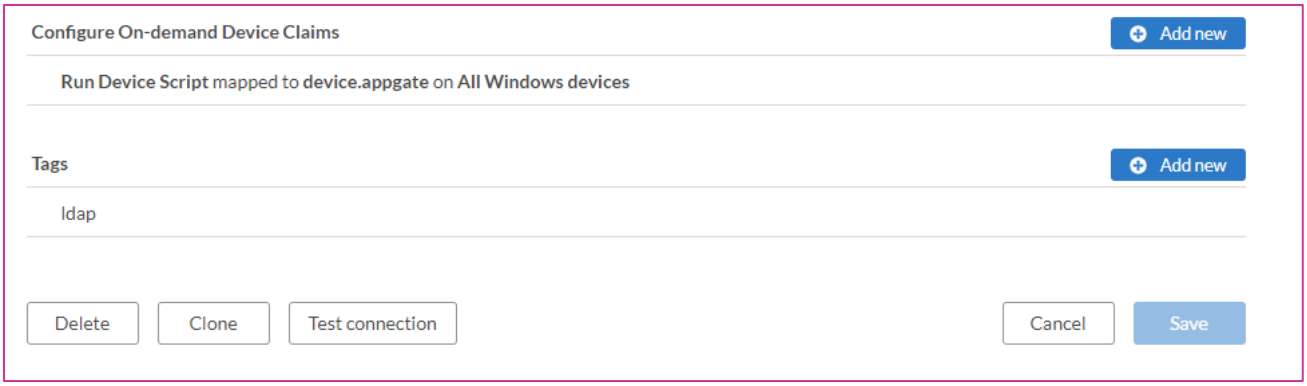
Lab 1. Publishing a new SPA via device script

Your security team have done some auditing test and inform you that you need to change your built-in SPA key to a new one. Due to security policy you cannot send the new URL via email nor publish it in your intranet. Moreover, most of your users are not technical, so you need to transfer them to the new SPA as transparent as possible. A way to do that would be by using a device script and taking advantage of Message of the Day feature to inform the users about the new SPA. Let us dive into the details

- Login to the admin UI and navigate to **Settings → Client Connections**
- Press **Add new** and choose any name such as **NEW_SPA** and press **Save**. Note that space is not allowed for SPA name.
- Based on your OS, download the relative script from http://intranet.packnot.intra/files/course/ and open it with any text-editor such as notepad.
- Copy the URL of the new SPA and paste it in the field where it is noted **" PUT YOUR NEW SPA"** and save the file
- In the admin UI, Navigate to **Scripts →Device Scripts → Add New** and fill the following information
  Name: NEW SPA
  Notes: Anything as it is optional
  File → choose a file and browse to your script**.**
  Press **Save**



- Navigate to **System → Identity Providers →openldap → Configure On-demand Device Claims→ Add new → select a command → Run Device Script→ Device Scripts →** choose **NEW SPA**
  - Leave Arguments empty
  - Claim Name: set **appgate**
  - For Platform choose **All Windows Devices or Mac or Linux (Based on your OS)**
  - Click on **Done** then **Save**



- Now let us utilize the **Message of the Day** feature to inform our users that the old URL will be deprecated, and we will move to new URL. To do so navigate to **Settings → Global Settings → Message of the Day** and type a message to inform your users about the new process, something like "***You should now see a new shortcut on your Desktop called Appgate. You need to log out of your AppGate client and double click on the shortcut to login again.***"
- Now you need to apply the device script to all your users, so when they login they will get a shortcut with the new SPA with IdP in their desktop **IF they are on Mac or Linux (Ubuntu),** and on Windows it will be in the **link folder, ex:- C:\Users\zahir.alli\Links**
- Now all they need is to logout and double click on the shortcut.

*** Sometimes users tend to ignore admin messages and continue to work as they used to, however your security team is pushing to delete the old SPA and force your users to use the new one. Before doing that you need to know how many users are still using the old SPA and how many users are using the new one , how to do that ?**

The easiest way is to SSH to your Controller and run the below command:

journalctl -u cz-proxyd.service | egrep "Built-in-be*"

, this command will tell you if there are any users still using the SPA. If you want to be more specific, you can use something like:

journalctl -u cz-proxyd.service --since "1 hour ago"| egrep "Built-in-be*"| wc -l

The above command will tell how many users were connected with the old SPA the last hour.

Note: you can change time (**"1 hour ago"**) as you wish.

Finally check how many users are using the new URL. Simply run the below command:

journalctl -u cz-proxyd.service | egrep 'name "your_SPA_name"'

Note:- to troubleshoot the device script itself, you can run the script manually on your OS. Here is where they are located:

- **Windows → C:\ProgramData\AppGate\Scripts**
- **Linux → ~/.cache/appgatesdp-service/scripts/**
- **Mac OS → ~/.appgatesdp/scripts/**

Lab 2. Using Ringfence rules to block specific packets

Ringfence can be useful to mitigate the security risk of transmission of malware between devices or to block specific traffic when a user connects via AppGate. In this lab, we will block ICMP out as an example:

1- In admin UI navigate to **Operations → Ringfences Rules → Add New**
2- Under **Name** put **Block ICMP-OUT**
3- **Actions → Add new**

Name	**Block ICMP-OUT**
Notes	Block ICMP out for IPv4
Actions -Rule	BLOCK
Protocol	ICMP out
Network Resources	0.0.0.0/0
Types	0-255

Press Save

For the Ringfence Rule to take effect, you need to navigate to **Operations → Policies** and add the Rule under the Device Security section within the selected Policy – in your case you can add it under the Distribution Policy.

Log out and back in your client for the change to take effect. Are you able to ping anymore from your machine?

Lab 3. Access to distribution server is not working!

Your users cannot login to distribution server, you check the backend server and it is up and working fine. You want to access the **admin UI,** but it seems the security team has changed the password; however, you have the SSH key so you can SSH to the GW. Will that be useful?

Hint:- **cz-vpnd** handles the actual VPN traffic and has the firewall engine. Since you don't have admin UI access, it may be a good idea to check the **vpnd** log for a specific user or all users

On the terminal run the following:

journalctl -u cz-vpnd@0 (for vpnd instance number 0)

journalctl -u cz-vpnd@* (for all vpnd instances)

What can you tell from the logs?

Finally, Security team has granted you access to the admin UI. Now how to fix the problem based on the log output you saw previously?