HOWTO – Custom Configuration monitoring (fortiweb example)

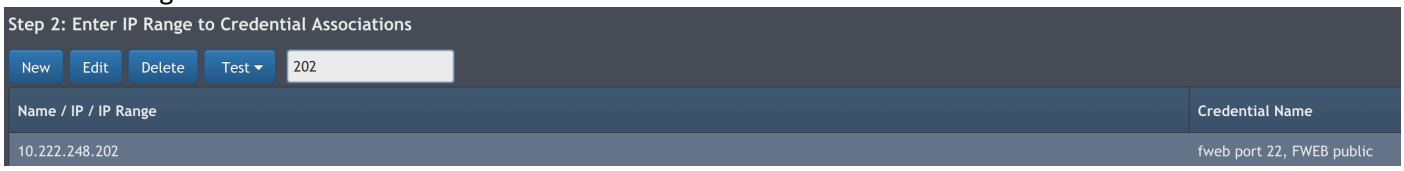
Contents

Custom Configuration Monitoring..... 2

Custom Configuration Monitoring

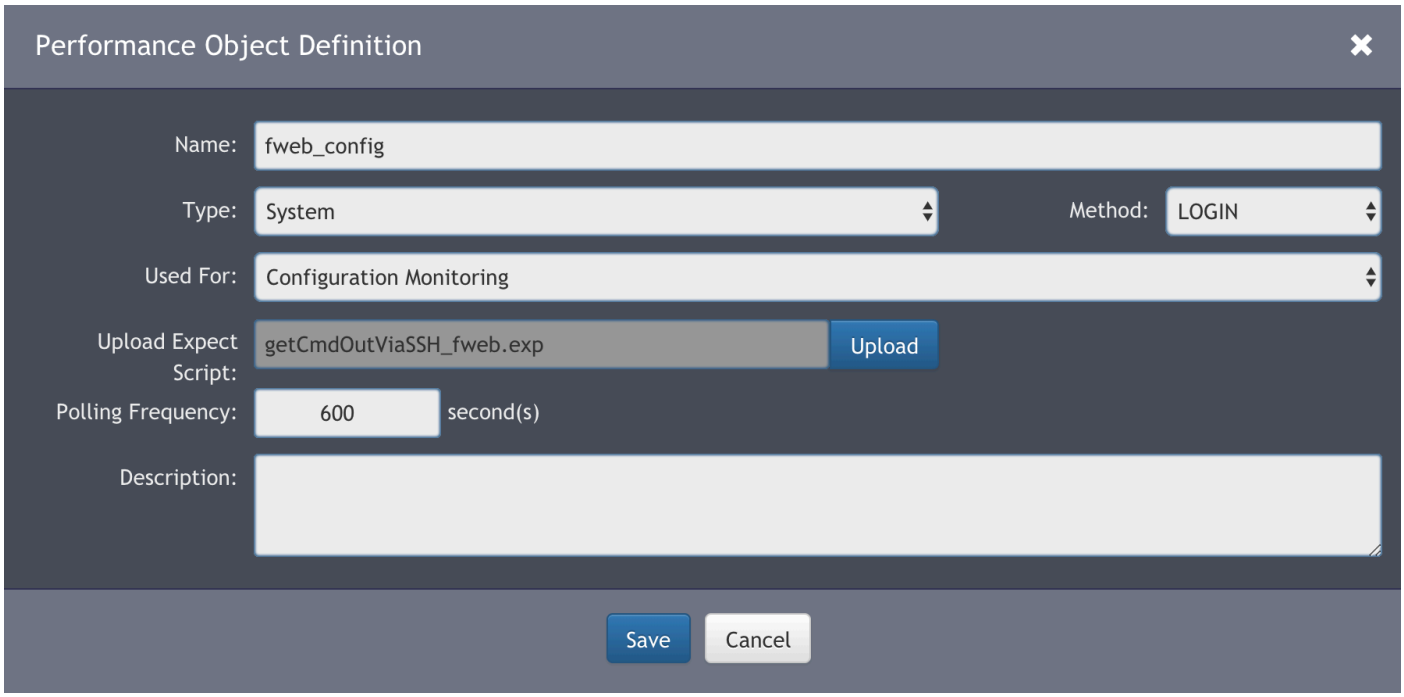
FortiSIEM has feature in place to enable monitoring of any configuration file from any device, using the LOGIN method (SSH). This example will walk you through the steps to import the FortiWeb configuration (currently not supported out of the box – expected for Release 5.2)

1. Go to Admin / Setup / Credentials and Add SNMP and SSH credentials for your FortiWeb and assign them to the FortiWeb IP.



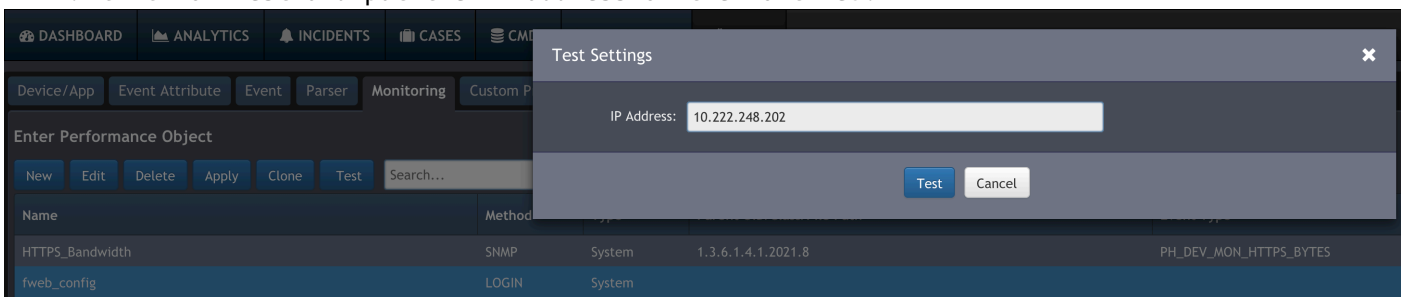
2. Download the following expect script from Egnyte:
   getCmdOutViaSSH_fweb.exp
   Password: jzXTE9m9
   https://fortinet.egnyte.com/dl/clk0bKoQSC

3. Go to Admin / Device Support / Monitoring / Enter Performance Object / New

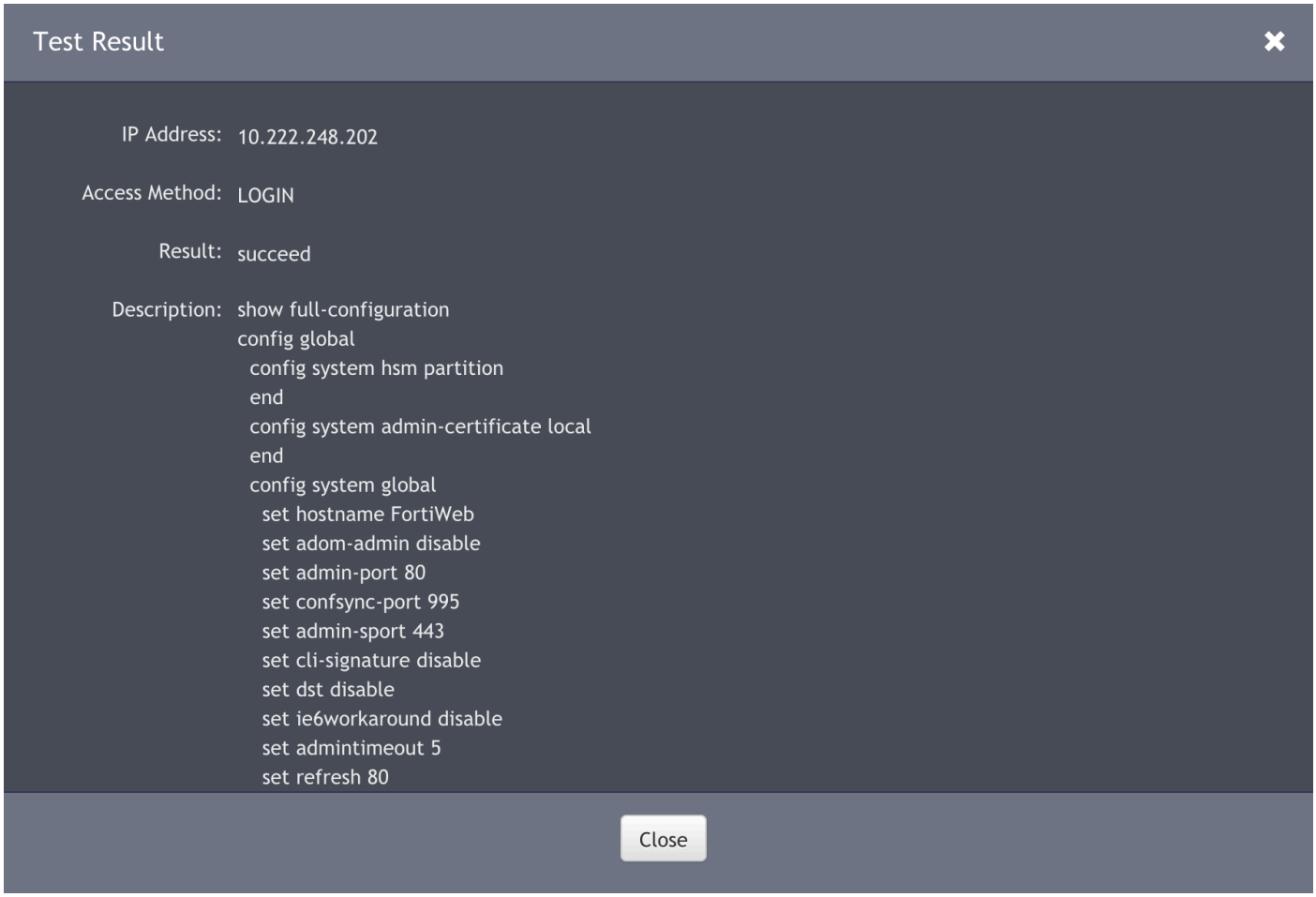


Click Save once you've uploaded the file. You can change the polling frequency to whatever you like (it affects how often we connect to the fortiweb and execute "show full-configuration")

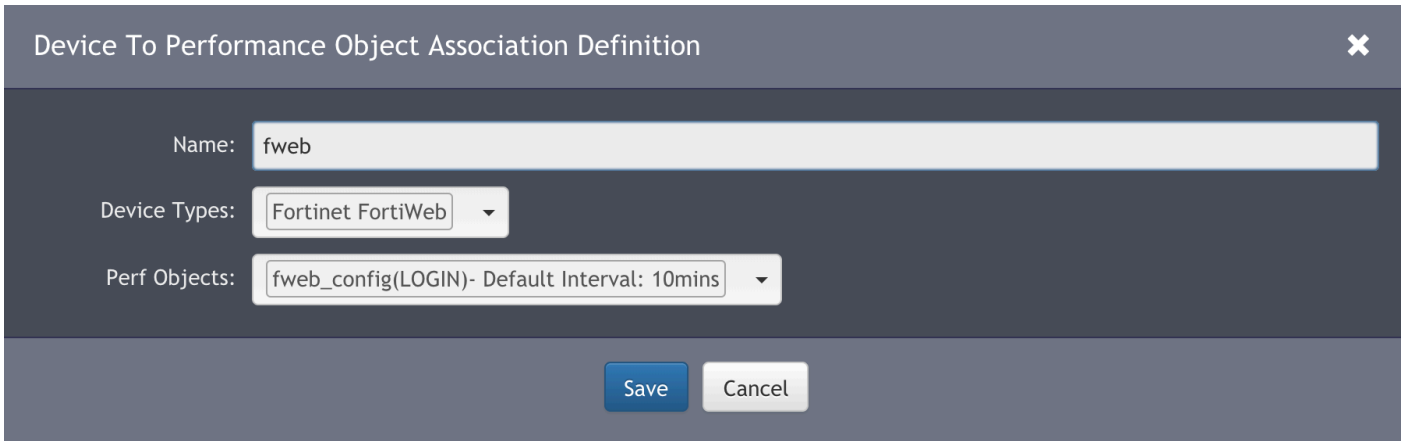
4. Click on Test and put the IP address of the Fortiweb:



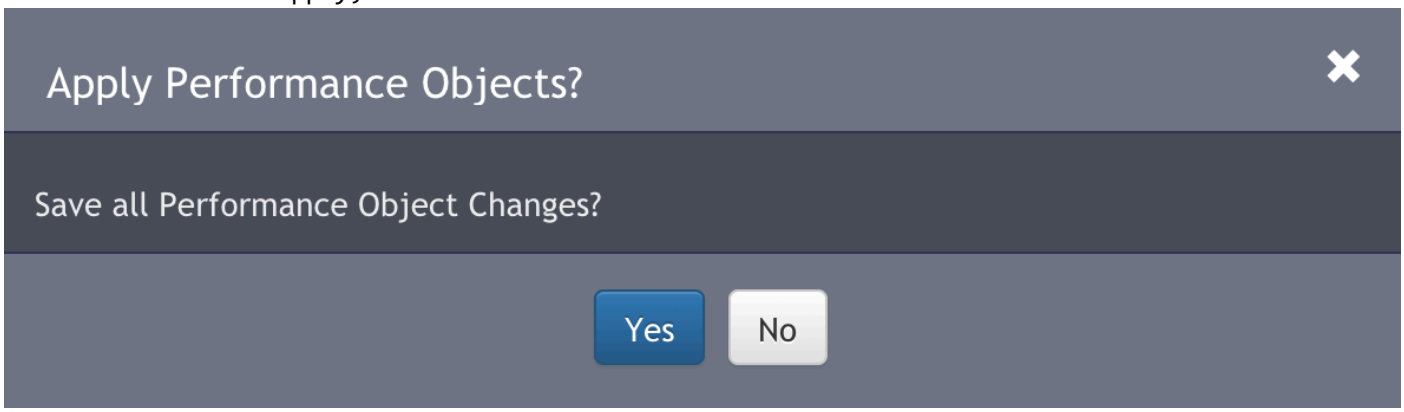
If successful, you should have a similar output:



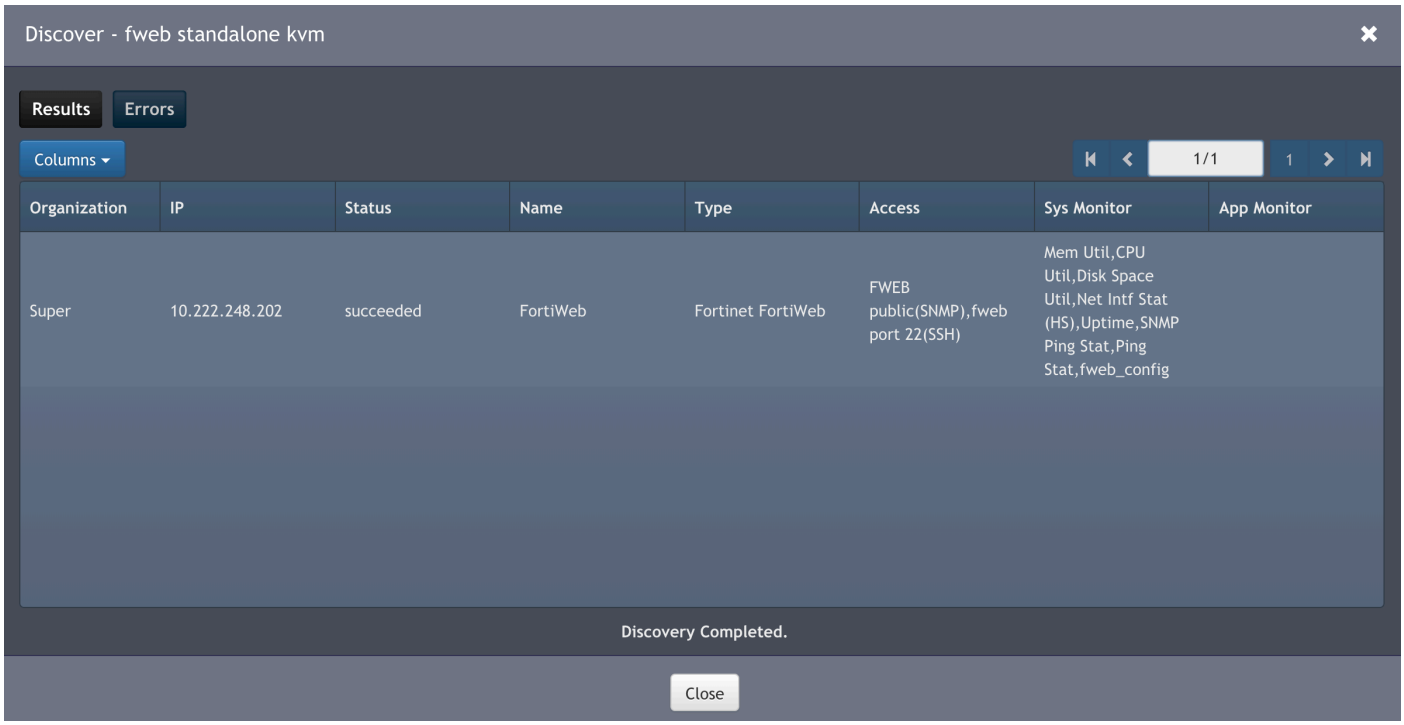
5. Create a new Device Type to Performance Object Association:



6. Click Save. Apply, Yes:



7. Go back to Admin / Setup / Discovery and discover your FortiWeb:



If you see the new fweb_config sysmonitor being applied, it means it will start pulling configuration from the fortiweb shortly.

If, by any chance, your FortiWeb is identified as a FortiOS, it is because your FortiWeb model is not mapped into the /opt/phoenix/config/systemSnmpSysObjId.csv file.