AC.L2-3.1.16

Access Control

Wireless Access Authorization

"Authorize wireless access prior to allowing such connections."

Objectives

[a]
Wireless access points are identified.

[b]
Wireless access is authorized prior to allowing such connections.

Key Discussion Points

Identify Before Authorizing: [a] must precede [b] — without a complete inventory of wireless access points, authorization cannot be systematically applied or verified.

Pre-Connection Authorization: [b] requires authorization before the connection is established — an open SSID that anyone can join and a retroactive review process both fail this objective.

Rogue AP Risk: Consumer routers and wireless repeaters added without IT approval are rogue access points — they bypass every perimeter control and are an immediate finding.

Guest Network Separation: Guest Wi-Fi must be completely isolated from CUI network segments — VLAN separation verified by firewall rules is the standard implementation.

Assessment Methods

EXAMINE

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

INTERVIEW

Personnel with responsibilities for managing wireless access connections; personnel with information security responsibilities.

TEST

Wireless access management capability for the system.

AC.L2-3.1.16

ACCESS CONTROL — Wireless Access Authorization

Plain English

What this control is really saying:

Every wireless access point connected to the CUI environment must be known and authorized before it accepts connections. An employee who plugs in a consumer Wi-Fi router to 'get a better signal' in the back shop has just created an unauthorized access point — and anyone within range can join the network. Authorization comes before connection, not after.

How it is used:

- All wireless access points in the CUI environment are inventoried — each one is listed in the SSP with its location, MAC address, and the individual responsible for its authorization.
- Wireless access requires 802.1X certificate-based authentication — only devices with a valid corporate certificate can connect, pre-shared passwords are not used for CUI network segments.
- Wireless IDS monitors for rogue access points and alerts the security team immediately — the alert procedure and response time are documented in the SSP.
- Guest Wi-Fi is on a completely isolated VLAN with no routing path to the CUI network — the isolation is verified by quarterly firewall rule review.

Real World Example

The Scenario

Acme Defense has a corporate Wi-Fi network. Two years ago an engineer brought in a consumer Netgear router to improve coverage in the back shop. That router is still running and connected to the corporate network switch.

What the assessor finds

The Netgear router broadcasts an open Wi-Fi SSID with no password. Its LAN port is connected to the production network switch, giving any Wi-Fi device within range full access to the CUI network. Guest and corporate Wi-Fi share the same subnet. No wireless access point inventory exists in the SSP.

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

Wireless access points inventoried in SSP, per-device authorization required before connection, rogue AP detection active, guest Wi-Fi on isolated VLAN with no CUI access, IoT devices on separate segment, unauthorized wireless devices promptly disabled.

Common Gaps

What assessors actually find in the field:

✗ **Rogue access points**

An employee plugged in a consumer router for better coverage — it is broadcasting an open SSID with a LAN port connected to the CUI network switch.

✗ **No access point inventory**

The organization does not know how many wireless access points exist or where they are — [a] is not met and [b] cannot be verified without an inventory.

✗ **Guest Wi-Fi on CUI network**

Guest and corporate Wi-Fi share the same VLAN — visitors can reach CUI systems and endpoints over the guest network.

✗ **No per-device authorization**

Any device that knows the Wi-Fi password can connect — there is no per-device authorization, only a shared credential.

✗ **IoT devices on CUI segment**

Smart TVs, printers, and other Wi-Fi-capable devices are connected to the same network as CUI systems without individual authorization.