



Validating WLAN Mobility Security Values

- [WLAN Mobility Security Values, on page 1](#)

WLAN Mobility Security Values

For any anchoring or mobility event, the WLAN security policy values on each controller must match. These values can be validated in the controller debugs. This table lists the WLAN mobility security values and their corresponding security policy.

Table 1: WLAN Mobility Security Values

Security Hexadecimal Value	Security Policy
0x00000000	Security_None
0x00000001	Security_WEP
0x00000002	Security_802_1X
0x00000004	Security_IPSec*
0x00000008	Security_IPSec_Passthrough*
0x00000010	Security_Web
0x00000020	Security_PPTP*
0x00000040	Security_DHCP_Required
0x00000080	Security_WPA_NotUsed
0x00000100	Security_Cranite_Passthrough*
0x00000200	Security_Fortress_Passthrough*
0x00000400	Security_L2TP_IPSec*
0x00000800	Security_802_11i_NotUsed
	Note Controllers running software release 6.0 or later do not support this security policy.

Security Hexadecimal Value	Security Policy
0x00001000	Security_Web_Passthrough



Note Controllers do not support these security policies: Security_IPSec, Security_IPSec_Passthrough, Security_PPTP, Security_Cranite_Passthrough, Security_Fortress_Passthrough, and Security_L2TP_IPSec.
