RISORSA GRATUITA

Checklist Wi-Fi Enterprise

37 punti di verifica per validare la tua infrastruttura wireless prima di un audit, di un go-live o di un assessment NIS2.

Per chi è questa checklist

IT Manager, sistemisti, security officer e responsabili infrastruttura che gestiscono reti Wi-Fi enterprise (Ubiquiti, MikroTik, Cisco, Aruba) in ambienti regolamentati o ad alta densità.

Come usarla

Compila la checklist con il tuo team, segna i punti coperti e quelli da migliorare. Usa il risultato come base per il piano di rimedio o come evidenza in fase di audit.

Versione 1.0 · 12 pagine · Italiano · Maggio 2026

Indice

Introduzione

Una rete Wi-Fi enterprise non è solo una questione di copertura. È un componente critico dell'infrastruttura, soggetto a requisiti di sicurezza, performance, compliance e auditabilità.

Questa checklist nasce dall'esperienza pratica di consulenze e audit su reti wireless di medie e grandi imprese. Copre 6 aree fondamentali con 37 punti di verifica concreti, ognuno verificabile in poche minuti con i tool standard del settore.

Non sostituisce un audit professionale, ma ti aiuta a fare un self-assessment serio prima di chiamare un consulente — o per validare il lavoro fatto da uno.

AREA 1 / 6

Design & Site Survey

Verifica che la fase di progettazione e survey sia stata svolta con metodo, dati e tool adeguati.

- ■ Survey predittivo (Ekahau, iBwave, Hamina) basato su planimetrie aggiornate e materiali corretti (gesso, vetro, mattoni).
- ■ Survey on-site post-deploy con misure RSSI, SNR, copertura per banda (2.4/5/6 GHz).
- ■ Validazione capacity planning: client per AP, throughput per area, applicazioni critiche (voce, video).
- ■ Definizione cell size target (-65 dBm primaria, -72 dBm secondaria) e overlap 15-20%.
- ■ Documentazione AP placement con coordinate, modello, antenne, orientamento, canale, potenza.
- ■ Heatmap di copertura, SNR e capacità rilasciata al cliente con report formale.

AREA 2 / 6

Capacity & Performance

Garantisci che l'infrastruttura regga il carico atteso con margine, su tutte le bande e per tutti i client.

- Band steering attivo verso 5/6 GHz con soglia RSSI configurata (-65 dBm tipico).
- Airtime fairness e DFS abilitati su 5 GHz dove i canali sono disponibili.
- MU-MIMO e OFDMA verificati su AP Wi-Fi 6/6E/7, con client compatibili in lab.
- QoS WMM e mappatura DSCP coerente fra wired e wireless (voce EF, video AF41).
- Limiti broadcast/multicast e snooping IGMP/MLD configurati per ridurre rumore di rete.
- Test di throughput (iperf3) per AP, per banda, per VLAN, con baseline documentata.
- Limite client per AP/SSID coerente con capacity plan (no AP "sovraccarichi").

AREA 3 / 6

Security & Authentication

Controlla che gli SSID e le credenziali siano allineati alle best practice e ai requisiti normativi.

- WPA3-Enterprise (o WPA2/3 transition) sugli SSID corporate; WPA3-SAE sugli SSID PSK.
- 802.1X EAP-TLS con certificati client gestiti da PKI interna o MDM.
- RADIUS server ridondato (primario + secondario), shared secret robusti, accounting attivo.
- PMF (Protected Management Frames) richiesto su tutti gli SSID enterprise.
- SSID guest isolato (client isolation, DHCP/DNS dedicati, NAT, captive portal con T&C;).
- Rotazione PSK programmata e gestita (no PSK condivise via mail/chat).
- Disabilitazione protocolli legacy 802.11b e rate < 12 Mbps; WPS disattivato.

AREA 4 / 6

Roaming & Mobility

Roaming fluido fra AP è critico per voce, video e applicazioni mobili. Verifica i meccanismi 802.11k/v/r.

- 802.11k (Neighbor Reports) attivo: i client ricevono lista AP candidati per roaming.
- 802.11v (BSS Transition Management) attivo per suggerire l'AP migliore lato infrastruttura.
- 802.11r (Fast BSS Transition) attivo su SSID voice-grade, testato con device target.
- Min RSSI / sticky client kick configurato (es. -75 dBm) per forzare roaming.
- Test roaming reale con telefono softphone o smartphone: drop chiamata < 50 ms.
- VLAN/subnet coerente nel roaming domain (no roaming L3 non gestito).

AREA 5 / 6

Monitoring & SIEM Integration

Una rete enterprise non monitorata è una rete non gestita. Allinea logging, allerte e correlazione SIEM.

- Syslog dei controller/AP inviato a SIEM (Wazuh, Graylog, Splunk) con parser dedicato.
- WIDS/WIPS attivo: rilevamento rogue AP, evil twin, deauth flood, KARMA.
- Alert su anomalie autenticazione 802.1X (fallimenti ripetuti, lockout brute force).
- Dashboard real-time: AP up/down, client count, retry rate, channel utilization.
- Backup configurazione controller automatizzato (giornaliero, off-site).
- Test ripristino configurazione documentato (RTO definito).
- Log retention conforme ai requisiti legali (NIS2/DORA: minimo 6 mesi).

AREA 6 / 6

Compliance & Documentation

Audit-ready: documentazione, evidenze, processi formali. Indispensabile per NIS2, DLGS 138, GDPR, DORA.

- Inventario AP completo (modello, MAC, posizione, firmware) aggiornato.
- Procedura formale di patching firmware AP/controller con cadenza definita.
- Risk assessment wireless documentato (asset, minacce, vulnerabilità, mitigazioni).
- Policy uso rete wireless approvata e comunicata agli utenti (acceptable use).

Appendice

Riferimenti normativi

- Direttiva UE 2022/2555 (NIS2) — recepita in Italia con DLGS 138/2024.
- Regolamento UE 2022/2554 (DORA) per il settore finanziario.
- Regolamento UE 2016/679 (GDPR) — gestione dati personali su rete guest.
- Linee guida ENISA su sicurezza reti wireless aziendali.
- Standard IEEE 802.11 (k/v/r/w) e Wi-Fi Alliance Certified.

Prossimi passi

Se dalla compilazione della checklist emergono lacune significative, WiFiSecure offre tre tipi di intervento:

1. Wi-Fi Assessment

Audit on-site con survey on-site e on-air, report formale, piano di rimedio prioritizzato. Tipicamente 3-5 giornate/uomo.

2. Formazione tecnica

Percorsi certificati CWNP (CWNA, CWSP, CWAP, CWDP) e Ubiquiti (UWA, UEWA), MikroTik (MTCNA, MTCWE) erogati da istruttori certificati.

3. Progettazione & deploy

Design predittivo, deploy chiavi in mano, integrazione SIEM (Wazuh, Graylog), tuning post-installazione e knowledge transfer al team IT.

Vuoi un confronto sul tuo caso?

Contattaci per una call gratuita di 30 minuti.

wifisecure.dadonet.it/contatti