

October 2017

WPA/WPA2 Vulnerability Mitigation

Until the vSZ-H patch code for release 3.4 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-H network (this is the default setting). Navigate to your AP Zone by selecting Configuration> AP Zones> (Your AP Zone Name). In the General Information area, if Mesh is disabled, no further action is needed.

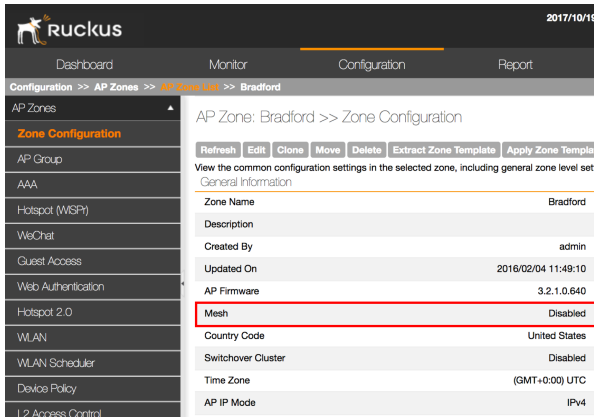


Figure 1: Mesh vSZ-H

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 Configuration> Access Points> Edit for each access point then Disable Mesh and save your changes.

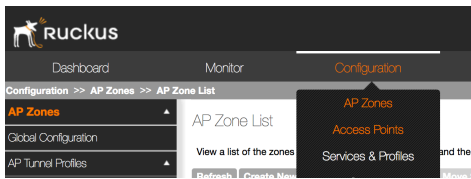


Figure 2: Mesh vSZ-H

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, navigate to Configuration > AP Zones > (Your AP Zone) > (Your WLAN Name).

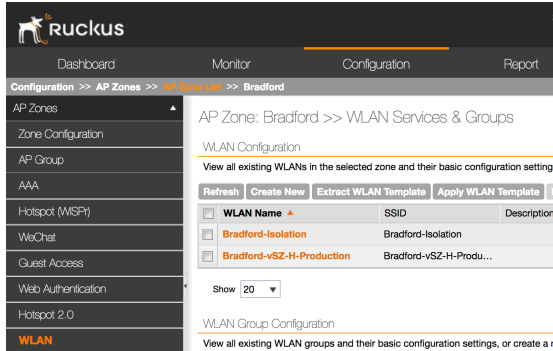


Figure 3: 802.11r vSZ-H

Select your WLAN; 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.

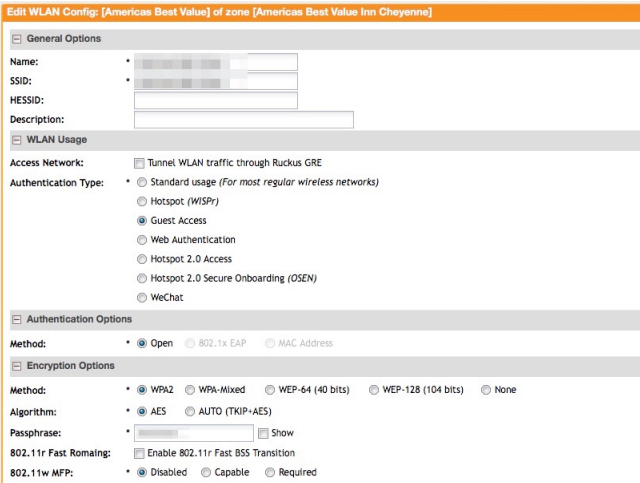


Figure 4: 802.11r vSZ-H