Quantum IoT Controller | Cheat sheet

/opt/CPvsec-R80.40/conf	Content	IoT Policy Layer	Components
Commonprotocols.JSON	Discovered protocols	IoT Access Policy	IoT Access Policy (destined to get the IoT Policy layer)
IotIpsProtections.JSON	IPS signatures configured in the IoT Threat Prevention Protection	IoT Threat Prevention Policy	IoT Threat Prevention Policy
IotPolicyConfgurations.JSON	All components of the IoT Policy Layer	IoT Threat Prevention Profile	IoT Threat Prevention Protection
IotTags.conf	Tags shared with us by Discovery Service	Web-socket API	JSON API, using TLS 1.2
PolicyconverterConf.JSON	Commonprotocols.JSON	Every 24 hours (hard coded)	Asset pull from management
Crs.xml	List of of all delivered hotfixes	IoT API sk121360	IoT API v1.6
Iot_datastore.dat	IoT Controller UUID	**IoT Controller performance indicators**	**Subject**
CloudGuard (vSEC)	**Command**	JAVA performance	IoT CloudGuard Controller
Stop and start IoT Policy process	Run vSec off and then vSec on	Consume events	Gateway ID Awareness API
Claroty TCPdump error	**Command**	ID sharing/Asset sharing	Gateway type
Machine does not have tcpdump or dumppcap!	CLI CTD: : #lm set_config force_allocate_ptty False	If you want to configure > 100K assets	sk113833
API status & info	**Elg file location**	If you want to configure < 100K assets	sk172829
IoT.elg	/opt/CPsuite-R80.40/fw1/log/iot.elg	**On-going policy push**	**Modification**
API version 1.6	sk121360	$FWDIR/conf/vsec.conf	iotdiscovery.handleFirstPolicyRequestOnly =true >>> false, Run vSEC off and then vSEC on
ID sharing	**Command**	**IotTags.conf**	**Procedure**
Check PDP and PEP processes	• # pdp m a • # pep show pdp all • # pep show user all • # pep show network pdp	/opt/CPsuite-R80.40/fw1/conf	File is not in by default. Adding and changing using Microsoft? Use dos2unix. #dos2unix ./vsec.conf
Subject	**sk's**	**Global scanner**	**vSECDIR/conf file**

Usergroup, internal user and access role	sk60701	# Global scanner config	global.scannerInterval=30
			Global.connectTimeoutInMilliseconds=30000 -> 0.5 minute
			global.readTimeoutInMilliseconds=120000 -> 2 minutes

Illegal tags	sk40179	**Discovery Service recommended policy**	**Policysource options**
Other relevant sk's	• sk170445 • sk164053 • sk163993 • sk172286 • sk172829 • sk168732	VISIBILITY_RULES, VENDOR, CHECKPOINT_BASELINE	iotdiscovery.policySource=VENDOR
IoT view & report	**Policysource options**	**IoT Controller & Quantum Spark**	**sk's**
controls.xml and views.xml	1. Copy the files on the MGMT machine to $RTDIR/smartview/db 2. Install database 3. $RTDIR/scripts/stopSmartView 4. $RTDIR/scripts/startSmartView	Quantum Spark	sk169715 sk149255 Mandatory is a static IP address on the WAN interface
IPS Tailored Safe	**sk**	**Claroty**	**Commands**
Tailored safe is reading log files from the last 7 days and proposes disabling of protections that have not matched.	sk164812	System performance and troubleshooting	• HTOP • df –h • cd /opt/icsranger or ./health_check.sh