

## WPA2 in CISCO 1130AG - PreSharedKey

### Assumptions:

1. SSID - configured
2. SSID – broadcasted

- Configure „cipher” to AES CCMP „Security” – „Encryption Manager” and apply it to both interfaces

Security: Encryption Manager - Radio0-802.11G

**Encryption Modes**

None

WEP Encryption Optional

Cisco Compliant TKIP Features:  Enable Message Integrity Check (MIC)  
 Enable Per Packet Keying (PPK)

Cipher AES CCMP

- Configure “Client Authentication Setting” and “Client Authenticated Key Management”. Select “Open Authentication” in “Methods Accepted”, next in “Client Authenticated Key Management” choose “Mandatory”, check “WPA” and type pre-shared key(ASCII or HEX)

**Client Authentication Settings**

**Methods Accepted:**

Open Authentication: < NO ADDITION >

Shared Authentication: < NO ADDITION >

Network EAP: < NO ADDITION >

**Server Priorities:**

**EAP Authentication Servers**

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

**MAC Authentication Servers**

Use Defaults [Define Defaults](#)

Customize

Priority 1: < NONE >

Priority 2: < NONE >

Priority 3: < NONE >

---

**Client Authenticated Key Management**

**Key Management:** Mandatory  CCKM  WPA

**WPA Pre-shared Key:** [.....]  ASCII  Hexadecimal

dzbanek