AC.L2-3.1.17

Access Control

Wireless Access Protection

"Protect wireless access using authentication and encryption."

Objectives

[a]

Wireless access to the system is protected using authentication.

[b]

Wireless access to the system is protected using encryption.

Key Discussion Points

Auth + Encryption = Both: [a] and [b] are independently evaluated — WPA2 with a strong password satisfies [a] but must also use FIPS-validated AES to satisfy [b]. Both must be demonstrated.

FIPS Validated Module: v2.13 references SC.L2-3.13.11 — using AES-256 is not enough. The hardware or software module implementing the encryption must have a current FIPS 140 CMVP certificate.

PSK vs. Enterprise: WPA2-PSK is permissible but the shared key must be rotated when any authorized user departs. WPA2-Enterprise with 802.1X is the stronger implementation for environments with staff turnover.

No Open Authentication: v2.13 explicitly states that open authentication must not be used — it authenticates any user and lacks security capabilities. This applies to guest networks that access CUI segments.

Assessment Methods

EXAMINE

Access control policy; system design documentation; procedures addressing wireless implementation and usage including restrictions; system security plan; system configuration settings and associated documentation; system audit logs and records.

INTERVIEW

System or network administrators; personnel with information security responsibilities; system developers.

TEST

Mechanisms implementing wireless access protections to the system.

AC.L2-3.1.17

ACCESS CONTROL — Wireless Access Protection

Plain English

What this control is really saying:

Knowing the Wi-Fi name is not security. This control requires that wireless access use real authentication — per-user credentials or certificates, not a shared password — and encryption that meets the FIPS standard. v2.13 explicitly ties the encryption requirement to SC.L2-3.13.11. WPA2-PSK with a shared password is permitted for small organizations but the key must change when any authorized user departs.

How it is used:

- Corporate Wi-Fi uses WPA2-Enterprise with 802.1X and RADIUS authentication — each user authenticates with their AD credentials, eliminating shared passwords on the CUI network.
- Access points are configured with AES-CCMP encryption — TKIP is disabled, and the FIPS 140-2 validated module is documented with its CMVP certificate number in the SSP.
- Default access point admin passwords have been changed and management interfaces are on a separate management VLAN inaccessible from user devices.
- Certificate-based authentication is implemented for device-level wireless authentication — device certificates are issued only to managed, domain-joined endpoints.

Real World Example

The Scenario

Acme Defense has a corporate Wi-Fi network with a single Cisco Meraki access point. The Wi-Fi uses WPA2-PSK with a password set three years ago and shared with all employees and some contractors. The same SSID and password serve guests.

What the assessor finds

The shared password is known to current and former employees and contractors. It has never been changed. Guest users connect on the same network with the same credentials. Traffic analysis would expose all communications between wireless clients. The AP admin interface still uses the default Meraki credentials.

SPRS Score Impact

3.1.1 carries a point value of 1. An acceptable use policy without monitoring is unenforceable — and monitoring without a defined authorized use baseline cannot reliably distinguish authorized from unauthorized activity.

What Good Looks Like

WPA2-Enterprise with 802.1X and RADIUS for CUI network segments, per-user authentication enforced, AES-CCMP with FIPS-validated module documented in SSP, default AP credentials changed, guest Wi-Fi isolated with encryption enforced, no open authentication on any network segment with CUI access.

Common Gaps

What assessors actually find in the field:

- ✗ **WPA2-PSK with stale shared key**
  The corporate Wi-Fi uses a shared password that former employees still know — the key has never been rotated after any departure, failing both [a] and [b].
- ✗ **WEP or open authentication**
  Legacy access points use WEP or open authentication — WEP is cryptographically broken and open authentication provides no protection at all.
- ✗ **Default AP credentials**
  Access point admin interfaces use default manufacturer credentials — these are published online for every model and provide full configuration access.
- ✗ **No FIPS validation documented**
  WPA2-AES is in use but no FIPS 140 validation has been verified — the encryption is strong algorithmically but [b] requires validated implementation.
- ✗ **Open guest network on CUI subnet**
  Guest Wi-Fi has no authentication or encryption — all guest traffic is in plaintext and the network is not isolated from CUI segments.