Networking

The **Networking** section of the Apple Policy Editor configures Wi-Fi networks and VPNs on the devices, installs certificates and restricts connectivity features such as AirDrop and Bluetooth. Each Wi-Fi network, VPN and certificate is installed as its own configuration profile, which you can see on the device in **Settings > General > VPN & Device Management** (Mac: **System Settings > General > Device Management**, or **Privacy & Security > Profiles** on macOS 13 and 14) and in the **Profiles, certificates and security** panel of the device page.

> Certificates are taken from the **Certificates** page: import them there first. The policy only refers to them, so a certificate is never copied in the policy.

Restrictions

- **Allow AirDrop**
- **Allow AirPlay incoming requests**
- **Allow Bluetooth modification**
- **Allow Bluetooth Sharing modification**
- **Allow Files Network Drive Access**
- **Allow Internet Sharing Modification**
- **Allow content caching**
- **Allow iTunes file sharing**

Wi-Fi networks

Click **Add Wi-Fi network** and fill in:

- **Network name (SSID)**: the name of the network, up to 32 characters.
- **Security**: none (open network), WEP, WPA or WPA2, WPA2 or WPA3, WPA3 only, or any.
- **Password**: the password of a personal network.
- **Join automatically** and **Hidden network** (for networks that don't broadcast their name).
- **Proxy**: none, manual (server and port) or automatic (a PAC file URL, or empty to find the settings on the network with WPAD).
- **Profile name** (optional) and **Applies to**, to limit the network to some device types.

Enterprise networks (802.1X)

Turn on **Enterprise (802.1X)** when users authenticate with their own credentials or a certificate instead of a shared password.

- **Authentication**: PEAP, TTLS (with its inner authentication, for example MSCHAPv2) or TLS (certificate only).
- **Credentials of the device user**: each device uses the EAP identity, anonymous identity and password of its user, set in the Users page. Devices without a user don't get the network.
- **Identity**, **Anonymous identity** and **Password**: the same for every device. The identity can contain the variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ and $UDID$. Leave the password empty to let the user type it on the device.
- **Identity certificate**: the client certificate the device presents (required for TLS). See the certificate options below.
- **Trusted certificates**: the CA certificates that issued the certificate of your RADIUS server. They are installed with the network.
- **Trusted server names**: the names of the RADIUS server certificates the devices accept, for example radius.example.com or *.example.com.

VPN

Click **Add VPN** to configure an IKEv2 or Cisco IPSec VPN, built into iOS, iPadOS and macOS (no VPN app needed).

- **Type** and **Server**. For IKEv2 also the **Remote identifier** (the server identity, empty means the server address) and the **Local identifier**, which can contain the variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ and $UDID$.
- **Authentication** of the device: a certificate (from the Certificates page, the certificate of the device user, or requested from a SCEP server), a shared secret (with the optional group name for IPSec), or none for IKEv2 servers that only check the user name and password.
- **Trusted certificates**: the CA certificates of your VPN server, installed with the VPN. For IKEv2 you can also set the expected server certificate issuer and name.
- **User name and password**: the user also authenticates with a user name (variables allowed) and a password (EAP for IKEv2, XAuth for IPSec). Leave the password empty to let the user type it on the device.
- **VPN name** (shown in Settings) and **Applies to**.

Connection

- **The user connects in Settings**: the VPN is installed and the user turns it on when needed.
- **On demand**: the device connects the VPN automatically. With **except on trusted Wi-Fi** the VPN is not used on the Wi-Fi networks you list, for example the office network.
- **Always On** (IKEv2, supervised iPhone and iPad only): all the traffic goes through the VPN on cellular and Wi-Fi and the user can't turn it off. Other devices don't get this VPN. If the VPN uses a user name, the password must be set in the policy.
- **Per-app VPN**: only some apps use the VPN. Choose the VPN for each app in the **App management** section (field **VPN** of the app, not available on Mac), and optionally list Safari domains that use it.

> Test an Always On or on-demand VPN on a test device first: if the server can't be reached, the device may have no connection.

Global proxy, encrypted DNS and web content filter

These settings apply to all the traffic of the device. Turn them on with their toggle.

- **Global HTTP proxy** (supervised iPhone and iPad, Mac): all the HTTP traffic goes through the proxy, on every network. Set the server and port (with an optional user name and password) or an automatic configuration (PAC file URL, or empty to find it on the network). **Allow Wi-Fi login pages** lets the user sign in to public Wi-Fi networks without the proxy.
- **Encrypted DNS**: the device resolves names with your DNS server over DNS over HTTPS (server URL) or DNS over TLS (server name), optionally only for some domains. On supervised devices you can prevent the user from turning it off.
- **Web content filter** (supervised iPhone and iPad): the filter built into iOS limits adult websites, with lists of websites always allowed or always blocked, or allows only a list of websites, shown as bookmarks in Safari.

> A wrong proxy or DNS server can leave the devices without a connection: try the settings on a test device first.

Certificates

Click **Add certificate** to install a certificate on its own: a certificate authority that Safari and the apps must trust, or an identity used by apps. The certificates of a Wi-Fi network or a VPN don't

need to be added here.

Certificate options

- **A certificate of the Certificates page**: the same certificate on every device. Click **Choose a certificate** to pick it.
- **The certificate of the device user**: each device gets the client certificate linked to its user. Devices whose user has no certificate don't get it. When you link another certificate to the user, the devices are updated.
- **Requested from a SCEP server**: each device requests its own certificate from your SCEP server (for example Microsoft NDES), so the private key never leaves the device. Set the server URL, the challenge if the server requires one, the subject (for example CN=$EMAIL$), the alternative names, the key size and the key usage.

> Client certificates (.p12) protected with the old RC2 encryption can't be installed on Apple devices. Export them again with 3DES or AES encryption before importing them.

Security

Profiles that contain passwords or private keys are sent only to the device they were made for: the device must sign its request with its management certificate. Passwords and certificates aren't written in the logs.

Revision #7
Created 2026-11-10 15:12:14 UTC by Admin
Updated 2026-11-12 09:51:56 UTC by Admin