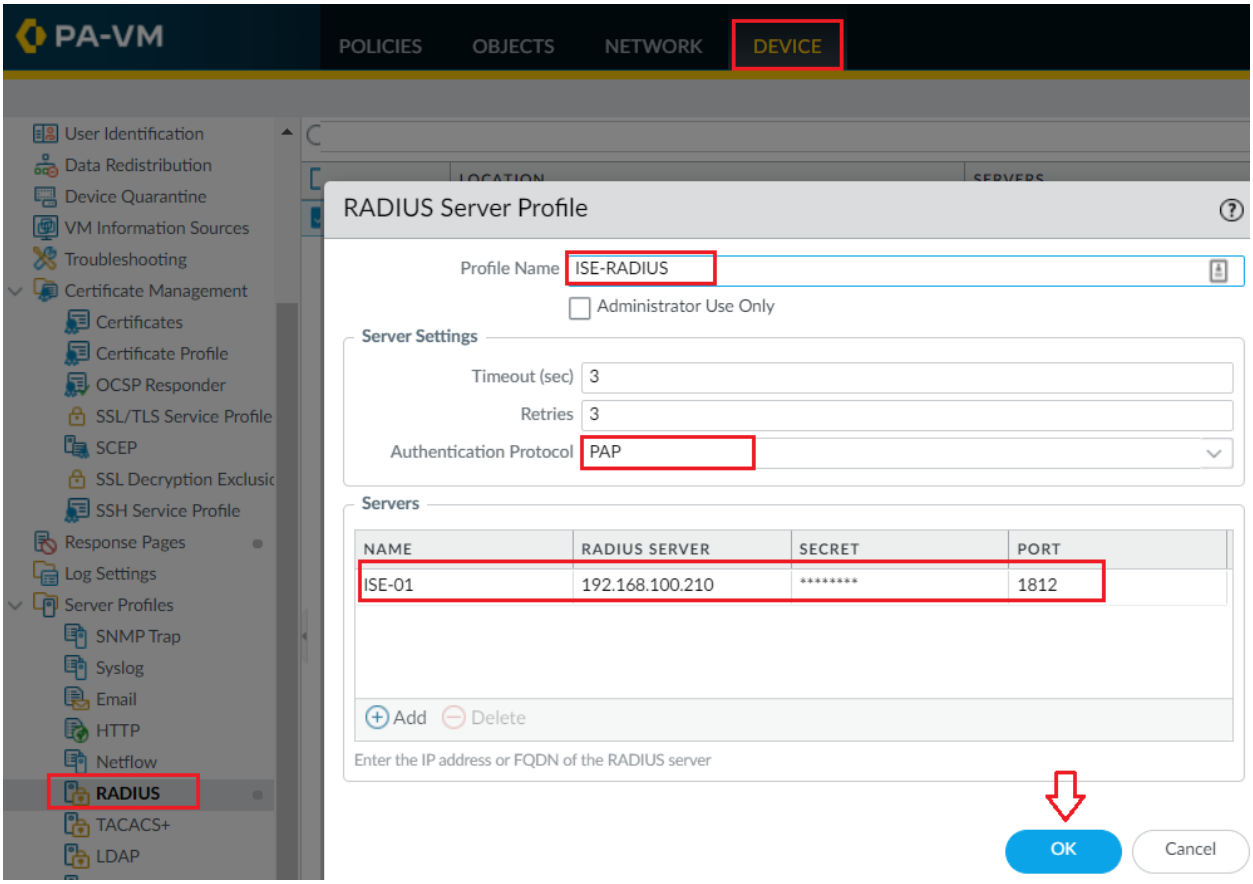
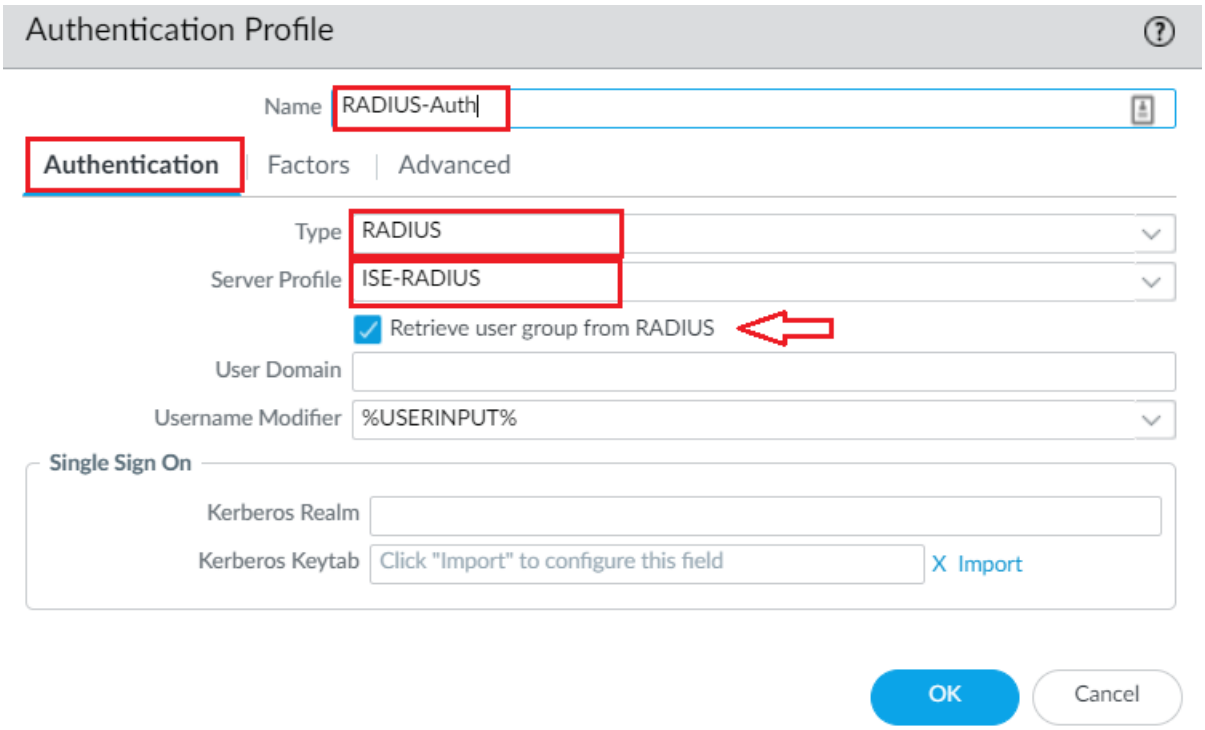
PA Firewall Configuration:

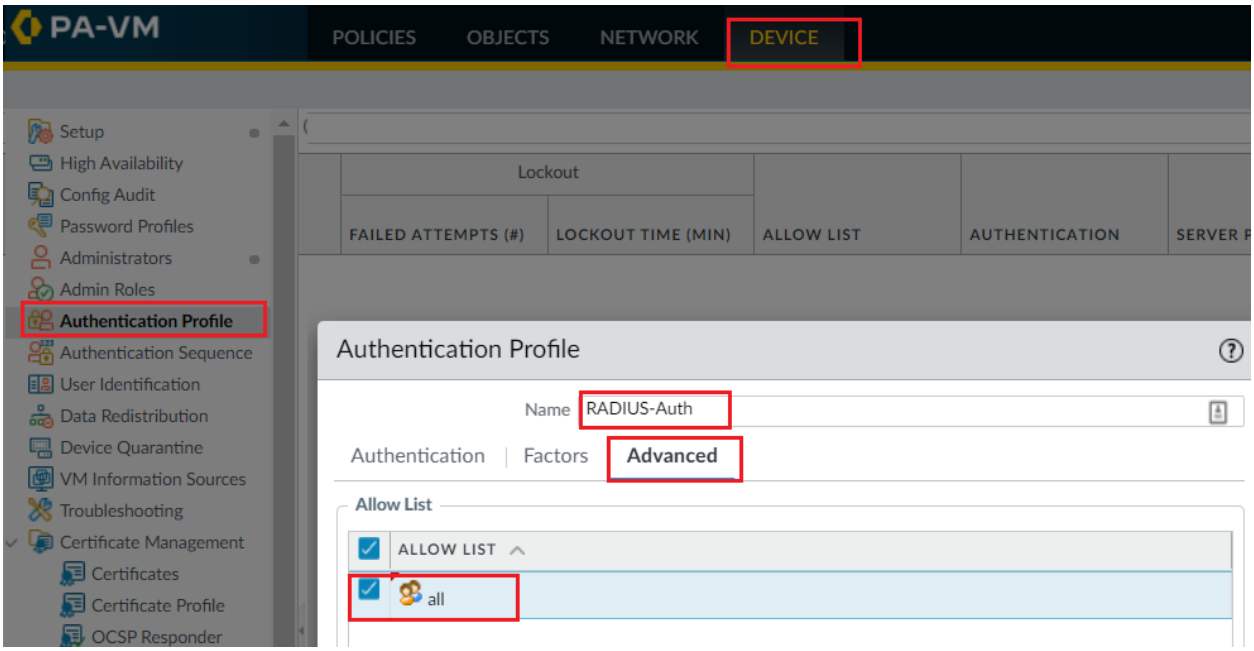
Navigate to Device > Server Profile > Radius> Add. Here to add the details of your RADIUS server. Don't forget to use the same secret key already in the RADIUS configuration. Profile Name: ISE-RADIUS can give any name you like. Choose Authentication Protocol: PAP, click add type any name you like for RADIUS Server I put ISE-01, type RADIUS Server IP: 192.168.100.210, Type Share Secret Key in my case Test123, leave the Port 1812 default. Press OK to submit.



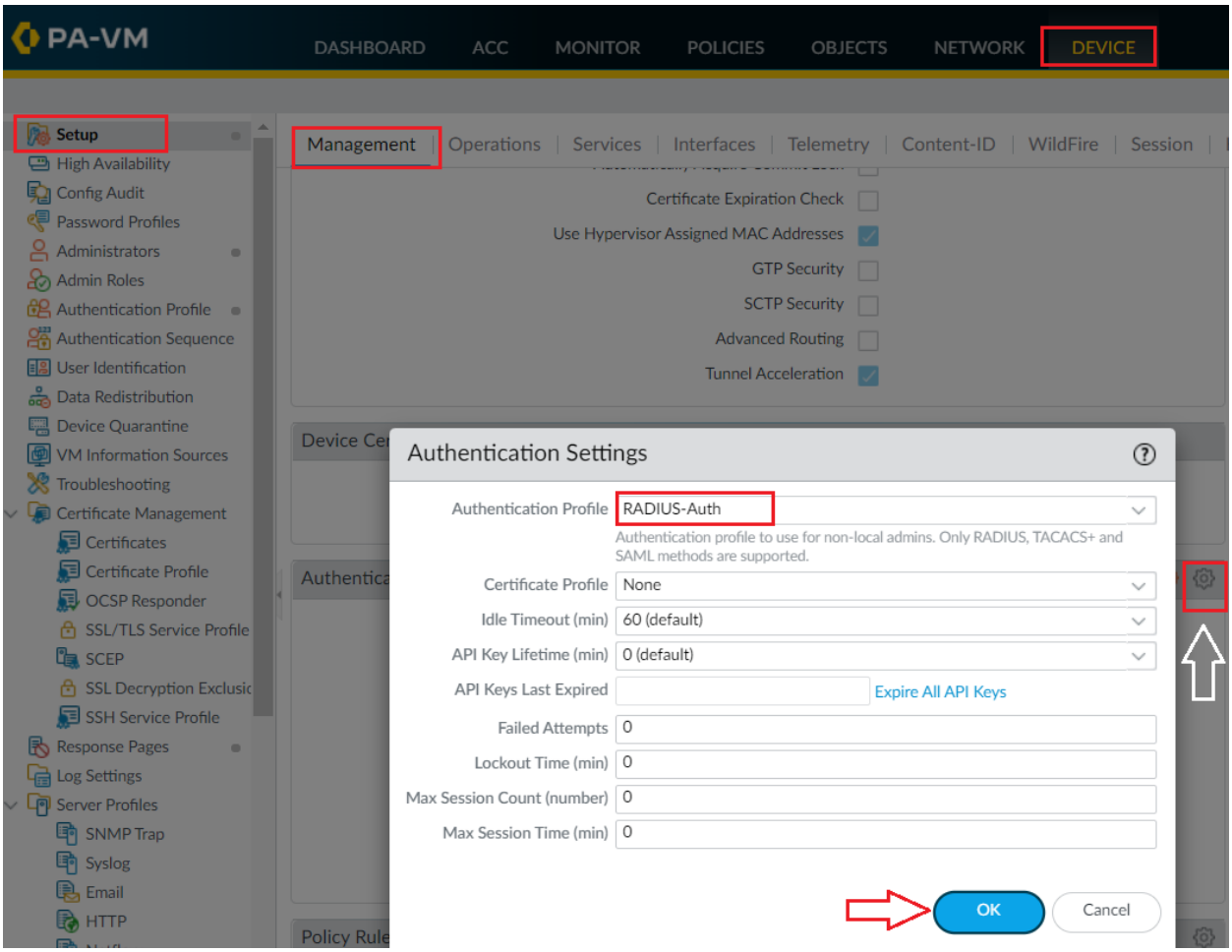
Click Device –> Authentication Profile –> Add. Here you want to make the type 'RADIUS' and choose the profile you created earlier. Give any name you like in my case RADIUS-Auth,



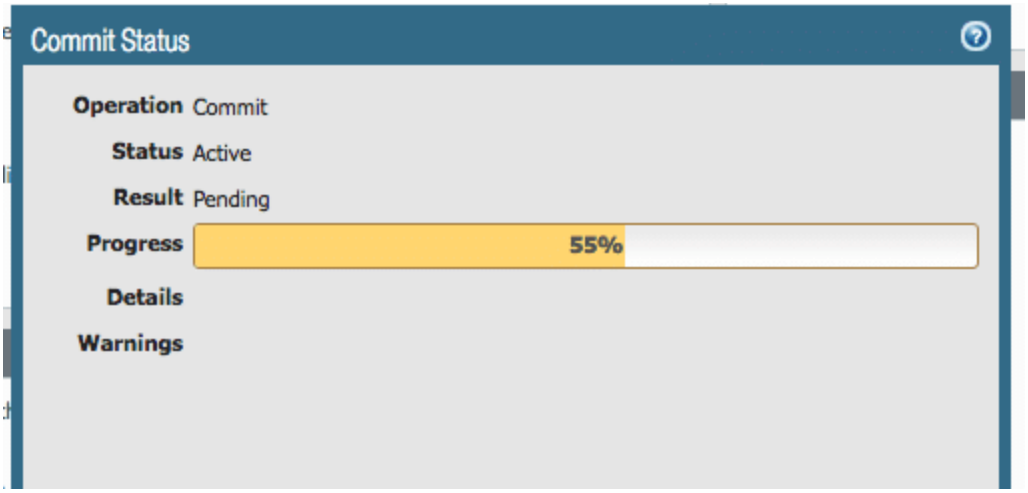
Navigate to Advanced tab click on Add button and choose all click OK to submit.



Navigate to Device > Setup > Management > Authentication Settings click on Gear Icon choose Authentication Profile RADIUS-Auth which earlier created Click OK.

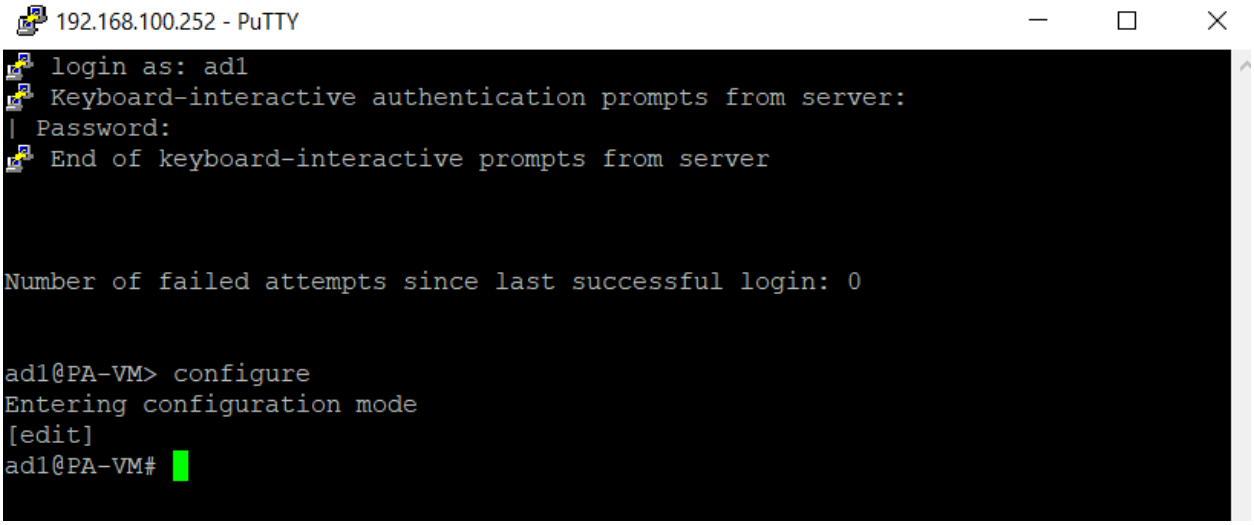


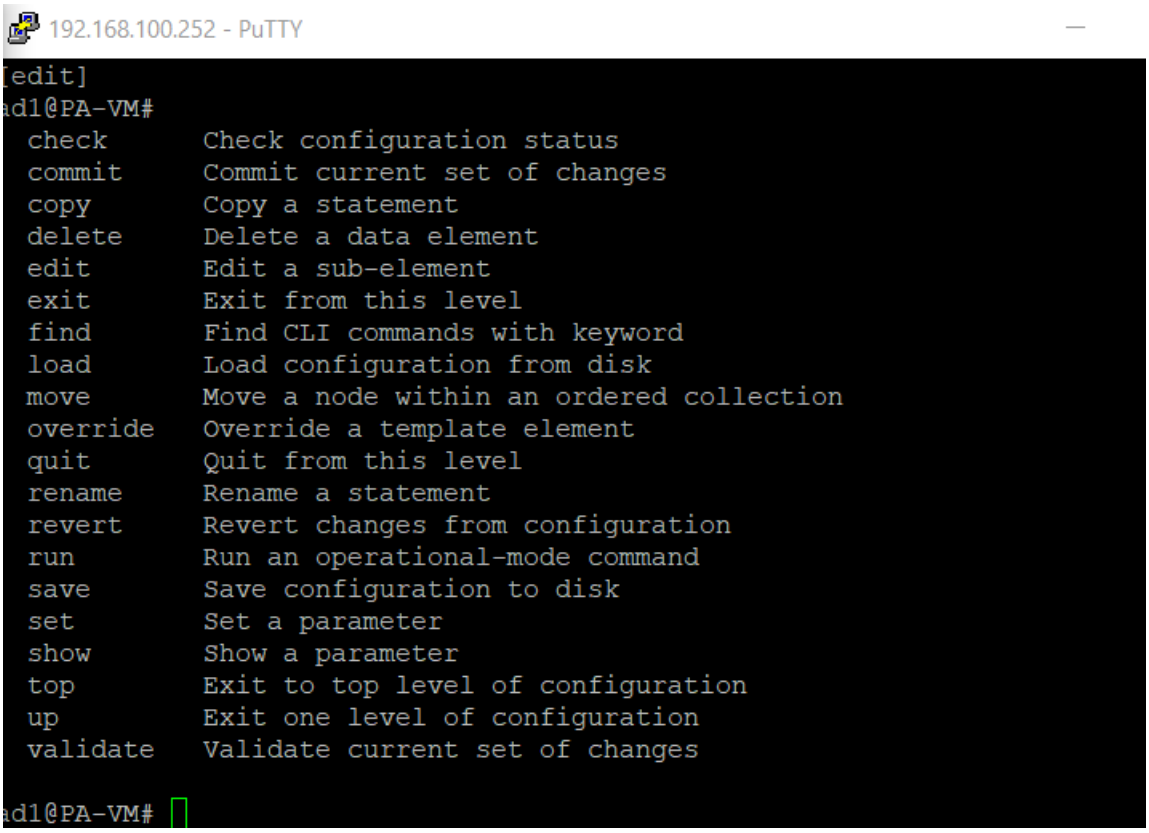
Commit the Changes by Clicking Commit on top right corner to save the configuration.

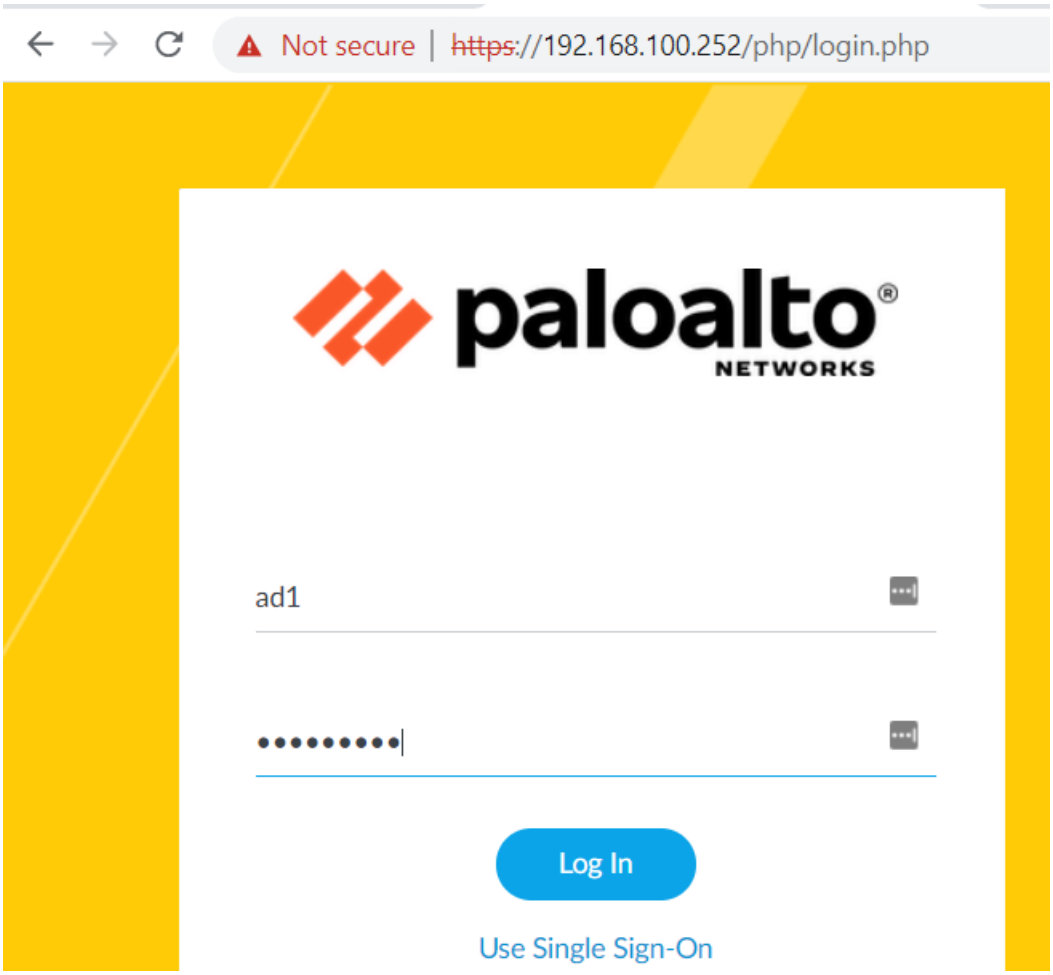


Testing and Verification:

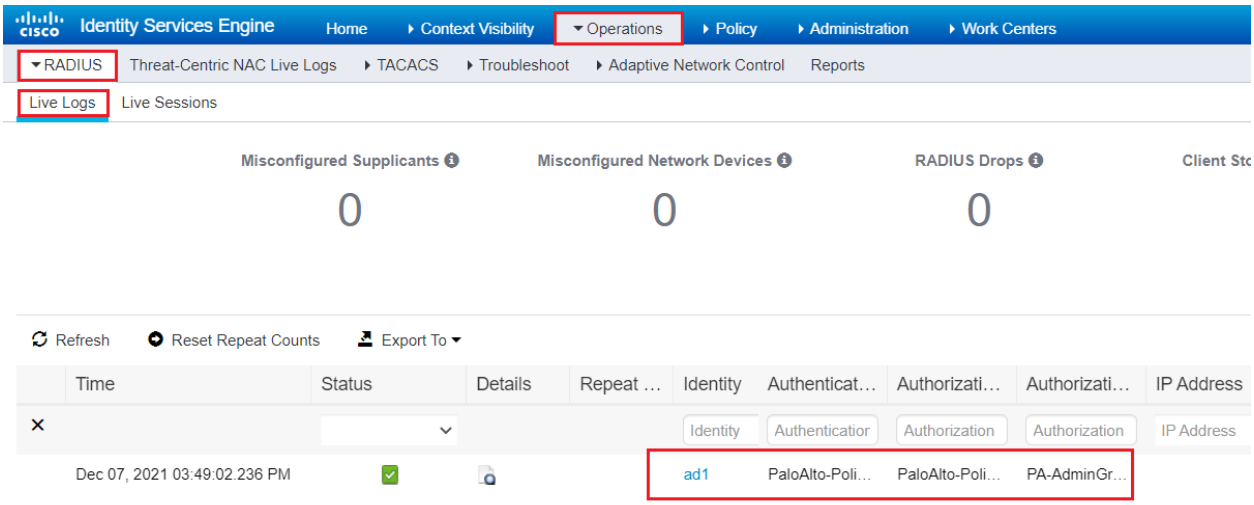
We can test our configuration by login into the Palo Alto Firewall by SSH. Let's try using the ad1 user credential.



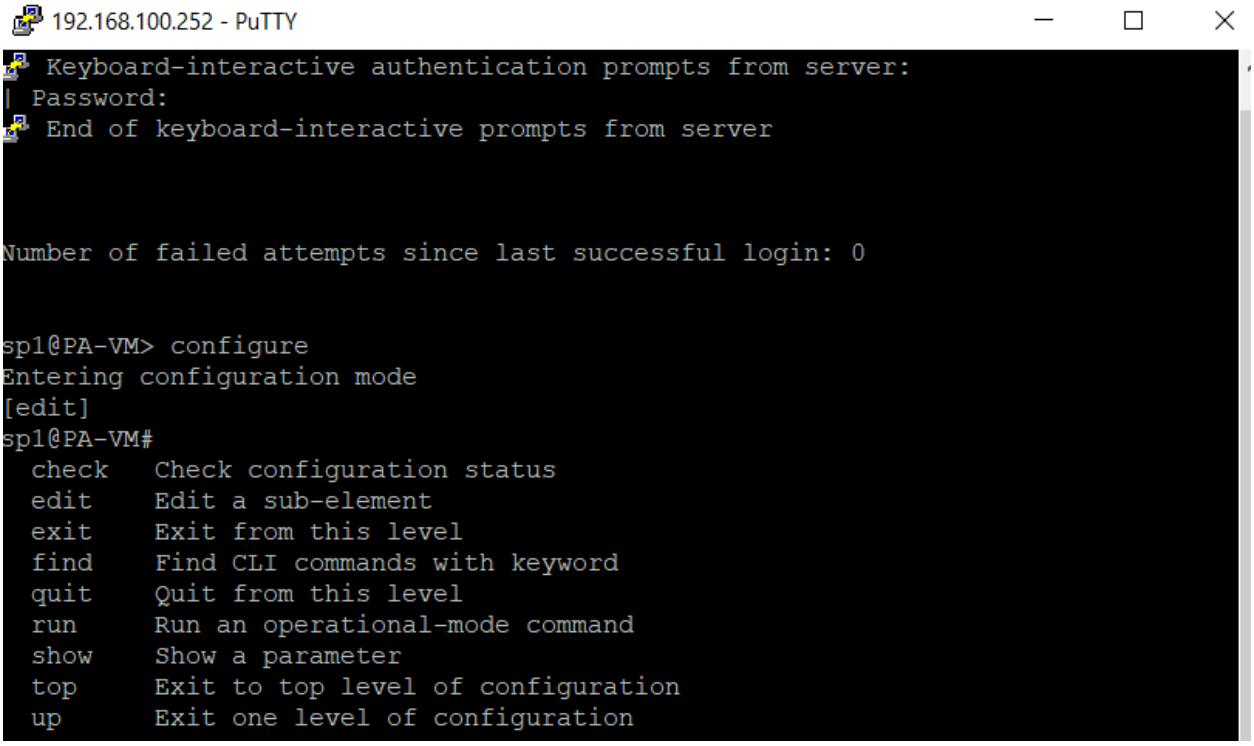


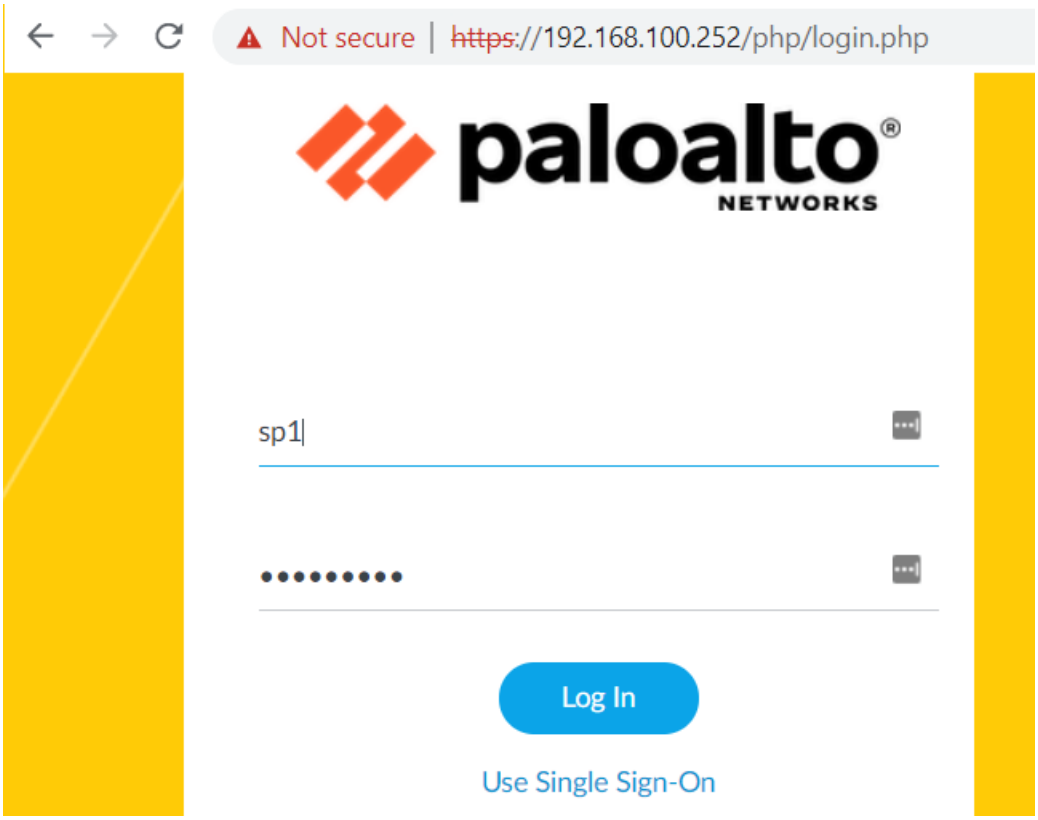


We can monitor the authentication/authorization logs on ISE Operations > RADIUS > Live Logs. The ad1 user was successfully authenticated and authorized to run privileged commands.



Now let's try again using support account users sp1. The user sp1 was successfully authenticated but wasn't authorized to run more commands.





We can monitor the authentication/authorization logs on ISE Operations > RADIUS > Live Logs.