DFS device channel plan and software operational declaration

Date: 2019-05-06

We, **SonicWall Inc.**, declare that the device, FCC ID: 2AKCZ-0D0 Model Name: **APL45-0D0**, does not operate Ad Hoc on "non-US frequencies" and/or on"DFS frequencies". When in role as Access Point (master to client(s)) or as Mesh Point (node in mesh network) installed software complies with per FCC 905462 D02 DFS UNII DFS V02. This includes restriction on transmissions for beacons and support for mesh nodes on Mesh Point to Mesh Point. Operation as Access Point Master and Mesh Point are concurrent.

Below is the channel / frequency plan for the device:

CH	1	2	3	4	5	6	7	8	9	10	11
Frequency (MHz)	2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462
Scan Type	Active	Active	Active	Active	Active	Active	Active	Active	Active	Active	Active

CH	36	38	40	42	44	46	48
Frequency (MHz)	5180	5190	5200	5210	5220	5230	5240
Scan Type	Active	Active	Active	Active	Active	Active	Active

CH	52	54	56	58	60	62	64
Frequency (MHz)	5260	5270	5280	5290	5300	5310	5320
Scan Type	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh

CH	100	102	104	106	108	110	112	116	118	120	122
Frequency (MHz)	5500	5510	5520	5530	5540	5550	5560	5580	5590	5600	5610
Scan Type	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh

CH	124	126	128	132	134	136	140
Frequency (MHz)	5620	5630	5640	5660	5670	5680	5700
Scan Type	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh	Active Mesh

CH	149	151	153	155	157	159	161	165
Frequency (MHz)	5745	5755	5765	5775	5785	5795	5805	5825
Scan Type	Active	Active	Active	Active	Active	Active	Active	Active

On all US channels including US DFS channels, the WLAN functions operates under the control SonicOs user interface and/or mesh point node. The device scans all US frequencies including DFS frequencies to identify other mesh nodes device is detected. <u>The control of DFS functionality is not accessible to anyone under any conditions.</u> Furthermore, SonicWall uses Public Key Infrastructure (PKI) to authenticate source of firmware reliably. SonicWall secure signing server uses PKI private key to sign the firmware. And SonicWall appliance has PKI public key to authenticate the firmware image. Digital Signature Algorithm (DSA) and secure hashing algorithm SHA to validate only SonicWall signed legitimate firmware can be allowed for upgrading. Digest hash ensure firmware is not modified. DSA can ensure firmware is authentic

Thank you

Sincerely yours,

Rick Linford
Regulatory Compliance Engineer
SonicWall Inc.
email : rlinford@sonicwall.com
Phone : 408.962.8798
Fax Number: 408.745.9300