



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.

Step 2: Enter IP Range to Credential Associations

New Edit Delete Test 202

Name / IP / IP Range	Credential Name
10.222.248.202	fweb port 22, FWEB public

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

Performance Object Definition

Name: fweb_config

Type: System Method: LOGIN

Used For: Configuration Monitoring

Upload Expect Script: getCmdOutViaSSH_fweb.exp Upload

Polling Frequency: 600 second(s)

Description:

Save Cancel

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 fortieweb and execute “show full-configuration”)



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

Name	Method
HTTPS_Bandwidth	SNMP	System	1.3.6.1.4.1.2021.8	PH_DEV_MON_HTTPS_BYTES
fweb_config	LOGIN	System		

If successful, you should have a similar output:

IP Address: 10.222.248.202

Access Method: LOGIN

Result: succeed

Description: show full-configuration
 config global
 config system hsm partition
 end
 config system admin-certificate local
 end
 config system global
 set hostname FortiWeb
 set adom-admin disable
 set admin-port 80
 set confsync-port 995
 set admin-sport 443
 set cli-signature disable
 set dst disable
 set ie6workaround disable
 set admintimeout 5
 set refresh 80

Close

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



Device To Performance Object Association Definition ✕

Name:

Device Types:

Perf Objects:

6. Click Save. Apply, Yes:

Apply Performance Objects? ✕

Save all Performance Object Changes?

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

Discover - fweb standalone kvm ✕

Results

Columns 1/1 1

Organization	IP	Status	Name	Type	Access	Sys Monitor	App Monitor
Super	10.222.248.202	succeeded	FortiWeb	Fortinet FortiWeb	FWEB public(SNMP), fweb port 22(SSH)	Mem Util, CPU Util, Disk Space Util, Net Intf Stat (HS), Uptime, SNMP Ping Stat, Ping Stat, fweb_config	

Discovery Completed.

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