Redes

La sección **Redes** del Editor de políticas de Apple configura redes Wi-Fi y VPN en los dispositivos, instala certificados y restringe funciones de conectividad como AirDrop y Bluetooth. Cada red Wi-Fi, VPN y certificado se instala como su propio perfil de configuración, que puedes ver en el dispositivo en **Configuración > General > VPN y gestión de dispositivos** (Mac: **Configuración del Sistema > General > Gestión de dispositivos**, o **Privacidad y seguridad > Perfiles** en macOS 13 y 14) y en el panel **Perfiles, certificados y seguridad** de la página del dispositivo.

> Los certificados se toman de la página **Certificados**: primero impórtalos allí. La política solo hace referencia a ellos, así que un certificado nunca se copia en la política.

Restricciones

- **Permitir AirDrop**
- **Permitir solicitudes entrantes de AirPlay**
- **Permitir modificación de Bluetooth**
- **Permitir modificación de Compartir Bluetooth**
- **Permitir acceso a unidades de red de Archivos**
- **Permitir modificación de Compartir Internet**
- **Permitir el almacenamiento en caché de contenido**
- **Permitir compartir archivos por iTunes**

Redes Wi-Fi

Haz clic en **Añadir red Wi-Fi** y rellena:

- **Nombre de la red (SSID)**: el nombre de la red, de hasta 32 caracteres.
- **Seguridad**: ninguna (red abierta), WEP, WPA o WPA2, WPA2 o WPA3, solo WPA3, o cualquiera.
- **Contraseña**: la contraseña de una red personal.
- **Unirse automáticamente** y **Red oculta** (para las redes que no difunden su nombre).
- **Proxy**: ninguno, manual (servidor y puerto) o automático (una URL de archivo PAC, o vacío para encontrar la configuración en la red con WPAD).
- **Nombre del perfil** (opcional) y **Se aplica a**, para limitar la red a algunos tipos de dispositivo.

Redes empresariales (802.1X)

Activa **Empresarial (802.1X)** cuando los usuarios se autentican con sus propias credenciales o un certificado en lugar de una contraseña compartida.

- **Autenticación**: PEAP, TTLS (con su autenticación interna, por ejemplo MSCHAPv2) o TLS (solo certificado).
- **Credenciales del usuario del dispositivo**: cada dispositivo usa la identidad EAP, la identidad anónima y la contraseña de su usuario, configuradas en la página Usuarios. Los dispositivos sin usuario no reciben la red.
- **Identidad**, **Identidad anónima** y **Contraseña**: las mismas para todos los dispositivos. La identidad puede contener las variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$. Deja la contraseña vacía para que el usuario la escriba en el dispositivo.
- **Certificado de identidad**: el certificado de cliente que presenta el dispositivo (obligatorio para TLS). Consulta las opciones de certificado a continuación.
- **Certificados de confianza**: los certificados de CA que emitieron el certificado de tu servidor RADIUS. Se instalan con la red.
- **Nombres de servidor de confianza**: los nombres de los certificados del servidor RADIUS que aceptan los dispositivos, por ejemplo radius.example.com o *.example.com.

VPN

Haz clic en **Añadir VPN** para configurar una VPN IKEv2 o Cisco IPSec, integrada en iOS, iPadOS y macOS (no se necesita ninguna app de VPN).

- **Tipo** y **Servidor**. Para IKEv2, también el **Identificador remoto** (la identidad del servidor; vacío significa la dirección del servidor) y el **Identificador local**, que puede contener las variables $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ y $UDID$.
- **Autenticación** del dispositivo: un certificado (de la página Certificados, el certificado del usuario del dispositivo, o solicitado a un servidor SCEP), un secreto compartido (con el nombre de grupo opcional para IPSec), o ninguna para los servidores IKEv2 que solo comprueban el nombre de usuario y la contraseña.
- **Certificados de confianza**: los certificados de CA de tu servidor VPN, instalados con la VPN. Para IKEv2 también puedes establecer el emisor y el nombre del certificado de servidor esperados.
- **Nombre de usuario y contraseña**: el usuario también se autentica con un nombre de usuario (se permiten variables) y una contraseña (EAP para IKEv2, XAuth para IPSec). Deja la contraseña vacía para que el usuario la escriba en el dispositivo.
- **Nombre de la VPN** (se muestra en Configuración) y **Se aplica a**.

Conexión

- **El usuario se conecta en Configuración**: la VPN está instalada y el usuario la activa cuando es necesario.
- **Bajo demanda**: el dispositivo conecta la VPN automáticamente. Con **excepto en redes Wi-Fi de confianza** no se usa la VPN en las redes Wi-Fi que indiques, por ejemplo la red de la oficina.
- **Siempre activa** (IKEv2, solo iPhone y iPad supervisados): todo el tráfico pasa por la VPN en redes móviles y Wi-Fi, y el usuario no puede desactivarla. Los demás dispositivos no reciben esta VPN. Si la VPN usa un nombre de usuario, la contraseña debe establecerse en la política.
- **VPN por app**: solo algunas apps usan la VPN. Elige la VPN para cada app en la sección **Gestión de apps** (campo **VPN** de la app, no disponible en Mac) y, opcionalmente, indica los dominios de Safari que la usan.

> Prueba primero una VPN Siempre activa o bajo demanda en un dispositivo de prueba: si no se puede alcanzar el servidor, el dispositivo puede quedarse sin conexión.

Proxy global, DNS cifrado y filtro de contenido web

Estos ajustes se aplican a todo el tráfico del dispositivo. Actívalos con su interruptor.

- **Proxy HTTP global** (iPhone y iPad supervisados, Mac): todo el tráfico HTTP pasa por el proxy, en todas las redes. Establece el servidor y el puerto (con un nombre de usuario y una contraseña opcionales) o una configuración automática (URL de archivo PAC, o vacío para encontrarla en la red). **Permitir páginas de inicio de sesión Wi-Fi** permite al usuario iniciar sesión en redes Wi-Fi públicas sin el proxy.
- **DNS cifrado**: el dispositivo resuelve nombres con tu servidor DNS mediante DNS over HTTPS (URL del servidor) o DNS over TLS (nombre del servidor), opcionalmente solo para algunos dominios. En los dispositivos supervisados puedes impedir que el usuario lo desactive.
- **Filtro de contenido web** (iPhone y iPad supervisados): el filtro integrado en iOS limita los sitios web para adultos, con listas de sitios web siempre permitidos o siempre bloqueados, o permite solo una lista de sitios web, que se muestran como marcadores en Safari.

>

> Un proxy o servidor DNS incorrecto puede dejar los dispositivos sin conexión: pruebaprimero los ajustes en un dispositivo de prueba.

Certificados

Haz clic en **Añadir certificado** para instalar un certificado por separado: una autoridad de certificación en la que Safari y las apps deben confiar, o una identidad que usan las apps. Los certificados de una red Wi-Fi o una VPN no necesitan añadirse aquí.

Opciones de certificado

- **Un certificado de la página Certificados**: el mismo certificado en todos los dispositivos. Haz clic en **Elegir un certificado** para seleccionarlo.
- **El certificado del usuario del dispositivo**: cada dispositivo recibe el certificado de cliente vinculado a su usuario. Los dispositivos cuyo usuario no tiene certificado no lo reciben. Cuando vinculas otro certificado al usuario, los dispositivos se actualizan.
- **Solicitado a un servidor SCEP**: cada dispositivo solicita su propio certificado a tu servidor SCEP (por ejemplo Microsoft NDES), así que la clave privada nunca sale del dispositivo. Establece la URL del servidor, el desafío si el servidor lo requiere, el sujeto (por ejemplo CN=$EMAIL$), los nombres alternativos, el tamaño de la clave y el uso de la clave.

> Los certificados de cliente (.p12) protegidos con el antiguo cifrado RC2 no se pueden instalar en dispositivos Apple. Vuelve a exportarlos con cifrado 3DES o AES antes de importarlos.

Seguridad

Los perfiles que contienen contraseñas o claves privadas se envían solo al dispositivo para el que se crearon: el dispositivo debe firmar su solicitud con su certificado de gestión. Las contraseñas y los certificados no se escriben en los registros.

Revision #7
Created 2026-11-10 15:14:48 UTC by Admin
Updated 2026-11-12 09:54:42 UTC by Admin