

		Testing Company:					MAKE A COPY									
		Device bug:					Bug to include Device type, manufacturer, model, serial number & firmware version									
Test No.	Test Category	Software/Tool used for the Test	Required / Recommended PASS	Manual test off-corp (MSI)	DAQ Ready	Test on-corp (RESOURCE TBA)	Test	Observations	Implemented / Not Required	Result Pass/Fail	OnCorp test results	Other Comments	Problem Tracking ID	Notes on data used in a test	Other Comments	
Network																
1	Connection		Required	Y	Y	Y	Check the device shows no errors on the port									
2	Connection		Required	N	n/a		Does the device support MDI-X	Redstone think this is not a test required anymore		Device						
3	Connection		Required	Y	Y		Verify the device auto-negotiates connection speed									
4	Connection		Required	Y	Y		Verify the device supports full duplex - Re-word to "Does this auto-negotiate duplex & speed"	Informational								
5	Connection		Required	Y	Y	Y	Check the device has received an IP address via DHCP			Pass						
6	Connection		Required	Y	Y	Y	Verify the devices re-requests a DHCP after its comms are disconnected			Pass						
7	Connection		Required	Y	Y	Y	Verify the devices re-requests a DHCP after its lease has expired									
8	Connection		Required	Y	Y		Validate device works with second DHCP server available									
9	Connection		Required	Y	Y		Verify the device obtains a new IP address when the DHCP server address is changed									
10	Connection		Recommended	Y	Y	Y	Verify the device send data < 5mins intervals	Informational - record								
11	Connection		Required	Y	Y	Y	Check device can be pinged			Pass						
12	Connection		Required	Y	Y		Check the device still operates correctly when DHCP Snooping and ARP inspection are running.	Valid for config template on switch								
13	Connection		Required	Y	Y	Y	In Situ: Obtain device MAC address and store it			Pass	B8:27:EB:07:1A:90					
14	Connection		Required	N	Y		Echeck-Physical device address OUI against IEEE registration- is it registered and who with?	Reward: Check MAC is not a duplicate		Pass	(Raspberry Pi Foundation)					
15	Connection		Required	Y	Y	Y	Verify mac address is unique			Pass						
16	Connection		Recommended	Y	Y	Y	Verify the device supports IPV6, SLAAC & privacy extensions	Required on roadmap and live 2019		Device						
17	Connection		Required	Y	Y	Y	Verify the device operates with comms down			Pass						
18	2nd Port Connection		Required	Y	Y		Verify second port is disabled	If Applicable		NA						
19	2nd Port Connection		Required	Y	Y		Verify second port does not request a IP once disabled	If Applicable		NA						
20	DNS		Recommended	Y	Y		Does the device allow for a DNS server to be entered automatically?	Should reference to DHCP be removed or reworded? (Yes)		Device						
21	DNS		Required	Y	Y		Verify the device connects to third parties using a Hostname?	Clare to check system testing with MSI		Device						
			Required	Y	Y		Verify the device has the ability to sync the correct time using any protocols used for time synchronisation	For IP based devices. This is a "must" in the partner security iot requirements. "Reliable clock source" NTP only required for anything related to certificates.								
22	Network Time		Recommended	Y	Y		Does the device support: RFC 5905 - Network Time Protocol Version 4: Protocol and Algorithms Specification	For IP based devices. This is a "must" in the partner security iot requirements. "Reliable clock source" NTP only required for anything related to certificates.		Device						
23	Network Time		Required	Y	Y	Y	Check NTP port 123 is disabled and the device is not operating as an NTP server	Only applicable if above test is a pass		Pass						
24	Network Time		Recommended	N	Y		Check device updates time from NTP server	This is a "must" in the partner security iot requirements		Device						
25	MUD File		Recommended	Y	Y		Is there a MUD file as specified in RFC 8520			Device						
26	MUD File		Recommended	Y	Y		Does device communication match the communication specified within the MUD file?			Device						
27	PoE		Recommended	Y	Y		Verify if the device supports POE	If Applicable		Device						
28	PoE		Required	Y	Y		Verify the device autonegotiates power requirements	If Applicable		Device						
29	PoE		Informational	Y	Y	Y	Verify if the device requires more than 15.4W of power	If Applicable								
30	Long Term Test		Recommended	Y	Y		Verify the device still communicates and shows no errors after 24hours			Device						
31	Long Term Test		Recommended	Y	Y		Verify the device still communicates and shows no errors after 7 days			Device						
32	Communication		Informational	Y	Y		Verify and record device communication (flow type) - Unicast, multicast, broadcast	Informational - if multicast needs to be flagged to network eng		Device						
33	Wireless		If applicable	Y	Y		Does the device support Wireless communication	If Applicable		Device						
34	Wireless		If applicable	Y	Y		Check the devices supports connections to WPA2-PSK	If Applicable		Device						
35	Wireless		If applicable	Y	Y		Verify the devices supports 802.11g-2003 - Wireless communication extended throughput up to 54Mbps in 2.4Ghz Band	This is a "must" IEEE 802.11i in partner security iot requirements		Device						
36	Wireless		If applicable	Y	Y		Verify the devices supports 802.11n-2009 - Wireless communication extended throughput up to 600Mbps in 2.4 or 5Ghz band	must be lab deploy for 2 years		Device						
37	Wireless		If applicable	Y	Y		Verify the devices supports 802.11ac-2013 - Wireless communication extended throughput up to 1Gbps in 5Ghz band	If Applicable		Device						
38	Wireless		If applicable	Y	Y		Verify if the devices acts as a AP, if it supports hidden SSID and if this functionality can be disabled	If Applicable		Device						
Security																
39	Basic Security		Required	Y	Y		Perform port scan and output all ports that are enabled	Identify all ports that are enabled		Device						
40	Basic Security	nmap	Required	Y	Y		Ensure the following ports are disabled: FTP port 20/21 TELNET port 23 SMTP port 25 TFTP port 69 HTTP port 80 POP port 110 IMAP port 143 SNMP port 161/162 VNC	UDP often used for device firmware upgrade SNMP may be needed for network monitoring	REVIEW WITH CARE	Device	Worked					
41	TLS	Nessus	Required	Y	Y		Verify the device supports TLS 1.2 or above (as a client)			Passed	pass					
42	TLS	Nessus	Recommended	Y	Y		Verify the device support TLS 1.3?	Preferred Compliance		Device	fail					
43	TLS		Required on roadmap and live 2019	Y	Y		Does the device support EAP-TLS?	Required 2019		Device	future					
44	Access Control		Required on roadmap and live 2019	Y	Y	Y	Verify the devices supports 802.1x-2001 - Port Based Network Access Control	Required 2019 - Confirm requirement with Google		Future						
45	Access Control		Required on roadmap and live 2019	Y	Y	Y	Verify the devices supports RFC 2459 - Internet X.509 Public Key Infrastructure Certificate and CRL Profile	Required 2019		Device						
46	Security		Required	Y	Y		Verify the device default passwords are changeable			device						
47	Security		Required	Y	Y		Insitu: Verify all default password have been reset. Ensure new Google provided passwords are set			device						
48	Security		Recommended	Y	Y		Verify a login trap ia in place to prevent multiple failed logins			device						
49	Security		Required	Y	Y		Verify the device does not require a Java plugin	Not preferable		device	pass					
50	Security		Required	Y	Y		verify the device does not require flash	Not preferable		device	pass					
51	Security		Required	Y	Y		Verify the device uses https and not http	Preferable		device	pass					
52	Security		Required	Y	Y		Verify the device is not impacted when Storm control is implemented			device						
Device functionality																
53	IoT System functionality		Recommended	Y	Y		Verify Device data is plotting on the server									

			MAKE A COPY												
Testing Company:															
Device bug:			Bug to include Device type, manufacturer, model, serial number & firmware version												
Test No.	Test Category	Software/Tool used for the Test	Required / Recommended PASS	Manual test off-corp (MSI)	DAQ Ready	Test on-corp (RESOURCE TBA)	Test	Observations	Implemented / Not Required	Result Pass/Fail	OnCorp test results	Other Comments	Problem Tracking ID	Notes on data used in a test	Other Comments
54	IoT System functionality		Recommended	Y			Verify the devices shows as offline in Cloud when disconnected								
55	IoT System functionality		Recommended	Y			Verify the devices shows as online in Cloud when reconnected								
56	IoT System functionality		Recommended	Y			Verify Device data is replotting on the server after disconnection and if disconnection is recorded								
57	IoT System functionality		Recommended	Y			Verify device peer to peer communication where required								
58	IoT System functionality		Required	Y			Verify device alarms received by server								
59	IoT System functionality		Required	Y			Verify device control signals transmitted/received								
60	IoT System functionality		Required	Y			Each device is discovered by server								
61	Protocol		Required	Y			Verify BacNet Traffic is compliant	If Applicable							
62	Protocol		Required	Y	Y		Verify Bacnet traffic is compliant to the PIC statement	If Applicable							
63	Protocol		Required	Y	Y		Insitu: Verify and record version of Bacnet used by the device	If Applicable							
BOS & IoT FUNCTIONALITY															
64	BOS functionality		Recommended	Y		Y	Verify if the device supports MQTT								
65	BOS functionality		Recommended	Y		Y	Verify if the device support MQTT v3.1.1								
66	BOS functionality		Recommended	Y		Y	Cloud IoT data matches server data								
67						Y	Verify MQTT packet vs validator	For future testing							
68	BOS functionality		Recommended	Y		Y	Device registered in Cloud IoT								
69	BOS functionality		Recommended	Y		Y	Device traffic seen in Cloud IoT								
70	BOS functionality		Recommended	Y		Y	JSON format file over MQTT								
71	IoT System functionality		Recommended	Y		Y	Verify if the devices supports coap								
72	Bluetooth		Recommended	Y			Verify if the device supports Bluetooth Core Specification 4.x & addendums	Preferred Compliance - Check for version 5?							

