macOS

يدير قسم **macOS** في محرّر سياسة Apple إعدادات الأمان والخصوصية وتسجيل الدخول لأجهزة Mac: FileVault، وجدار الحماية، وGatekeeper، وشاشة التوقف والقفل، والتخزين الخارجي والشبكي، ومشاركة الشاشة، وأذونات الخصوصية، وعناصر تسجيل الدخول، وامتدادات النظام والنواة المسموح بتحميلها. كما يثبّت ملفات تكوين خدمات النظام والمهام الخلفية. لا تتلقى الأجهزة الأخرى في السياسة هذه الإعدادات. فعّل إعدادًا لإدارته؛ وبينما هو معطّل، يحتفظ المستخدمون بخياراتهم.

> تُثبّت معظم الإعدادات على جهاز Mac كملفات تعريف تكوين، وتظهر في إعدادات النظام > عام > إدارة الأجهزة. تتطلب FileVault وأذونات الخصوصية وعناصر تسجيل الدخول وإعدادات الامتدادات MDM معتمدًا من المستخدم: على جهاز Mac مسجّل عبر عنوان URL للتسجيل أو رمز QR، يعتمد المستخدم ملف تعريف التسجيل في إعدادات النظام. تعرض صفحة الجهاز ذلك في حقل **MDM معتمد من المستخدم**. عندما يعتمده المستخدم لاحقًا، يتلقى جهاز Mac هذه الإعدادات تلقائيًا.

FileVault

يشفّر FileVault قرص جهاز Mac. عند تفعيل هذا الإعداد، يُطلب من المستخدمين تفعيل FileVault باستخدام كلمة المرور الخاصة بهم، ويرسل جهاز Mac مفتاح الاسترداد الشخصي الخاص به إلى Cerberus Enterprise، مشفّرًا بمفتاح يخص مؤسستك فقط. يُعرض المفتاح ويُعيّن من حقل **FileVault** في صفحة الجهاز (راجع أوامر الجهاز). يتطلب الإعداد macOS 13 أو أحدث وMDM معتمدًا من المستخدم؛ دون MDM معتمد من المستخدم لا يُطلب من جهاز Mac تفعيل FileVault، لكن إذا فعّله المستخدم، يُخزّن مفتاحه.

- **مطلوب عند تسجيل الدخول**: عند تسجيل الدخول التالي، أو بعد عدد من التخطيات (يُسأل المستخدم مرة أخرى عند كل تسجيل دخول وعند تسجيل الخروج)، أو فقط عندما يسجّل المستخدم الخروج.
- **عدم السؤال عند تسجيل الخروج**: يُسأل المستخدم عند تسجيل الدخول فقط. لا يمكن دمجه مع «السؤال فقط عند تسجيل الخروج».
- **عرض مفتاح الاسترداد للمستخدم**: معطّل افتراضيًا، لذا يعرف المفتاح المسؤولون فقط، من صفحة الجهاز.
- **منع إيقاف FileVault**: مفعّل افتراضيًا.
- **إزالة المفتاح من الذاكرة في وضع الاستعداد**: يعيد المستخدم كتابة كلمة المرور عندما يستيقظ جهاز Mac من وضع الاستعداد.
- **مكان حفظ المفتاح**: نص يُعرض للمستخدم في نافذة تسجيل الدخول، مثلًا بمن يجب الاتصال لاسترداد جهاز Mac (الافتراضي «Cerberus Enterprise»).

> يحتفظ جهاز Mac الذي كان مشفّرًا بالفعل عند تلقّي الإعداد بمفتاحه الحالي، ولا يتلقاه Cerberus Enterprise: لا يُخزّن المفتاح إلا بعد أن يوقف المستخدم FileVault ويعيد تفعيله (مع إيقاف «منع إيقاف FileVault»). إيقاف الإعداد، أو إزالة جهاز Mac من الإدارة، لا يوقف FileVault، ويستمر المفتاح المخزّن في العمل. لا يمكن حفظ الإعداد عندما لا يكون الخادم مهيأً لتخزين مفاتيح الاسترداد.

جدار الحماية

- **تفعيل جدار الحماية**: عندما يكون معطّلًا، يبقى جدار الحماية معطّلًا ولا يمكن للمستخدمين تفعيله.
- **حظر جميع الاتصالات الواردة**: لا يمكن إلا لخدمات الشبكة الأساسية (DHCP وBonjour وIPSec) تلقّي الاتصالات.
- **الوضع الخفي**: لا يجيب جهاز Mac على طلبات ping والاتصالات بالمنافذ المغلقة.
- **السماح للبرامج المضمّنة والسماح للتطبيقات الموقّعة التي تم تنزيلها** بتلقّي الاتصالات دون سؤال المستخدم (macOS 12.3 أو أحدث).
- **قواعد لتطبيقات محددة**: اسمح بالاتصالات الواردة لتطبيق أو احظرها، حسب معرّف الحزمة.

Gatekeeper

يفحص Gatekeeper التطبيقات قبل فتحها. اختر ما إذا كانت أجهزة Mac تفتح تطبيقات App Store فقط، أو أيضًا تطبيقات المطوّرين المعروفين. مع تعطيل Gatekeeper، يمكن فتح أي تطبيق، حتى غير الموقّعة أو التالفة. في macOS 15 أو أحدث يمكنك أيضًا اختيار ما إذا كان يُطلب من المستخدمين إرسال البرامج الضارة المحظورة إلى Apple.

شاشة التوقف والقفل

ابدأ شاشة التوقف بعد فترة من عدم النشاط، واطلب كلمة المرور عند بدء شاشة التوقف أو نوم الشاشة، فورًا أو بعد تأخير. الإعداد الذي يبقى على **غير مُدار** يظل خيار المستخدم.

التخزين الخارجي والشبكي

اسمح بالتخزين الخارجي (محركات USB، وبطاقات SD، والأقراص الخارجية) والتخزين الشبكي (مشاركات الملفات) لأجهزة Mac أو اجعله للقراءة فقط أو احظره. يتطلب macOS 15 أو أحدث.

مشاركة الشاشة

حدود الأشخاص الذين يتصلون بأجهزة Mac هذه عبر مشاركة الشاشة: نسخ الملفات من جهاز Mac أو إليه، والاتصالات عالية الأداء، وعدد شاشات العرض الافتراضية. يظل تفعيل مشاركة الشاشة خيار المستخدم. يتطلب macOS 14 أو أحدث.

أذونات الخصوصية

امنح التطبيقات أو امنعها الوصول الذي قد يسمح به المستخدمون في إعدادات النظام > الخصوصية والأمان، مثل الوصول الكامل إلى القرص لتطبيق نسخ احتياطي، أو منع الكاميرا لتطبيق. لكل إذن اختر:

- **الإذن**: الوصول الكامل إلى القرص، وإمكانية الوصول، والأتمتة، والمجلدات، وجهات الاتصال، والتقويمات، والصور، والكاميرا، والميكروفون، وتسجيل الشاشة، وغيرها من الخصوصية والأمان.
- **الوصول**: السماح أو المنع. لا يمكن لملف تعريف السماح بالكاميرا أو الميكروفون أو تسجيل الشاشة أو مراقبة الإدخال، بل المنع فقط؛ بالنسبة لتسجيل الشاشة ومراقبة الإدخال يمكن السماح للمستخدمين بالسماح بها أيضاً دون حقوق المسؤول.
- **التطبيق**: معرّف الحزمة لتطبيق، أو مسار برنامج (مثل أداة سطر أوامر).
- **متطلب الشيفرة**: يعرّف التطبيق بتوقيعه. احصل عليه في Terminal باستخدام `codesign -dr - /Applications/Example.app` وانسخ النص بعد `designated =>`.
- **الأتمتة** تحتاج أيضاً إلى التطبيق المتحكّم به (مثل Finder) وإلى متطلب الشيفرة الخاص به.

عناصر تسجيل الدخول والخلفية

تُدار عناصر تسجيل الدخول والعناصر الخلفية التي تطابق القواعد: تعمل دون سؤال، ولا يمكن للمستخدمين إيقافها في إعدادات النظام > عام > عناصر تسجيل الدخول. تطابق القاعدة معرّف فريق المطوّر لتطبيق، أو معرّف حزمته، أو تسمية launch daemon أو agent (أيضاً بالجزء الأول منها). يتطلب macOS 13 أو أحدث.

امتدادات النظام

امتدادات النظام هي الطريقة الحديثة لتوسيع التطبيقات لنظام macOS: مرشّحات الشبكة وشبكات VPN، ووكلاء أمن الأجهزة الطرفية وبرامج التشغيل. عند تفعيل هذا الإعداد، تُحمّل امتدادات النظام لفرق المطوّرين المدرجة دون سؤال المستخدم. يتطلب macOS 10.15 أو أحدث وMDM معتمداً من المستخدم.

- **معرّف الفريق**: معرّف الفريق المكوّن من 10 أحرف للمطوّر (مثلاً في تفاصيل «موقّع بواسطة» للتطبيق، أو باستخدام `codesign -dv`). يمكن أن يظهر لكل فريق مرة واحدة فقط.
- **السمات**: بكل امتدادات الفريق، أو فقط الامتدادات ذات معرّفات الحزم المدرجة.
- **الأنواع**: يقيّد الفريق ببرامج التشغيل أو امتدادات الشبكة أو أمن الأجهزة الطرفية. عند عدم اختيار أي منها، يُسمح بجميع الأنواع.
- **الإزالة** (للامتدادات المدرجة فقط): يمكن للتطبيق إزالة امتداده دون مسؤول (macOS 12 وأحدث)، أو ال يمكن إيقاف الامتداد أو إزالته أثناء تفعيل حماية تكامل النظام (System Integrity Protection)، أو ال يمكن إزالته في إعدادات النظام وFinder (macOS 15 وأحدث). ال تزال أجهزة Mac التي تعمل بإصدار macOS أقدم تسمح بالامتداد، دون خيار الإزالة.
- **يمكن للمستخدمين اعتماد امتدادات نظام أخرى**: مفعّل افتراضياً. عند تعطيله، ال يمكن تحميل إلا الامتدادات المسموح بها بواسطة ملف تعريف؛ وإذا عطّلته أي ملف تعريف على جهاز Mac، يكون معطّلاً.

> في macOS 11.3 وأحدث، تؤدي إزالة هذا الإعداد إلى إيقاف امتدادات النظام التي سمح بها، مثلاً وكيل أمان أو مرشّح شبكة. يحدث ذلك عند إيقاف الإعداد، وعند حذف السياسة، وعندما ينتقل جهاز Mac إلى سياسة لا تحتوي عليه. يطلب المحرّر تأكيداً قبل إيقاف الإعداد.

امتدادات النواة (قديمة)

امتدادات النواة هي الطريقة الأقدم والمهملة لتوسيع macOS: فضّل امتدادات النظام عندما يوفّرها المورّد. تُحمّل امتدادات النواة للفرق المدرجة (كل امتدادات فريق، أو فقط معرّفات الحزم المدرجة) دون سؤال المستخدم، بعد إعادة التشغيل. يتطلب macOS 10.13.2 أو أحدث وMDM معتمداً من المستخدم.

- **يمكن للمستخدمين اعتماد امتدادات نواة أخرى**: معطّل افتراضياً، لذا لا يمكن إلا للفرق المدرجة تحميل امتدادات النواة.
- **يمكن للمستخدمين القياسيين اعتمادها أيضاً**: مع تفعيل اعتمادات المستخدم، يمكن للمستخدمين دون حقوق المسؤول اعتمادها أيضاً (macOS 11 وأحدث).

> على أجهزة Mac المزوّدة بمعالجات Apple silicon، لا يكفي ملف تعريف وحده: يجب أن يبدأ شخص تشغيل جهاز Mac في recoveryOS، ويختار «الأمان المخفّض» في أداة أمان بدء التشغيل، ويسمح بإدارة المستخدم لامتدادات النواة من مطوّرين معروفين. قد يحتاج جهاز Mac أيضاً إلى Bootstrap Token مودع في Cerberus Enterprise لاعتمادها (راجع حقل Bootstrap Token في صفحة الجهاز).

ملفات Mac

تستخدم ملفات تكوين الخدمة والمهام الخلفية ملفات ترفعها إلى **ملفات Mac** الخاصة بمؤسستك: أرشيفات zip وقوائم خصائص (.plist) حتى 20 ميغابايت. ارفعها أو تحقّق من أماكن استخدامها أو احذفها باستخدام زر **ملفات Mac** في قسم macOS، أو عبر **اختيار ملف** في أحد الإعدادات. لا يمكن حذف ملف تستخدمه سياسة. لتغيير ملف، ارفع الإصدار الجديد واختره في السياسة: تعيد أجهزة Mac تنزيله.

ملفات تكوين الخدمة

يثبّت ملفات تكوين خدمة نظام من أرشيف zip. الخدمات المضمّنة هي خادم SSH (sshd)، وsudo، وPAM، والطباعة (CUPS)، وخادم ويب Apache، وbash، وzsh، وتسجيل الدخول بالبطاقة الذكية، والتفويض. يمكنك أيضاً استخدام خدمتك الخاصة، بمعرّف عكسي للنطاق مثل `com.example.service`: يعثر على الملفات عبر مكتبة ملفات التكوين المُدارة في macOS. يمكن أن يكون لكل خدمة إعداد واحد. يتطلب macOS 14 أو أحدث.

> تستخدم خدمة مضمّنة ملفات الأرشيف فقط وتتجاهل ملفاتها الخاصة، مثلاً /etc/ssh بالنسبة لـ sshd: ضع التكوين كاملاً في الأرشيف، في مجلدات تبدأ من جذر القرص (مثلاً `etc/ssh/sshd_config`). تكون الملفات للقراءة فقط على جهاز Mac، وتُزال مع الإعداد. اختبر الأرشيف على جهاز Mac واحد أولاً: قد يمنع تكوين sudo أو PAM خاطئ المستخدمين من تسجيل الدخول أو من استخدام حقوق المسؤول.

المهام الخلفية

برامج ونصوص تعمل في الخلفية، يبدأها launchd. لا يمكن للمستخدمين إيقافها، وتُزال مع الإعداد. يتطلب macOS 15 أو أحدث. لكل مهمة اختر:

- **معرّف المهمة**: معرّف عكسي للنطاق، مثل `com.example.task`، مختلف لكل مهمة.
- **البرامج والنصوص** (اختياري): أرشيف zip يفكّ جهاز Mac ضغطَه في `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` متبوعاً بمعرّف المهمة. احتفظ بإذن التنفيذ للملفات، ولا تضع قوائم خصائص فيه.
- **قوائم خصائص launchd**: المهام التي تبدأ البرامج، وتُحمّل كخدمة خلفية (للنظام بأكمله، بصلاحيات الجذر) أو كـ agent (في كل جلسة مستخدم). أشر إلى البرامج بمسارها في المجلد أعلاه.

تحتاج المهمة إلى البرامج أو إلى قائمة خصائص واحدة على الأقل. عند تغيّر الملفات، تعيد أجهزة Mac تشغيل المهمة.

Revision #7
Created 2026-11-10 15:13:31 UTC by Admin
Updated 2026-11-12 09:53:24 UTC by Admin