الشبكات

يكوّن قسم **الشبكات** في محرّر سياسة Apple شبكات Wi-Fi وشبكات VPN على الأجهزة، ويثبّت الشهادات ويقيّد ميزات الاتصال مثل AirDrop وBluetooth. تُثبّت كل شبكة Wi-Fi وكل VPN وكل شهادة كملف تعريف تكوين خاص بها، يمكنك رؤيته على الجهاز في **الإعدادات > عام > VPN وإدارة الأجهزة** (Mac: **إعدادات النظام > عام > إدارة الأجهزة**، أو **الخصوصية والأمان > ملفات التعريف** على macOS 13 و14) وفي لوحة **ملفات التعريف والشهادات والأمان** في صفحة الجهاز.

> تُؤخذ الشهادات من صفحة **الشهادات**: استوردها هناك أولاً. لا تشير السياسة إليها إلا، لذا لا تُنسخ أي شهادة في السياسة.

القيود

- **السماح بـ AirDrop**
- **السماح بطلبات AirPlay الواردة**
- **السماح بتعديل Bluetooth**
- **السماح بتعديل مشاركة Bluetooth**
- **السماح لتطبيق الملفات بالوصول إلى محركات أقراص الشبكة**
- **السماح بتعديل مشاركة الإنترنت**
- **السماح بالتخزين المؤقت للمحتوى**
- **السماح بمشاركة ملفات iTunes**

شبكات Wi-Fi

انقر على **إضافة شبكة Wi-Fi** وأملأ:

- **اسم الشبكة (SSID)**: اسم الشبكة، حتى 32 حرفًا.
- **الأمان**: لا شيء (شبكة مفتوحة)، أو WEP، أو WPA أو WPA2، أو WPA2 أو WPA3، أو WPA3 فقط، أو أي.
- **كلمة المرور**: كلمة مرور شبكة شخصية.
- **الانضمام تلقائيًا** و**شبكة مخفية** (للشبكات التي لا تبثّ اسمها).
- **الوكيل**: لا شيء، أو يدوي (الخادم والمنفذ)، أو تلقائي (عنوان URL لملف PAC، أو فارغ للعثور على الإعدادات على الشبكة عبر WPAD).
- **اسم ملف التعريف** (اختياري) و**ينطبق على**، لتقييد الشبكة بأنواع أجهزة معينة.

شبكات المؤسسات (802.1X)

فعّل **المؤسسة (802.1X)** عندما يصادق المستخدمون ببيانات اعتماده الخاصة أو بشهادة بدلًا من كلمة مرور مشتركة.

- **المصادقة**: PEAP، أو TTLS (مع مصادقته الداخلية، مثلًا MSCHAPv2)، أو TLS (شهادة فقط).
- **بيانات اعتماد مستخدم الجهاز**: يستخدم كل جهاز هويته EAP والهويته المجهولة وكلمة المرور الخاصة بمستخدمه، المضبوطة في صفحة المستخدمين. لا تتلقى الأجهزة التي ليس لها مستخدم الشبكة.
- **الهوية**، و**الهوية المجهولة** و**كلمة المرور**: نفسها لكل جهاز. يمكن أن تحتوي الهوية على المتغيرات $EMAIL$ و$USERNAME$ و$FULLNAME$ و$SERIAL$ و$UDID$. اترك كلمة المرور فارغة ليُدخلها المستخدم على الجهاز.
- **شهادة الهوية**: شهادة العميل التي يقدّمها الجهاز (مطلوبة لـ TLS). راجع خيارات الشهادة أدناه.
- **الشهادات الموثوقة**: شهادات CA التي أصدرت شهادة خادم RADIUS الخاص بك. تُثبّت مع الشبكة.
- **أسماء الخوادم الموثوقة**: أسماء شهادات خادم RADIUS التي تقبلها الأجهزة، مثلًا radius.example.com أو *.example.com.

VPN

انقر على **إضافة VPN** لتكوين VPN من نوع IKEv2 أو Cisco IPSec، مضمّنة في iOS وiPadOS وmacOS (دون الحاجة إلى تطبيق VPN).

- **النوع** و**الخادم**. بالنسبة لـ IKEv2 أيضًا **المعرّف البعيد** (هوية الخادم، والفارغ يعني عنوان الخادم) و**المعرّف المحلي**، ويمكن أن يحتوي على المتغيرات $EMAIL$ و$USERNAME$ و$FULLNAME$ و$SERIAL$ و$UDID$.
- **مصادقة** الجهاز: شهادة (من صفحة الشهادات، أو شهادة مستخدم الجهاز، أو مطلوبة من خادم SCEP)، أو سرّ مشترك (مع اسم المجموعة الاختياري لـ IPSec)، أو الشيء لخوادم IKEv2 التي تتحقق فقط من اسم المستخدم وكلمة المرور.
- **الشهادات الموثوقة**: شهادات CA لخادم VPN الخاص بك، مثبّتة مع VPN. بالنسبة لـ IKEv2 يمكنك أيضًا تعيين جهة إصدار شهادة الخادم المتوقعة واسمها.
- **اسم المستخدم وكلمة المرور**: يصادق المستخدم أيضًا باسم مستخدم (المتغيرات مسموح بها) وكلمة مرور (EAP لـ IKEv2، وXAuth لـ IPSec). اترك كلمة المرور فارغة ليُدخلها المستخدم على الجهاز.
- **اسم VPN** (يُعرض في الإعدادات) و**ينطبق على**.

الاتصال

- **يتصل المستخدم من الإعدادات**: تُثبّت VPN ويشغّلها المستخدم عند الحاجة.
- **عند الطلب**: يتصل الجهاز بـ VPN تلقائيًا. مع **باستثناء شبكات Wi-Fi الموثوقة** لا تُستخدم VPN على شبكات Wi-Fi التي تسردها، مثلًا شبكة المكتب.

- **دائم التشغيل** (IKEv2، لأجهزة iPhone وiPad الخاضعة للإشراف فقط): تمرّر كل حركة المرور عبر VPN على شبكة الجوال وWi-Fi والي يمكن للمستخدم إيقافها. لا تتلقى الأجهزة الأخرى هذه VPN. إذا كانت VPN تستخدم اسم مستخدم، فيجب تعيين كلمة المرور في السياسة.
- **VPN لكل تطبيق**: تستخدم بعض التطبيقات فقط VPN. اختر VPN لكل تطبيق في قسم **إدارة التطبيقات** (حقل **VPN** للتطبيق، غير متاح على Mac)، واختيارياً اسرد نطاقات Safari التي تستخدمها.

> اختبر VPN دائم التشغيل أو عند الطلب على جهاز اختبار أولاً: إذا تعذّر الوصول إلى الخادم، فقد لا يكون لدى الجهاز اتصال.

الوكيل العام وDNS المشفّر ومرشّح محتوى الويب

تنطبق هذه الإعدادات على كل حركة المرور في الجهاز. فعّلها باستخدام مفتاح التبديل الخاص بها.

- **وكيل HTTP العام** (أجهزة iPhone وiPad الخاضعة للإشراف، وMac): تمرّر كل حركة مرور HTTP عبر الوكيل، على كل شبكة. عيّن الخادم والمنفذ (مع اسم مستخدم وكلمة مرور اختياريين) أو تكوينًا تلقائيًا (عنوان URL لملف PAC، أو فارغ للعثور عليه على الشبكة). يتيح **السماح بصفحات تسجيل الدخول إلى Wi-Fi** للمستخدم تسجيل الدخول إلى شبكات Wi-Fi العامة دون الوكيل.
- **DNS المشفّر**: يحلّ الجهاز الأسماء باستخدام خادم DNS الخاص بك عبر DNS over HTTPS (عنوان URL للخادم) أو DNS over TLS (اسم الخادم)، واختيارياً لنطاقات معينة فقط. على الأجهزة الخاضعة للإشراف يمكنك منع المستخدم من إيقافه.
- **مرشّح محتوى الويب** (أجهزة iPhone وiPad الخاضعة للإشراف): يحدّ المرشّح المضمّن في iOS من مواقع البالغين، بقوائم مواقع مسموح بها دائمًا أو محظورة دائمًا، أو يسمح فقط بقائمة مواقع، تظهر كإشارات مرجعية في Safari.

> قد يترك وكيل أو خادم DNS خاطئ الأجهزة دون اتصال: جرّب الإعدادات على جهاز اختبار أولاً.

الشهادات

انقر على **إضافة شهادة** لتثبيت شهادة بحد ذاتها: جهة إصدار شهادات يجب أن يثق بها Safari والتطبيقات، أو هوية تستخدمها التطبيقات. الحاجة لإضافة شهادات شبكة Wi-Fi أو VPN هنا.

خيارات الشهادة

- **شهادة من صفحة الشهادات**: الشهادة نفسها على كل جهاز. انقر على **اختيار شهادة** لاختيارها.
- **شهادة مستخدم الجهاز**: يحصل كل جهاز على شهادة العميل المرتبطة بمستخدمه. لا تتلقاها الأجهزة التي ليس لمستخدمها شهادة. عند ربط شهادة أخرى بالمستخدم، تُحدَّث الأجهزة.
- **مطلوبة من خادم SCEP**: يطلب كل جهاز شهادته الخاصة من خادم SCEP الخاص بك (مثلاً Microsoft NDES)، لذا لا يغادر المفتاح الخاص الجهاز أبدًا. عيّن عنوان URL للخادم، والتحدّي إذا كان الخادم يتطلبه، والموضوع (مثلاً CN=$EMAIL$)، والأسماء البديلة، وحجم المفتاح، واستخدام المفتاح.

> لا يمكن تثبيت شهادات العميل (.p12) المحمية بتشفير RC2 القديم على أجهزة Apple. صدّرها مجددًا بتشفير 3DES أو AES قبل استيرادها.

الأمان

تُرسل ملفات التعريف التي تحتوي على كلمات مرور أو مفاتيح خاصة فقط إلى الجهاز المعدّ له: يجب أن يوقّع الجهاز طلبه بشهادة الإدارة الخاصة به. لا تُكتب كلمات المرور والشهادات في السجلات.

Revision #7
Created 2026-11-10 15:13:30 UTC by Admin
Updated 2026-11-12 09:53:24 UTC by Admin