RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

**BACK TO BASICS**

# SECURING WI-FI NETWORKS

Wi-Fi is a radio-frequency communications technology designed for the deployment of wireless local area networks. However, it presents numerous risks, such as the interception or alteration of network traffic.

Check out the French cybersecurity agency (ANSSI)'s essential resources for the secure deployment and use of Wi-Fi in a workplace environment..

## 1/ USING WI-FI WITH PROFESSIONAL TERMINALS

- **Disable the Wi-Fi interface and Wi-Fi hotspot sharing** when not in use.
- **Turn off automatic connection** to known Wi-Fi networks.
- **Connect only to Wi-Fi networks controlled by the organisation;** when the is not an option (for example, in railway stations, airports or cafés), **use a VPN controlled by the organisation.**
- **Configure the local firewall on laptops to block incoming connections**, notably via the Wi-Fi interface.
- **Delete known networks and associated credentials** from devices before refurbishment, disposal, or scrapping.
- **Find out more** by reviewing the threat landscape for mobile phones published by the CERT-FR.

## 2/ DEPLOYING WI-FI NETWORKS CONTROLLED BY THE ORGANISATION

- **Disable the Wi-Fi Protected Setup (WPS) function systematically on access points.**
- **Deactivate the Universal Plug and Play (UPnP) function** when not in use.
- **Allow Wi-Fi access points controlled by the organisation only** on the network. The use of personal Wi-Fi access points in a professional environment must be prohibited.
- **Use robust and proven security modes:** WPA3-Enterprise, WPA2-Enterprise (subject to conditions) or WPA3-Personal:
  - in WPA3-Enterprise mode, use only EAP (Extensible Authentication Protocol) suites that support certificate-based authentication. Ensure the validity and legitimacy of the certificates used before any connections (Public Key Infrastructure);
  - in WPA2-Enterprise mode, **enable Protected Management Frames (PMF);**
  - avoid mixed WPA3/WPA2 mode or transition configurations. This may result in the sharing of secrets between WPA2 and WPA3 modes, as well as a security downgrade for devices supporting WPA3.
- **Control the distribution of authentication secrets:**
  - share secrets only to authorised staff;
  - change login secrets regularly, and update them immediately following a compromise or suspected compromise.

**V1.0** (08/26)

www.cyber.gouv.fr / conseil.technique@ssi.gouv.fr

RÉPUBLIQUE FRANÇAISE
*Liberté*
*Égalité*
*Fraternité*

→ **Partition networks by use:**

> **partition each Wi-Fi network into its own VLAN, separate from one another and from wired networks. Control necessary communications between these networks** using filtering equipment (firewalls);

> **use distinct network names (SSIDs) for each security mode,** particularly if multiple configurations coexist. For example:

- a network named *Workstations* using WPA3-Enterprise mode;
- a second network named *IoT* using WPA2-Enterprise mode for the organisation's connected devices, such as Programmable Logic Controllers (PLC) or Human–Computer Interaction (HCI) that do not support WPA3. These devices are often more vulnerable, and do not always support the latest security standards. Therefore, it is important to dedicate a separate network to each of them.

→ **Do not hide the SSID** when configuring Wi-Fi networks. There is no point in hiding the SSID, as a device that has previously connected to a Wi-Fi network with a hidden SSID will broadcast the name of that network.

→ **Change the default SSID**. Avoid any overly explicit names which might reveal business activity or personal information.

→ **Block connections from unmanaged devices** (e.g. personal mobile phones) **by default,** whilst allowing enrolment only for controlled devices. With regard to guest Wi-Fi networks, they should be dedicated and isolated from other networks.

## 3/ ADMINISTERING SECURE WI-FI NETWORKS

→ **Log connections to Wi-Fi access points and controllers:**

> configure the access points and controllers so that security events can be collected. It is preferable to redirect all events generated to a central monitoring infrastructure (see ANSSI's guidelines regarding the architecture of a logging system - only available in French);

> comply with regulations on the retention of technical connection data for public Wi-Fi services (see the French Data Protection Authority (CNIL)'s resources on this subject – only available in French).

→ **Set up, if an IGC exists, automatic certificate** enrolment via Windows Group Policy Objects (GPOs) so that devices automatically receive the certificate required for authentication on the Wi-Fi network. Next, restrict access to the relevant SSID to connections authenticated by certificate only.

→ **Secure the administration of Wi-Fi access points and controllers:**

> **change the default connection credentials.** This includes secrets, such as Wi-Fi connection passwords and certificates, as well as administrator passwords. Secrets must be robust, in accordance with ANSSI's recommendations on multi-factor authentication and passwords (guide only available in French);

> use secure administration protocols (TLS, SSH);

> connect the administration interface to a dedicated, secure and isolated administration network, in accordance with ANSSI's recommendations (guide only available in French);

> **deploy updates** for operating systems, drivers, access points, controllers and terminals, **systematically and as soon as possible.**