"Cheat Sheet"

Un-KRACK vSZ 3.5

October 2017

WPA/WPA2 Vulnerability Mitigation

Until the vSZ 3.5 patch code is available, the CVE-2017-13082 PTK Reinstallation Vulnerability can be mitigated by ensuring 802.11r is disabled on any SSID/WLAN and that Mesh is disabled on any AP.

By default, 802.11r and Mesh are disabled. Your network is safe from attack, there is nothing required to be done if those defaults are intact. Otherwise, to mitigate CVE-2017-13082 PTK Reinstallation Vulnerability, follow the instructions to disable 802.11r (on SSID/WLAN) and Mesh (on AP).

Mesh

Verify that Mesh is not enabled for your vSZ 3.5 network (this is the default setting). Navigate to Access Points and select your AP Zone. Click the Edit icon. Under Configure > Mesh, if the Enable Mesh check box is not selected, no further action is needed.

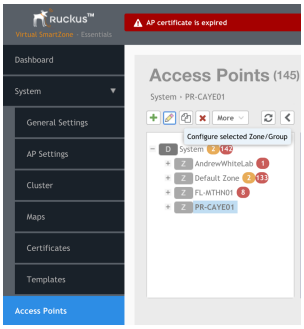

Figure 1: Mesh vSZ 3.5

Under Mesh Options, if the Enable Mesh Networking check box is not selected, no further action is needed.

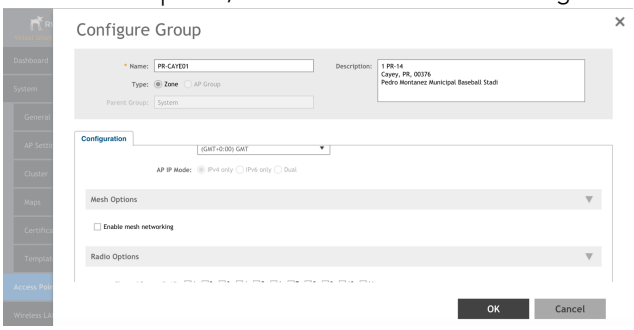

Figure 2: Mesh vSZ 3.5

If Mesh is enabled, it cannot be disabled for the system. However, the APs can have Mesh disabled. You should only do this if they are not participating in a Mesh link connection or you risk isolating any non-wired AP. To disable Mesh on each AP, select Access Points and Configure for each access point.

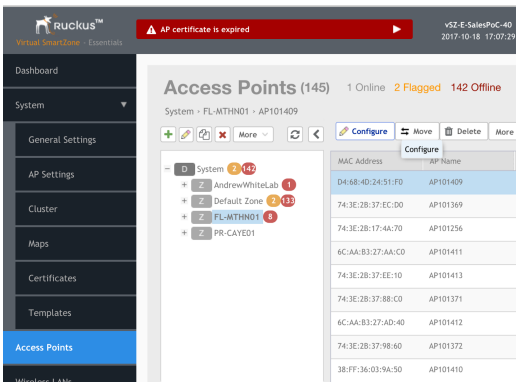

Figure 3: Mesh vSZ 3.5

Under Mesh Options, Disable Mesh Mode and save your changes.

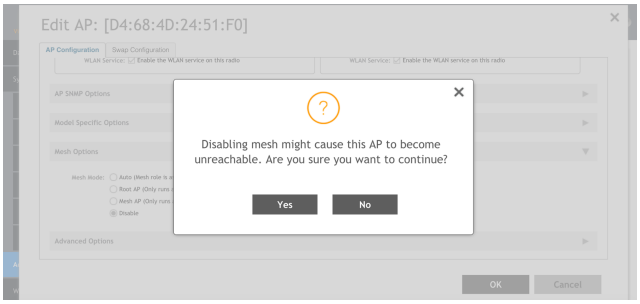

Figure 4: Mesh vSZ 3.5

802.11r (Fast Roaming)

The Fast BSS Transition (802.11r) feature is found under each Wi-Fi Network (WLAN) configured. This feature is disabled by default. To verify that 11r is not enabled for your WLAN, under WLANs > (Your WLAN Name) > Configure, if the Enable 802.11r Fast BSS Transition check box is not selected, no further action is needed. If it is, deselect it and save your changes.

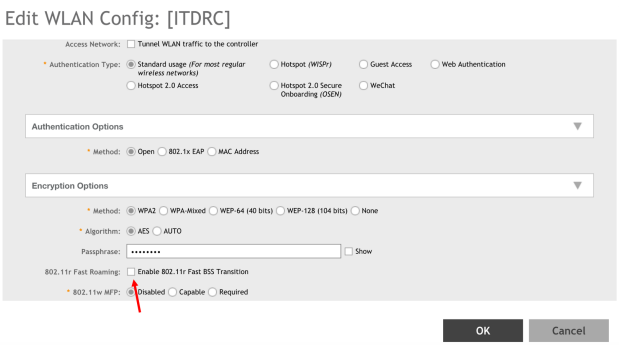

Figure 5: 802.11r vSZ 3.5