# Installation

1. Download Raspbian Stretch Lite from the following URL:

<https://www.raspberrypi.org/downloads/raspbian/>

1. Follow instructions here to create your bootable Raspbian SD card:

<https://www.raspberrypi.org/documentation/installation/installing-images/README.md>

1. Once the Raspberry Pi is functional, log into the console (user: pi, password: raspberry)
2. Verify that you’re running the correct version of Raspbian by typing the command:

cat /etc/os-release

It should look like this:

**pi@raspberrypi**:**~ $** cat /etc/os-release

PRETTY\_NAME="Raspbian GNU/Linux 9 (stretch)"

NAME="Raspbian GNU/Linux"

VERSION\_ID="9"

VERSION="9 (stretch)"

ID=raspbian

ID\_LIKE=debian

HOME\_URL="<http://www.raspbian.org/>"

SUPPORT\_URL="<http://www.raspbian.org/RaspbianForums>"

BUG\_REPORT\_URL="<http://www.raspbian.org/RaspbianBugs>"

1. Use raspi-config to connect it to your WiFi. You may also want to enable SSH while you’re at it.
2. Download the installer using the command below:

wget <https://raw.githubusercontent.com/p0lr/PAN_DUG/master/install.sh>

1. Change the permissions on the installer script using the command below:

chmod 755 install.sh

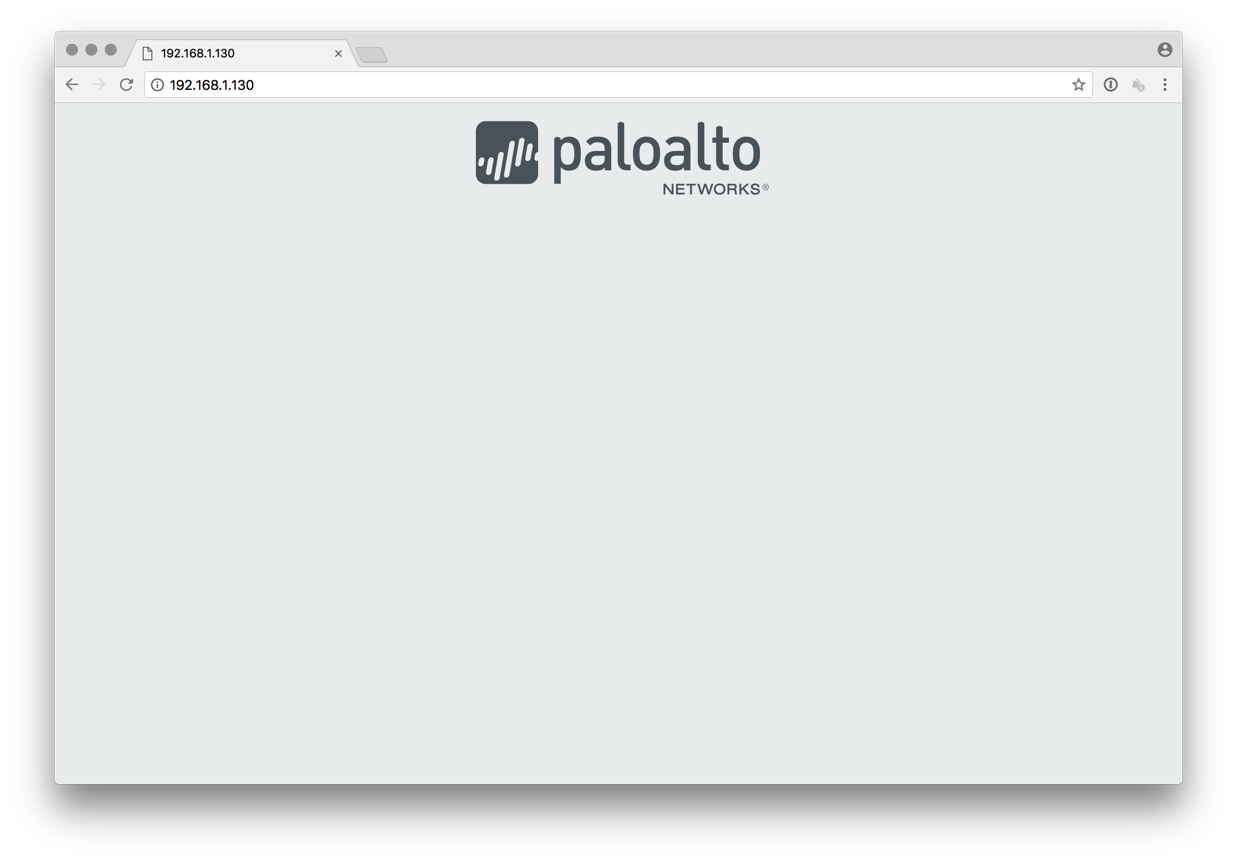
1. Run the installer:

./install.sh

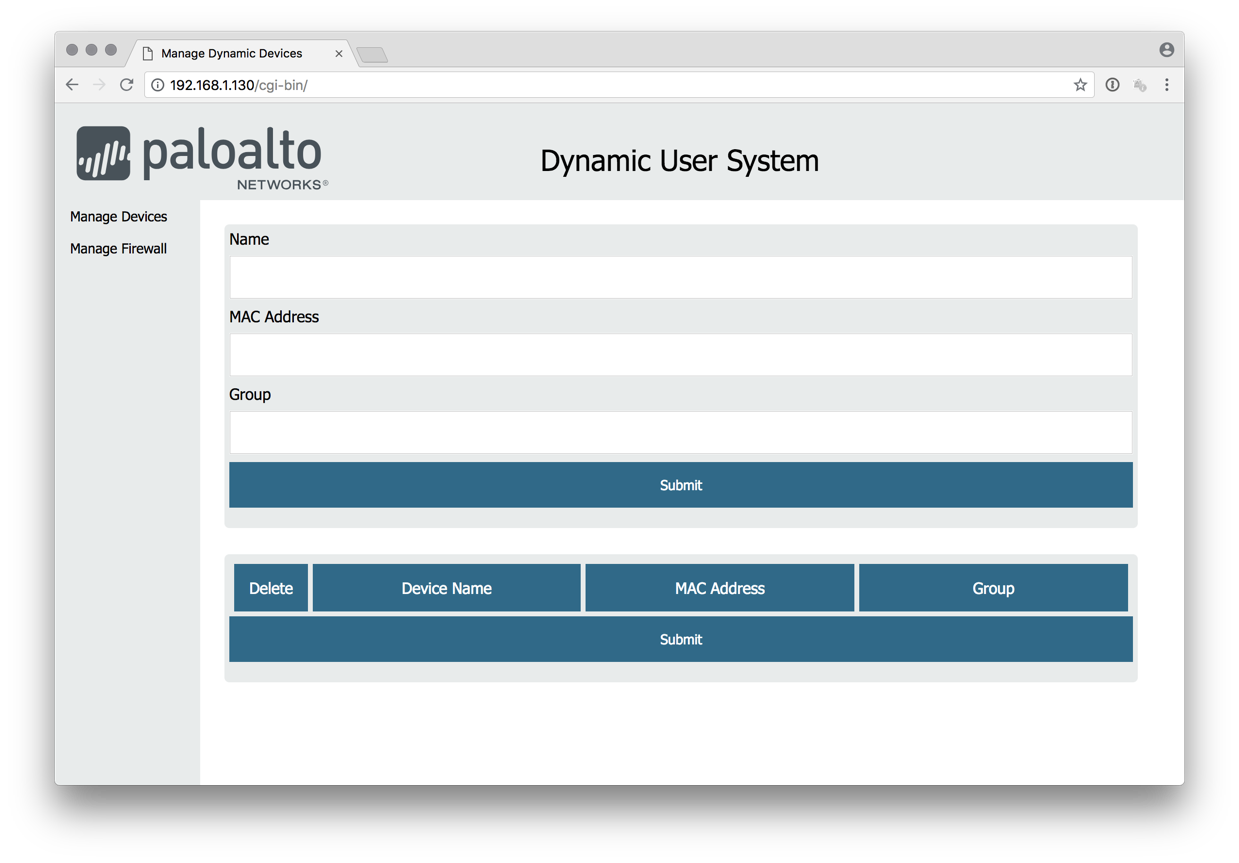
1. Reboot the Raspberry Pi

# Using the System

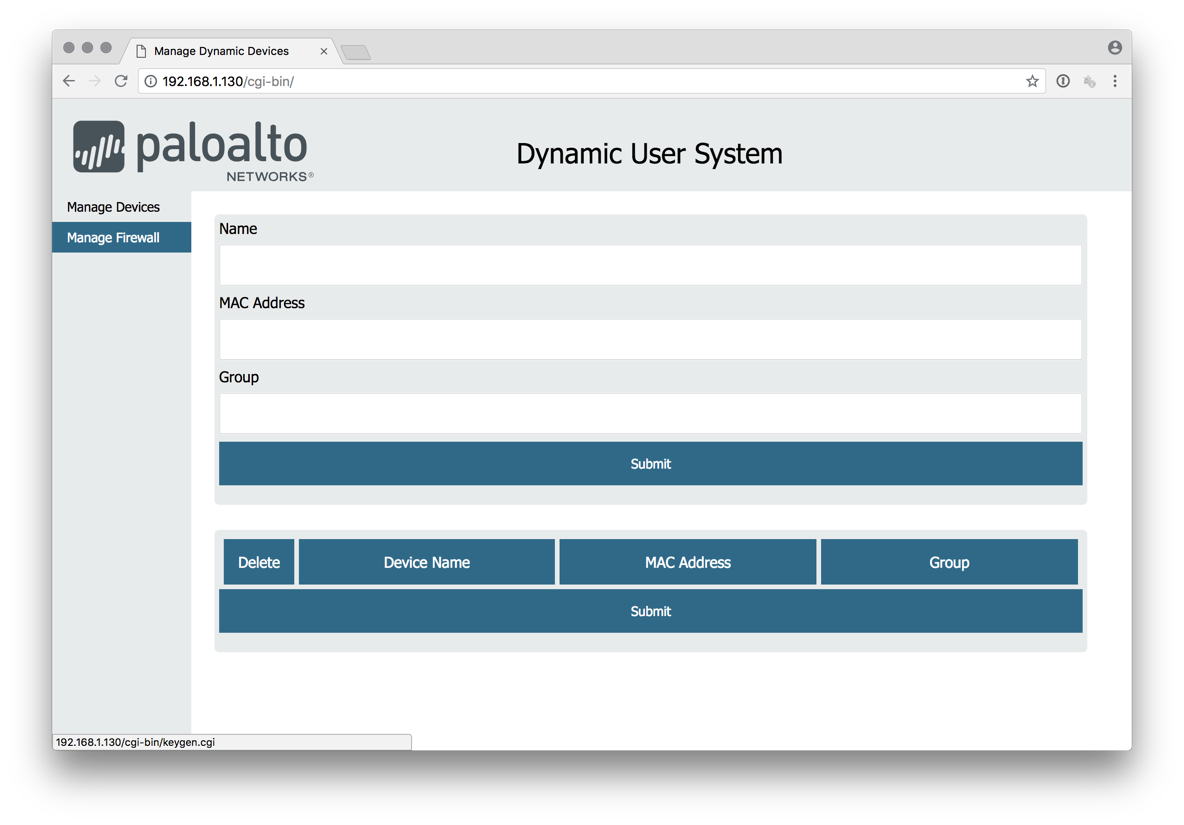
1. Point your web browser to the IP address of the Raspberry Pi



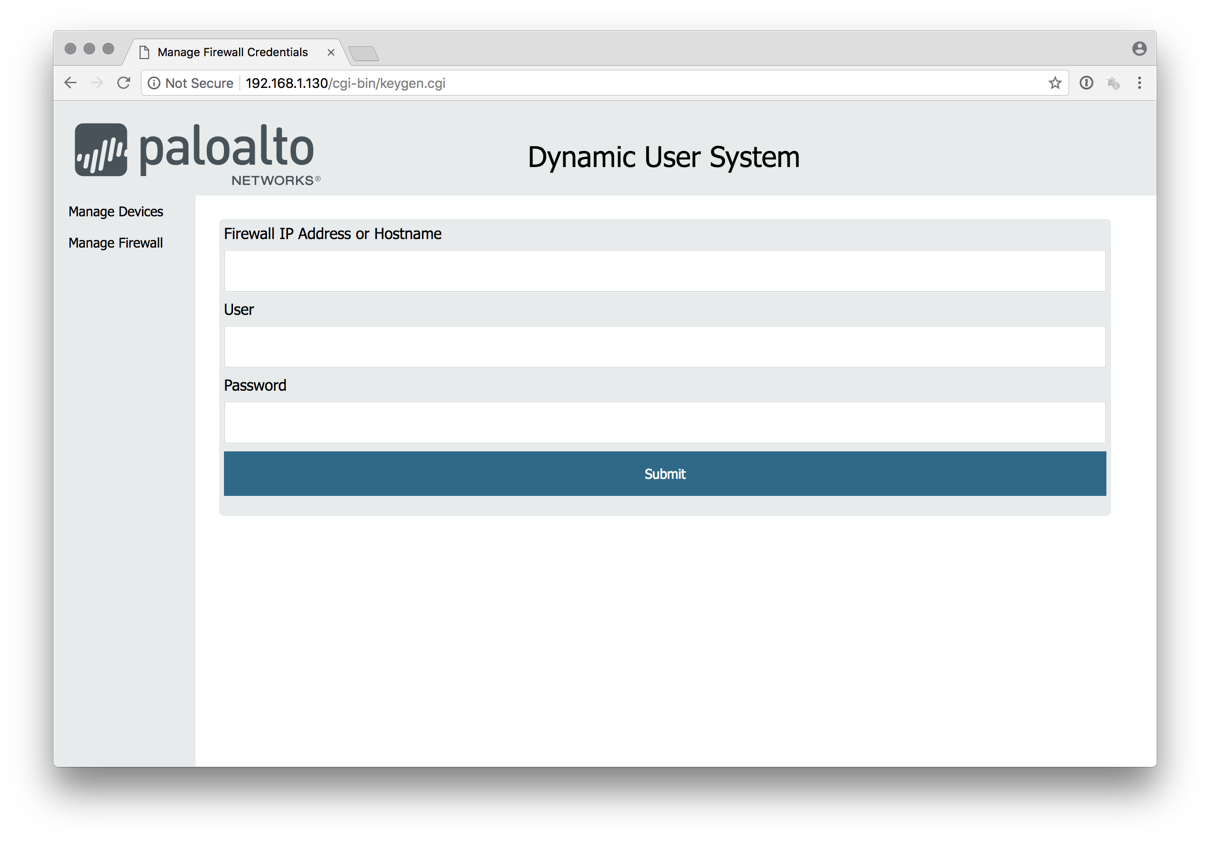
1. Click on the Palo Alto Networks logo



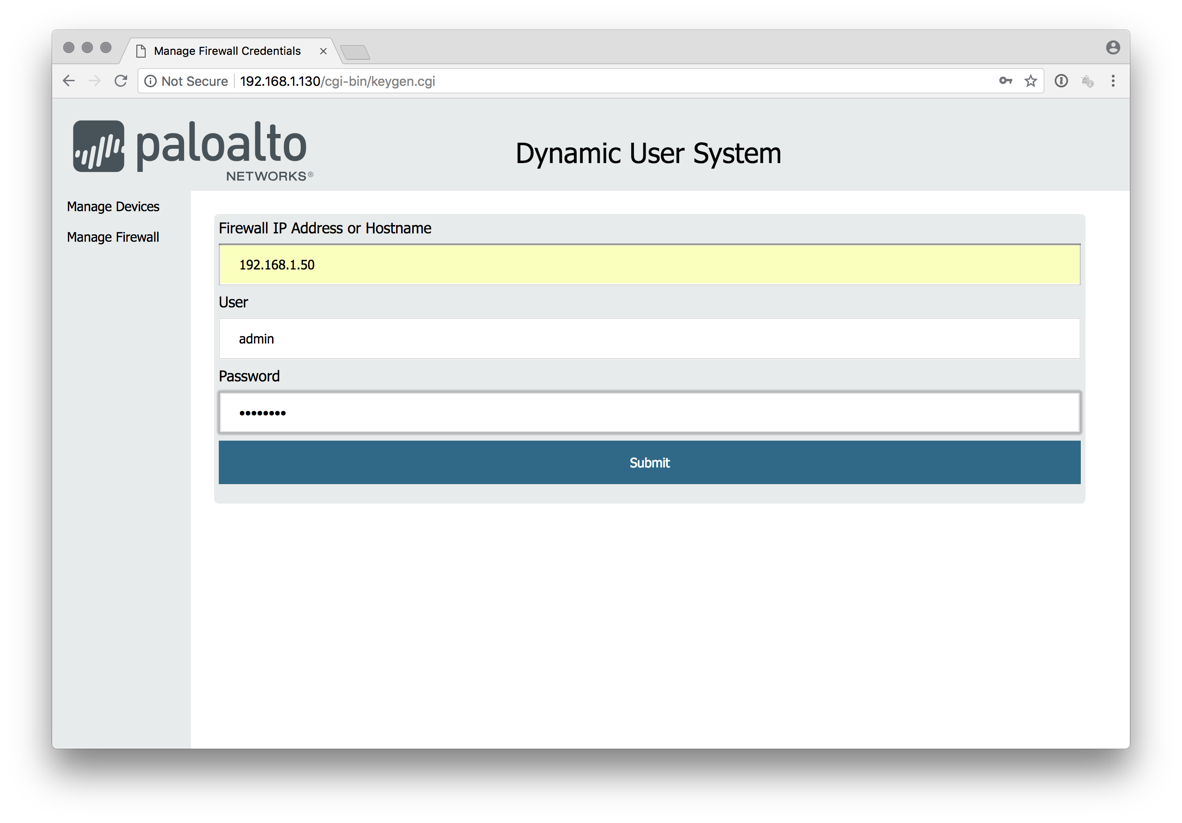
1. Click on the “Manage Firewall” navigation option



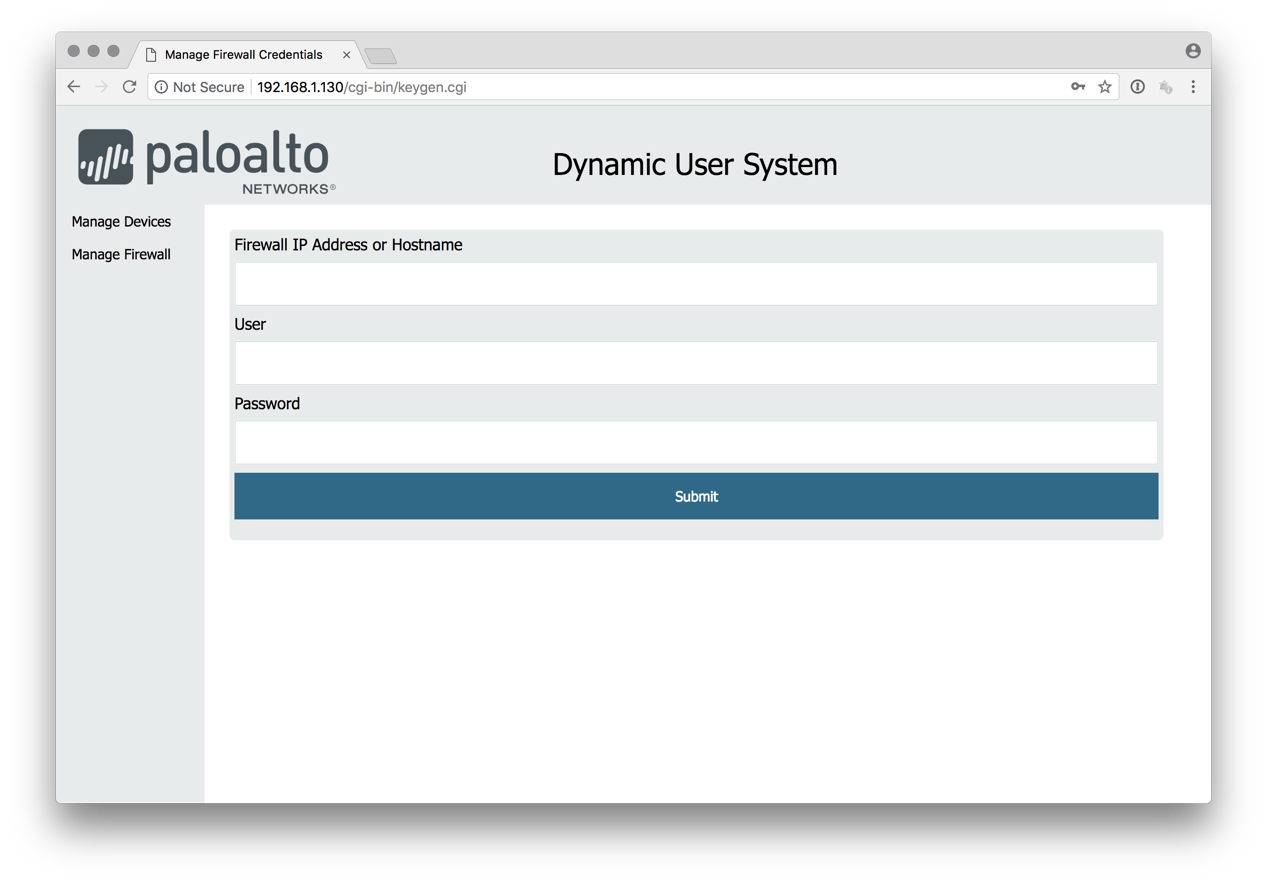
1. You should see the firewall management screen



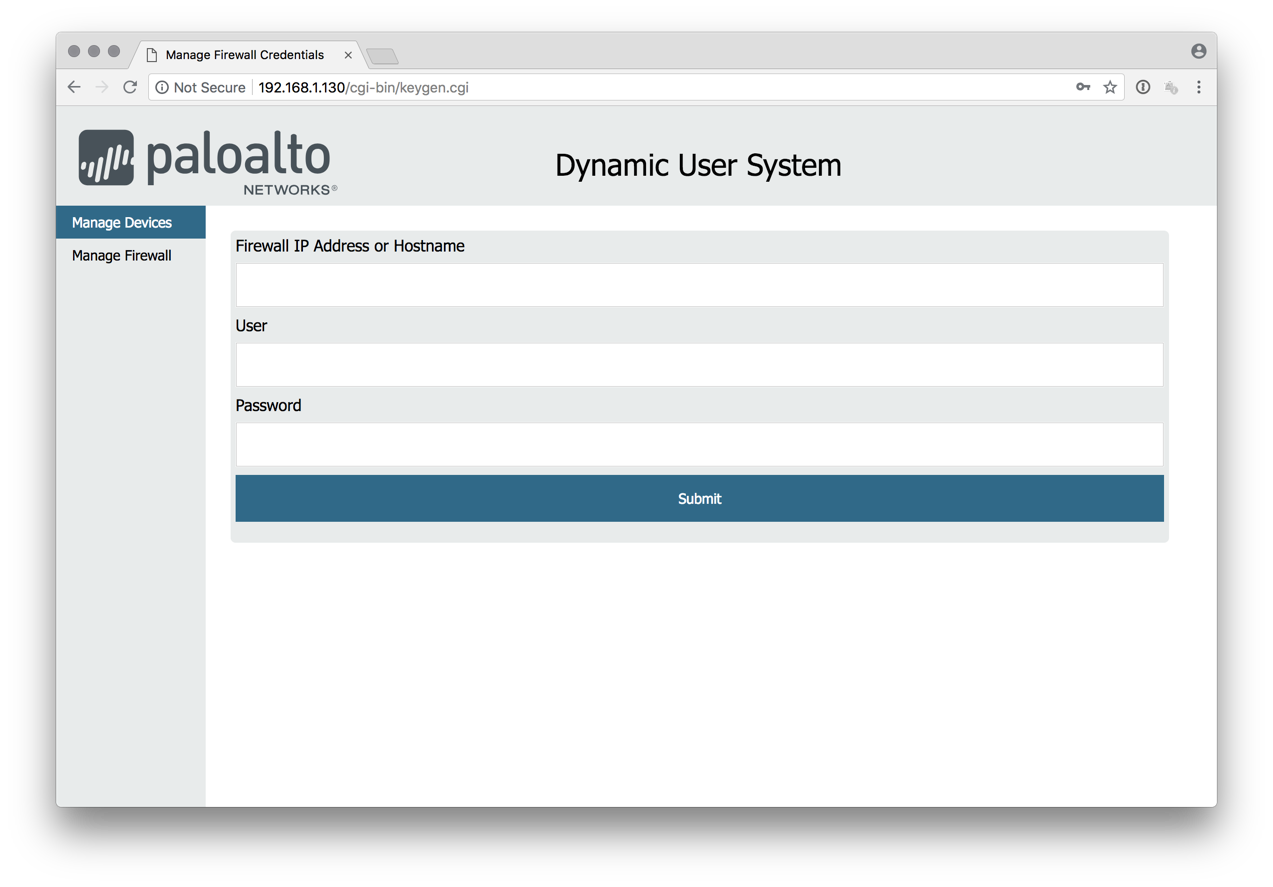
1. Enter the IP address and administrative credentials so the solution can generate an API key.



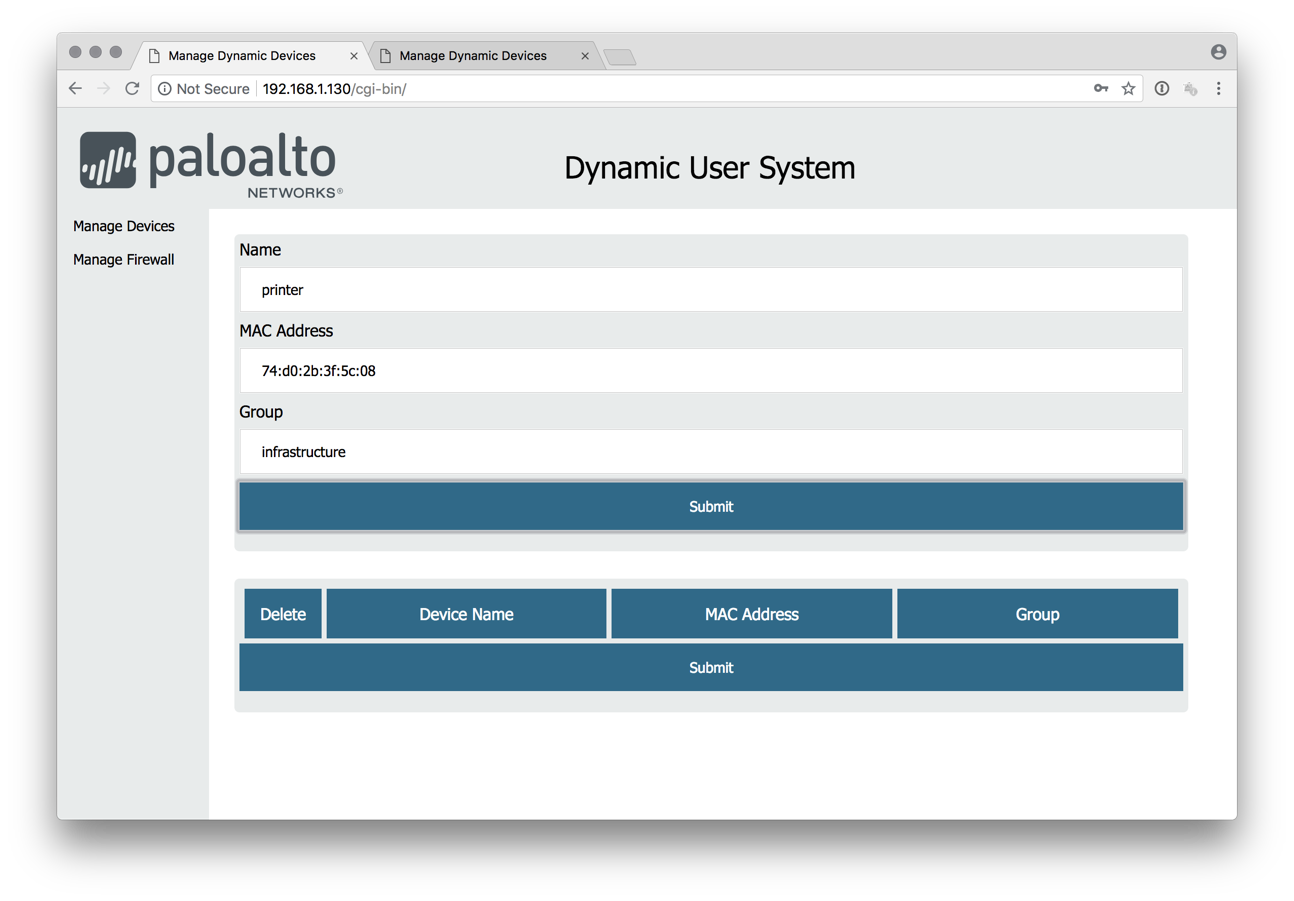
1. Once you click “Submit” you will not get a positive confirmation that the key generation was successful (maybe I can add this in a future release). You will be taken back to the “Manage Firewall” page.



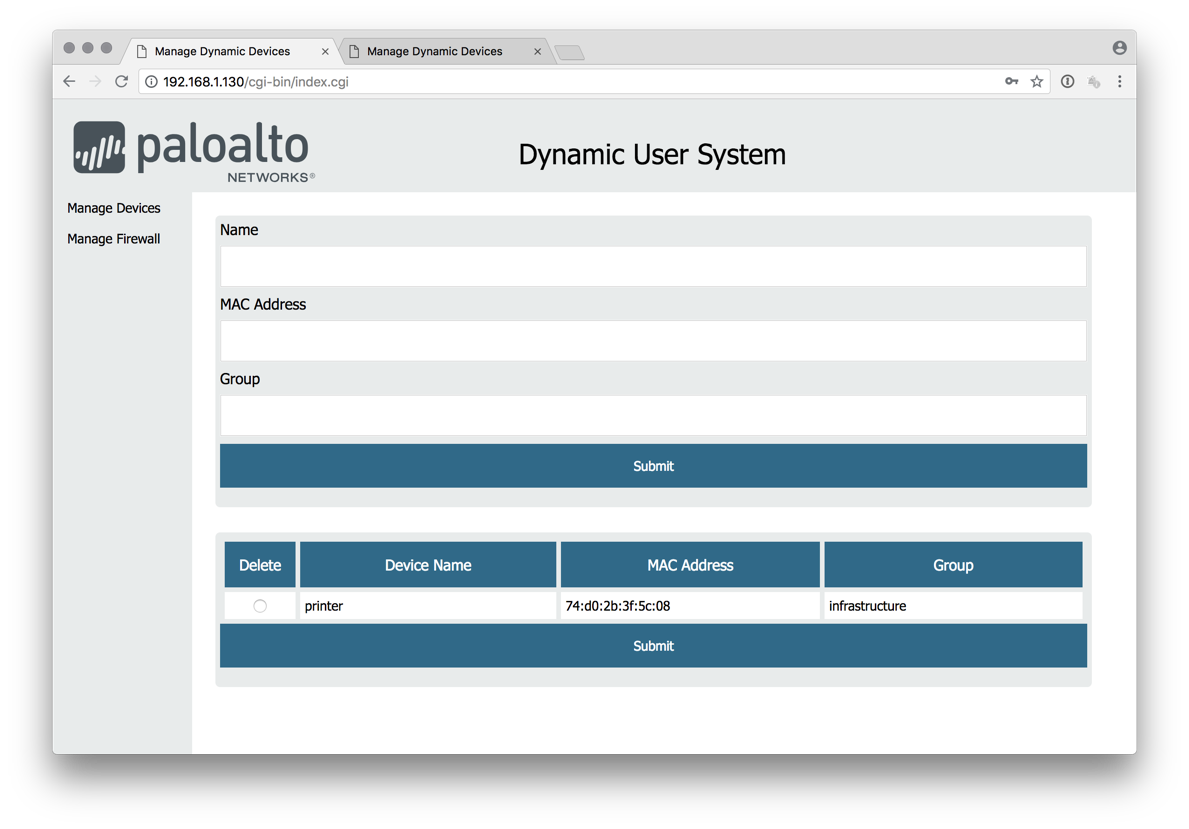
1. Click on the “Manage Devices” navigation option.



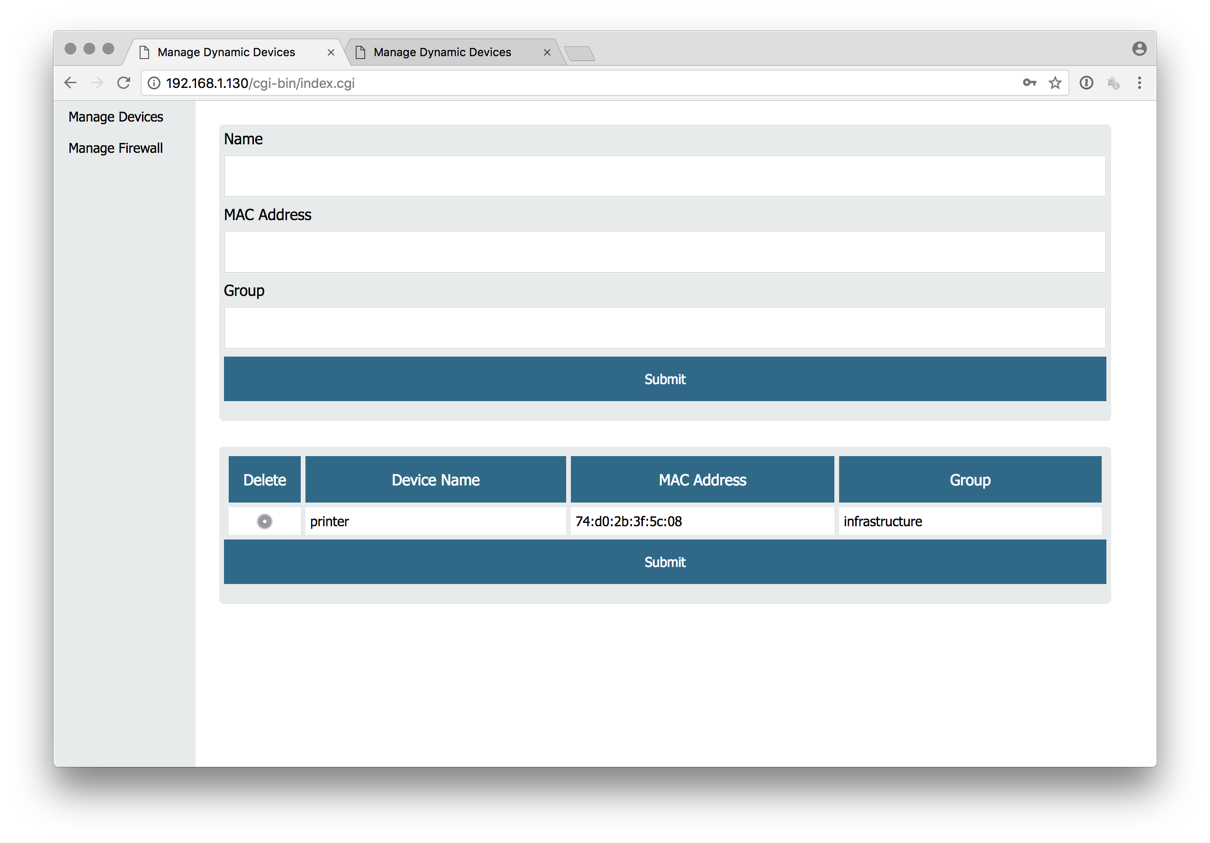
1. Add a name, MAC address, and group membership information for a device on your network.



1. Once you click “Submit”, you should see that the device was successfully added to the database.



1. If you made a mistake, you can remove the device by clicking on the “Delete” radio button next to the device and clicking “Submit”.



1. Ensure that you are using the DHCP serive on the Palo Alto Networks Next-Gen Firewall on the networks containing the devices you want to manage.
2. Ensure the network zone containing the networks for the devices you want to manage have User Identification enabled.
3. The user groups that you create in the solution will now show up in the management gui as policy objects that can easily be managed without requiring DHCP reservations.

