السياسات - Apple

- سياسات Apple
- التطبيقات وملفات التعريف
- وضع الكشك والشاشة الرئيسية
- رمز المرور
- القوي
- الشبكات
- تحديثات البرامج
- macOS
- الموقع والأسيجة الجغرافية
- الحسابات
- قواعد المامتثال

سياسات Apple

تحدد سياسات Apple إعدادات الإدارة التي يطبّقها Cerberus Enterprise على أجهزة Apple عبر MDM. تُضبط هذه الإعدادات من لوحة التحكم في محرر سياسة Apple.

قبل أن تبدأ

تتطلب إدارة أجهزة Apple تهيئة Apple Management (APNs). عند الحاجة، اقرأ صفحة إعداد Apple Management (APNs).

فتح محرر سياسة Apple

في لوحة التحكم، افتح **السياسات** وانقر على **إنشاء سياسة Apple جديدة**. لتعديل سياسة Apple موجودة، انقر على صفها في جدول السياسات.

تخطيط المحرر

ينظّم محرر سياسة Apple على شكل مجموعة من الأقسام القابلة للتوسيع. في أعلى الصفحة يمكنك دائماً تعديل:

- **الاسم** (مطلوب)
- **المعرّف** (للقراءة فقط)
- **الوصف** (اختياري)

أقسام السياسة

تتوافق الأقسام أدناه مع اللوحات المتاحة حالياً في محرّر سياسة Apple. عند فتح سياسة محفوظة، تكون الأقسام التي تغيّرت إعداداتها مفتوحة بالفعل وتبقى الأخرى مغلقة:

- **إدارة التطبيقات**: اضبط القيود المتعلقة بالتطبيقات والتطبيقات المُدارة وإعدادات تطبيق Cerberus Enterprise.
- **وضع Kiosk والشاشة الرئيسية**: وضع التطبيق الواحد، والتطبيقات المسموح بها والمحظورة، وتخطيط الشاشة الرئيسية، ومقاطع الويب، وإعدادات الإشعارات، ورسالة

شاشة القفل.

- **الأمان**: تحكم في ميزات مثل الفتح التلقائي والفتح بالمقاييس الحيوية.
- **إعدادات رمز المرور**: اضبط متطلبات رمز المرور والقواعد ذات الصلة.
- **الوسائط المتعددة**: السماح بالكاميرا والميزات ذات الصلة أو منعها.
- **الشبكة الخلوية**: التحكم في الإعدادات المتعلقة بالشبكة الخلوية (إعدادات بيانات الشبكة الخلوية للتطبيقات، وeSIM، وتغييرات الخطط)، وAPN الخلوي.
- **الشبكات**: شبكات Wi-Fi (بما في ذلك 802.1X للمؤسسات)، وشبكات VPN، والشهادات، والوكيل العام، وDNS المشفّر، وعامل تصفية محتوى الويب، وقيود الاتصال مثل AirDrop وBluetooth.
- **النظام وواجهة المستخدم**: تقييد ميزات النظام مثل Handoff واسم الجهاز وشاشة التوقف.
- **تحديثات البرامج**: اطلب إصدار نظام تشغيل بحلول موعد نهائي وتحكم في كيفية تنزيل التحديثات وتثبيتها.
- **macOS**: جدار الحماية، وGatekeeper، وشاشة التوقف والقفل، والتخزين الخارجي والشبكي، ومشاركة الشاشة، وأذونات الخصوصية، وعناصر تسجيل الدخول في أجهزة Mac.
- **تطبيقات Apple وخدماتها**: تقييد تطبيقات Apple وخدماتها مثل iMessage وGame Center وFind My.
- **Siri وApple Intelligence**: تقييد Siri والإملاء وميزات Apple Intelligence.
- **iCloud**: اسمح بخدمات iCloud محددة أو امنعها (النسخ الاحتياطي، ومزامنة سلسلة المفاتيح، والترحيل الخاص، وما إلى ذلك).
- **الموقع والنطاقات الجغرافية**: مناطق تُبلّغ أجهزة iPhone وiPad التي عليها تطبيق Cerberus Enterprise عند دخولها أو الخروج منها، لقواعد الأحداث.
- **الحسابات**: قيّد تعديل الحسابات واضبط حسابات البريد وExchange وGoogle والتقويم وجهات الاتصال والدليل.
- **قواعد الامتثال**: المتطلبات (رمز المرور، الحد الأدنى لإصدار نظام التشغيل، الإشراف، FileVault) التي تجعل الأجهزة غير ممتثلة، مع حظر اختياري.

> تتضمن العديد من الخيارات في محرر سياسة Apple تلميحًا يوثّق المتطلبات وإصدارات نظام التشغيل المدعومة.

الحفظ والحذف والأجهزة المرتبطة

استخدم **حفظ السياسة** لتطبيق تغييراتك. يكون الزر معطّلًا عند عدم وجود تعديلات معلّقة، أو عند انتهاء صلاحية الترخيص.

عند تعديل سياسة موجودة، تعرض الصفحة أيضًا إجراء **حذف السياسة**. يمكن للمحرر عرض قائمة **الأجهزة المرتبطة** في الأسفل، لترى عدد الأجهزة التي تستخدم السياسة حاليًا.

الصفحات التالية

- التطبيقات & ملفات التعريف: اضبط التطبيقات المثبتة وملفات تعريف التكوين.
- وضع Kiosk والشاشة الرئيسية: وضع التطبيق الواحد، والتطبيقات المسموح بها، وتخطيط الشاشة الرئيسية، ومقاطع الويب.
- رمز المرور: اضبط متطلبات رمز المرور وخيارات الأمان ذات الصلة.
- القيود: حدّد المميزات المسموح بها والقيود على مستوى نظام التشغيل.
- الشبكات: شبكات Wi-Fi وشبكات VPN والشهادات وقيود الاتصال.
- تحديثات البرامج: تحديثات نظام التشغيل المطلوبة وإعدادات تحديثات البرامج.
- macOS: جدار الحماية، وGatekeeper، وقفل الشاشة، والتخزين، وأذونات الخصوصية، وعناصر تسجيل الدخول في أجهزة Mac.
- الموقع والنطاقات الجغرافية: مناطق تُبلَّغ أجهزة iPhone وiPad بدخولها والخروج منها، وما تحتاج إليه للعمل.
- الحسابات: حسابات البريد وExchange وGoogle والتقويم وجهات الاتصال والدليل.
- قواعد الامتثال: متطلبات الأجهزة وحظر الأجهزة غير الممتثلة.

التطبيقات وملفات التعريف

يوثّق اذه القسم كيفية تكوين التطبيقات المدُارة وحمولات الحسابات لأجهزة Apple.

إدارة التطبيقات

تحتوي لوحة **إدارة التطبيقات** على قيود عامة متعلقة بالتطبيقات وعلى قائمة بالتطبيقات المدُارة.

قيود التطبيقات العامة

- **السماح بـ App Clips**
- **السماح بتثبيت التطبيقات**
- **السماح بإزالة التطبيقات**
- **السماح بتنزيل التطبيقات تلقائيًا**
- **السماح بإخفاء التطبيقات**
- **السماح بقفل التطبيقات**
- **السماح بعمليات الشراء داخل التطبيقات**
- **السماح بتعديل المتصفح الافتراضي**
- **السماح بالثقة في تطبيقات المؤسسة**

التطبيقات المدُارة

استخدم **إضافة تطبيق** لإضافة تطبيق إلى السياسة. ويُعرض كل تطبيق مُدار كبطاقة. يمكنك توسيع البطاقة لتعديل إعداداتها وإزالة التطبيق باستخدام إجراء الحذف.

- **معرّف App Store**: معرّف App Store للتطبيق المدُار.
- **معرّف الحزمة**: معرّف حزمة التطبيق.
- **سلوك التثبيت**: يتحكم في ما إذا كان يجب أن يبقى التطبيق مثبتاً أم يمكن للمستخدم تثبيته/إزالته.
- **التعيين**: نوع الترخيص الذي يختاره Cerberus لكل جهاز: ترخيص جهاز على أجهزة iPad وiPhone الشركة، وترخيص مستخدم لحساب Managed Apple Account على أجهزة iPhone وiPad الشخصية (تسجيل المستخدم). ولا يمكن تغيير هذا الحقل.
- **ترخيص VPP**: نوع ترخيص VPP المستخدم للتثبيت عبر App Store.

تعرض قائمة الخيار التطبيقات التراخيص المتاحة والإجمالية لكل تطبيق. وتعرض التطبيقات المجانية **غير محدود**: إذ تمنحها Apple تراخيص غير محدودة. ولا يمكن إضافة تطبيق إلى سياسة إلا مرة واحدة: فالتطبيق الذي يحمل معرّف App Store أو معرّف حزمة مطابقًا لتطبيق موجود بالفعل في السياسة يُرفض، وكذلك تُرفض السياسة التي تُدرج التطبيق نفسه مرتين عند حفظها.

تعرض قائمة الخيار التطبيقات تطبيقات مكتبة Apple Business لديك. لإضافة تطبيق، افتح في Apple Business **Apps & Services** ← **Apps & Books** ← **App Store**، وابحث عن التطبيق وانقر على **View**. بالنسبة إلى تطبيق مجاني، انقر على **Add**، واختر **All current and future** (أو الوحدة التنظيمية لرمز Apps and Books لديك) في **Organized Units**، ثم انقر على **Add**، ثم **Review** وأكّد. وبالنسبة إلى تطبيق مدفوع، انقر على سعره، واختر **Managed Licenses** كـ **License Type** (الذي لا يمكن لـ Cerberus Enterprise استخدام رموز الاسترداد)، واختر **Organizational Unit** لرمز Apps and Books لديك، وأدخل عدد **Licenses** (بحد أقصى 1000 لكل طلب)، ثم **Review** واشترِ. يجب إعداد طريقة دفع أولًا في **Settings** ← **Payments & Billing** ← **Apps & Services** ← **Payment Methods**. ثم تظهر التطبيقات في قائمة اختيار التطبيقات.

التطبيقات على الأجهزة الشخصية (تسجيل المستخدم)

لا تمتلك أجهزة iPhone وiPad الشخصية المسجّلة عبر تسجيل المستخدم رقم تسلسلي، لذا تحصل على تطبيقات App Store الخاصة بالسياسة بترخيص **مستخدم** لحساب Managed Apple Account المسجّل الدخول على الجهاز. ويسجّل Cerberus الحساب في Apps and Books ويعيّن التراخيص بنفسه، بما في ذلك التطبيقات المجانية. ويجب أن تنتمي حسابات Managed Apple Account ورموز Apps and Books إلى المؤسسة نفسها في Apple Business. ويستخدم التطبيق المدفوع ترخيصًا واحدًا لكل حساب، تشترك فيه جميع الأجهزة الشخصية لذلك الحساب.

- **في انتظار ترخيص مستخدم**: لا يُرسَل التطبيق إلى الجهاز إلا بعد أن تؤكد Apple ترخيصه، وعادةً خلال دقائق قليلة. وتعرض لوحة **التطبيقات** في الجهاز السبب.
- **فشل ترخيص المستخدم**: لم تتمكن Apple من تعيين الترخيص، مثلًا لأن تطبيقًا مدفوعًا لم يعد لديه ترخيص متبقٍ أو فات في Apple Business، ثم استخدم **إعادة الطلب**؛ ويحاول Cerberus أيضًا من جديد بنفسه كل يوم.
- **طلب التثبيت**: يسأل iOS المستخدم قبل تثبيت كل تطبيق. وإذا ألغى المستخدم، يعرض التطبيق **في انتظار موافقة المستخدم على التثبيت**؛ ويعرض **إعادة الطلب** الطلب مرة أخرى.
- **التحرير**: تؤدي إزالة التطبيق من السياسة أو إلغاء تسجيل آخر جهاز شخصي في الحساب إلى إزالة التطبيق وتحرير ترخيصه، ما لم يكن جهاز آخر مسجّل في الحساب نفسه لا يزال بحاجة إليه.

للاطلاع على التفاصيل، راجع **تسجيل Apple الموحّد بالحساب**.

التكوين المُدار

يمنح التكوين المُدار التطبيق إعداداته (مثل عنوان خادم أو اسم حساب)، بالطريقة التي يوثّقها مزوّد التطبيق. افتح التطبيق في السايسة وانقر على **إضافة تكوين مُدار**. ويُرسَل إلى أجهزة iPhone وiPad بنظام **iOS وأ iPadOS 18.4 وأ ث** وإلى أجهزة Mac بنظام **macOS 27 وأ أحدث**؛ ولم يُرسَل بعد إلى Apple Vision Pro. ويجب أن يدعم التطبيق التكوين المُدار: فالتطبيق الذي ال يقرأه يتجاهله. وتعرض لوحة التطبيق عدد المفاتيح بجانب اسم التطبيق.

- **المفاتيح**: يحتوي كل صف على مفتاح ونوع وقيمة. والأنواع هي Text وInteger وDecimal number وBoolean وDate وText list وInteger list. والمفاتيح حساسة لحالة الأحرف ويجب أن تكون فريدة. ويضيف **إضافة مفتاح** صفاً؛ ويحذف **إزالة التكوين** جميع المفاتيح.
- **المتغيرات**: يمكن أن تحتوي قيم Text وText list على $EMAIL$ و$USERNAME$ و$FULLNAME$ و$SERIAL$ و$UDID$، تُستبدَل بقيم كل جهاز ومستخدمه. ويُترك المتغير الذي ليس له قيمة (مثلاً $EMAIL$ على جهاز بال مستخدم) فارغاً، وتذكر سجالت النظام ذلك. وعندما تتغير تفاصيل مستخدم، تحصل الأجهزة على القيم الجديدة؛ وبالنسبة إلى المستخدمين المزامنين من Google Directory، تُحدَّث القيم عند التغيير التالي في السايسة أو في الجهاز.
- **استيراد تكوين**: افتح أو الصق الملف الذي ينشره مزوّد التطبيق لـ MDM، ثم انقر على **قراءة**. وملف **AppConfig specfile** (specfile.xml) يسرد لكل مفتاح يدعمه التطبيق مع وصفه ونوعه وقيمته االفتراضية وقيمه المسموح بها: حدد المفاتيح المراد استيرادها (تكون المفاتيح ذات القيمة االفتراضية محددة مسبقاً والمفاتيح الأخرى بعد االستيراد. ويظهر تحذير عندما يكون ملف specfile لتطبيق آخر. وتُستورد **قائمة الخصائص** (قائمة خصائص كاملة وأ <dict> الخاصة بها فقط) كما هي. ثم اختر ما إذا كنت تريد استبدال المفاتيح الحالية أو الإضافة إليها. والدعم القوائم ال تُدرج على المدخلة وقيم البيانات والقوائم ذات الأنواع المختلطة أو غير المعروفة، وتُدرج على أنها متخطاة. ال تنشر Apple مفاتيح تكوين التطبيقات، لذا اطلب الملف من المزوّد عندما ال يكون في وثائقه. وينسخ **نسخ كـ plist** التكوين كما يتلقاه الجهاز، قبل استبدال المتغيرات.
- **الحدود**: حتى 200 مفتاح لكل تطبيق؛ والمفاتيح حتى 255 حرفاً؛ والقيم النصية حتى 4096 حرفاً؛ والقوائم حتى 200 عنصر بطول 1024 حرفاً لكل عنصر؛ والتواريخ بين 1970 و9999؛ و64 كيلوبايت لكل تطبيق إجمالاً.
- **ليس لكلمات المرور**: يُرسَل التكوين فقط إلى الجهاز المُعدّ له، وتعرض السجالت أسماء المفاتيح وأنواعها فقط، لكن يمكن لمسؤولي لوحة التحكم قراءة القيم، كما يتغير العنوان الذي ينزّل منه الجهاز التكوين مع القيم، لذا يمكن استنتاج قيمة يسهل تخمينها (قيمة منطقية أو عدد صغير) منه. ال تضع كلمات المرور أو أي أسرار أخرى في تكوين مُدار.
- **الحالة**: عندما يُبلغ الجهاز بأن التطبيق لم يقبل تكوينه، تعرض لوحة التطبيقات في الجهاز **التكوين غير مقبول** بجانب التطبيق. وهذا ال يجعل الجهاز غير ممتثل. أما التكوين الذي ال يستطيع الجهاز تنزيله فيجعله غير ممتثل.

خيارات التطبيق

لكل تطبيق في السايسة (تطبيقات App Store والتطبيقات المخصصة) هذه الخيارات. ويترك **االفتراضي للجهاز** الخيار للجهاز. أما الأجهزة التي ال تدعم خياراً فلن تحصل عليه؛ ويبقى التطبيق مثبتاً.

- **التحديثات التلقائية**: إعداد App Store، إما Always أو Never. iOS وiPadOS وmacOS وvisionOS 26 وأحدث. وبالنسبة إلى التطبيقات المخصصة، يتصرف إعداد App Store كما لو كان Never.
- **التنزيلات عبر الشبكة الخلوية**: إعداد App Store، إما Always أو Never، للتثبيتات والتحديثات التلقائية. لأجهزة iPhone وiPad الخاضعة للإشراف بنظام iOS أو iPadOS 26 وأحدث فقط.
- **نسخ بيانات التطبيق احتياطيًا**: ما إذا كانت بيانات التطبيق مضمنة في نسخ الجهاز الاحتياطية. ليس على Mac.
- **يمكن للمستخدم إخفاء التطبيق** و**يمكن للمستخدم قفل التطبيق**: iOS وiPadOS 18.1 وأحدث، ويُفرَض على الأجهزة الخاضعة للإشراف. وعدم السماح بالقفل يمنع الإخفاء أيضًا. وينطبق القيدان **السماح بإخفاء التطبيقات** و**السماح بقفل التطبيقات** على جميع التطبيقات.
- **قفل الجهاز بعد معاملات Tap to Pay التي تتطلب رقم PIN الخاص بالعميل**: على iPhone فقط.
- **النطاقات المرتبطة**: النطاقات التي يرتبط بها التطبيق (مثل ًللوراطب العامة وأ التعبئة التلقائية لكلمة المرور)، بحد أقصى 50. أدخل أسماء مضيفين بسيطة مثل www.example.com، دون applinks: أو أحرف البدل أو ?mode=. ليس على Mac.
- **التحقق من النطاقات مباشرة**ً: يتحقق الجهاز من ملف ارتباط الموقع الخاص بالنطاقات مباشرة ًبدل ًمن التحقق عبر خوادم Apple. ال تمكّن هذه الخيارات إال للنطاقات الداخلية التي ال يمكن الوصول إليها من اإلنترنت.
- **اإلزالة**: ال يمكن للمستخدم إزالة التطبيقات المثبّتة بصفة **مطلوب**.

تطبيقات Mac App Store

تعرض قائمة اختيار التطبيقات منصات كل تطبيق (iPhone/iPad وMac وApple TV وVision)؛ ويُظهر التطبيق الموجود ألجهزة Mac فقط أيقونة Mac الخاصة به. وينطبق التطبيق الموجود ألجهزة Mac فقط على أجهزة Mac عند إضافته. والـ تطبيق App Store الذي ليس له إصدار Mac يُرسَل إلى أجهزة Mac: فتعرض السياسة "هذا التطبيق ليس له إصدار Mac: الـ يُرسَل إلى أجهزة Mac" ضمن **ينطبق على**. وتحصل أجهزة Mac على تطبيقات App Store بمعرّف App Store الخاص بها، إذا تُثبّت التطبيقات التي لها معرّف حزمة مختلف على Mac بشكل صحيح.

تطبيق Cerberus Enterprise

يثبّت Cerberus تطبيقه **Cerberus Enterprise** على كل جهاز iPhone وiPad يعمل بـ**iOS أو iPadOS 18.4 أو أحدث**، مع سياسة أو بدونها. يشارك التطبيق موقع الجهاز ويتلقى اإلشعارات وطلبات التتبّع المباشر. يُثبّت كـ**مطلوب**، بترخيص جهاز من Apps and Books (ترخيص مستخدم على الأجهزة الشخصية)، إذا ال يمكن للمستخدم حذفه.

- **إعداد لمرة واحدة**: أضف التطبيق المجاني إلى مكتبتك مرة واحدة. في Apple Business، افتح **Apps & Services** ← **Apps & Books** ← **App Store**، وابحث عن "Cerberus Enterprise"، وانقر على **View**، ثم **Add**، واختر **All current and future** في **Organizational Units**، ثم انقر على **Add**، ثم **Review** وأكّد. وإذا ظهر التطبيق **Manage** في مكتبتك: افتحه وتحقق من أن وحدته التنظيمية هي **All**، وهو موجود بالفعل

current and future units. وحتى ذلك الحين، تعرض لوحة التحكم شريطاً وتعرض الأجهزة التطبيق على أنه غير مثبّت. راجع **إعدادات الحساب**.

- **غير متاح في السياسات**: لا يمكن إضافة التطبيق إلى سياسة. وهو معطّل في قائمة اختيار التطبيقات ويُرفض كتطبيق مخصص (معرّف الحزمة نفسه). والسياسة التي تُدرج بالفعل تُزال منها الإدخال عند فتحها: احفظ السياسة للتأكيد.
- **غير مثبّت على**: الأجهزة التي تعمل بـiOS وأ iPadOS أقدم من 18.4. يُدعم iPad المشترك للتثبيت، لكن مميزات التطبيق غير مُتحقّق منها هناك.
- **الأجهزة الشخصية**: على أجهزة iPhone وiPad المسجّلة بـUser Enrollment، يُثبّت التطبيق أيضاً، مع طلب تثبيت وترخيص مستخدم لـManaged Apple Account. يتلقى الرسائل من مؤسستك، والوصول إلى الموقع إلا إذا فعّلت السياسة **الموقع والنطاقات الجغرافية على الأجهزة الشخصية** وسمح المستخدم بذلك.
- **يبقى مثبّتاً**: إذا انتهت صلاحية رمز Apps and Books أو غادر التطبيق مكتبتك، يبقى التطبيق على الأجهزة وتذكر صفحة الجهاز أن Apps and Books يحتاج إلى انتباهه. والإزالة إلا إذا كان التطبيق لا يزال مفقوداً من مكتبتك بعد 24 ساعة.

التطبيقات المخصصة

التطبيقات المخصصة هي تطبيقات iPhone وiPad الخاصة بك (ملفات .ipa)، توزّع دون App Store. في Xcode، صدّر التطبيق لتوزيع **Enterprise** (Apple Developer Enterprise Program: يُثبّت على كل جهاز) أو توزيع **Ad Hoc** (لا يُثبّت إلا على الأجهزة المسجّلة في ملف تعريف التوزيع الخاص به). ولا يمكن تحميل نسخ App Store.

انقر على **إضافة تطبيق مخصص** لفتح التطبيقات المخصصة لمؤسستك. ويضيف **تحميل تطبيق** ملف .ipa (بحد أقصى 2 غيغابايت). حدد تطبيقاً وانقر على **إضافة إلى السياسة**. وتعرض القائمة الإصدار ونوع التوقيع وعدد الأجهزة في ملف تعريف تطبيقات Ad Hoc وتاريخ انتهاء صلاحية ملف تعريف التوزيع.

- **إصدار جديد**: حمّل تطبيقاً بمعرّف الحزمة نفسه. فيحل محل الإصدار السابق، وتحدّث أجهزة السياسات التي تستخدمه التطبيق.
- **المتطلبات**: iPhone وiPad بنظام iOS 17.2 أو أحدث. والأجهزة التي لا تستطيع تثبيت التطبيق لا تحصل عليه: تطبيق خاص بـ iPad فقط على iPhone، أو نظام iOS أقدم مما يحتاجه التطبيق، أو جهاز ليس في ملف تعريف تطبيق Ad Hoc، أو ملف تعريف توزيع منتهي الصلاحية.
- **انتهاء الصلاحية**: عند انتهاء صلاحية ملف تعريف التوزيع، لا يفتح التطبيق بعد ذلك. حمّل إصداراً موقّعاً بملف تعريف جديد قبل تاريخ انتهاء الصلاحية.
- **معرّف حزمة محجوز**: لا يمكن إضافة تطبيق مخصص بمعرّف حزمة تطبيق Cerberus Enterprise (com.lsdroid.Cerberus.Enterprise) إلى سياسة، لأن Cerberus يثبّت ذلك التطبيق بنفسه.
- **حذف**: أزل التطبيق من سياساته أولاً؛ ثم تزيله الأجهزة.

حزم Mac

تقبل التطبيقات المخصصة أيضاً حزم مثبّت Mac (ملفات .pkg). يجب أن تكون الحزمة حزمة توزيع مبنية باستخدام **productbuild** (تُرفض الحزمة المكوّنة المصنوعة باستخدام pkgbuild

فقط) وموقّعة بشهادة **Developer ID Installer**. يُوصى بتوثيقها (notarizing) وإرفاق التذكرة بها (stapling) (**notarytool** و**stapler**). تُرفض الحزم غير الموقّعة، والحزم التي تغيّرت بعد التوقيع، والحزم الموقّعة بشهادات أخرى.

ارفع ملف .pkg باستخدام **رفع التطبيق** أو أضفه إلى السياسة: يظهر ضمن **حزم Mac**. تتجاهله أجهزة iPhone وiPad.

تستلم أجهزة Mac التي تعمل بنظام **macOS 26 أو أحدث** (خاضعة للإشراف، ويشمل ذلك أجهزة Mac المسجّلة يدويًا، باستثناء تسجيل المستخدم) الحزمَ بصفتها **إعلانًا (declaration)**: يقوم جهاز Mac بتنزيلها وتثبيتها وإعادة المحاولة وتحديثها بنفسه ويُبلغ عن حالتها. أما أجهزة Mac الأقدم، والحزم المثبّتة كتطبيقات مُدارة، فتستلمها عبر **أمر MDM**، على أي إصدار من macOS. ينتقل جهاز Mac الذي يُرقّى إلى macOS 26 إلى الإعلان تلقائيًا؛ وقد يثبّت لك حزمة مرة أخرى. يمكن أن يحدث الأمر نفسه عندما ينتقل جهاز Mac إلى سياسة أخرى تحتوي على الحزمة نفسها.

- **إصدار جديد**: ارفع حزمة بمعرّف الحزمة نفسه. يستبدل الإصدار السابق، وتثبّت أجهزة Mac في السياسات التي تستخدمه الإصدار الجديد.
- **أجهزة Mac المتخطّاة**: أجهزة Mac التي تعمل بإصدار macOS أقدم مما تسمح به الحزمة، وأجهزة Mac المزوّدة بمعالجات Intel بالنسبة للحزم المبنية لمعالجات Apple silicon فقط. تعرض صفحة الجهاز الحزمة على أنها متخطّاة، مع السبب؛ ويبقى الإصدار المثبّت سابقًا على جهاز Mac.
- **التثبيت**: **مطلوب** (افتراضي) يثبّت الحزمة على جهاز Mac؛ **اختياري** يجعل الحزمة متاحة على جهاز Mac دون تثبيتها. لا يعرض macOS 26 الحزم الاختيارية للمستخدم في إعدادات النظام أو App Store (تم الاختبار على macOS 26.3)، لذا يجب أن يثبّتها تطبيق أو برنامج نصي على جهاز Mac؛ اختر «اختياري» فقط إذا كان لديك واحد. ينطبق هذا على أجهزة Mac التي تعمل بنظام macOS 26 أو أحدث؛ أما أجهزة Mac الأقدم فتثبّت الحزمة دائمًا. الخيار غير متاح للحزم المثبّتة كتطبيقات مُدارة.
- **إزالة ملفات الحزمة عند خروجها من السياسة (macOS 27 أو أحدث)**: عند إزالة الحزمة من السياسة، تحذف أجهزة Mac التي تعمل بنظام macOS 27 أو أحدث الملفات التي ثبّتها. هذا الخيار معطّل افتراضيًا. على أجهزة Mac الأقدم تبقى الملفات. غير متاح للحزم المثبّتة كتطبيقات مُدارة.
- **التثبيت كتطبيق مُدار**: عيّن حزمة في السياسة لتثبيت تطبيقها كتطبيق مُدار (macOS 11 أو أحدث، وليس مع تسجيل المستخدم). عندها يُبلغ macOS عند فشل التثبيت، ويمكن لـ MDM إزالة التطبيق. يجب تثبيت التطبيق مباشرة في مجلد Applications، وموقّعًا بشهادة **Developer ID Application** وموثّقًا (notarized)؛ في macOS 11 إلى 13 يجب أن تحتوي الحزمة على ذلك التطبيق فقط (دون ملفات أو برامج نصية أخرى). تعرض التطبيقات المخصصة أي الحزم مؤهّلة. عندما يتعذّر تطبيق الخيار على جهاز Mac، تُثبّت الحزمة هناك كالمعتاد، وتوضّح صفحة الجهاز السبب.
- **خيارات الإزالة** لتطبيق مُدار: **إزالة التطبيق عند إزالة الحزمة من السياسة** (مفعّل افتراضيًا) و**إزالة التطبيق عند خروج جهاز Mac من الإدارة**. تؤدي إزالة تطبيق أيضًا إلى حذف بياناته. إذا كان المستخدم قد ثبّت التطبيق نفسه مسبقًا، تصبح تلك النسخة مُدارة وتُزال أيضًا.
- **الإزالة**: لا يمكن لأمر MDM إلغاء تثبيت حزمة. بالنسبة لحزمة مثبّتة كتطبيق مُدار، تؤدي إزالتها من السياسة إلى إزالة التطبيق (عند تفعيل الخيار)؛ وتبقى ملفاته الأخرى وإيصال الحزمة. تُزال الحزم التي يكون فيها خيار **إزالة ملفات الحزمة**

مفعّلًا من أجهزة Mac التي تعمل بنظام macOS 27 أو أحدث. الحزم الأخرى: إزالتها من السياسة توقف عمليات التثبيت الجديدة فقط، وتبقى الملفات على أجهزة Mac. جهاز Mac المتخطّى (مثلًا بعد إصدار جديد يتطلب macOS أحدث) يحتفظ بالتطبيق ما دامت الحزمة في السياسة؛ ثم تؤدي إزالة الحزمة من السياسة إلى إزالتها أيضًا. أزل الملفات المتبقية على جهاز Mac (مثلًا باستخدام أداة إلغاء التثبيت الخاصة بالحزمة)، وشغّل `sudo pkgutil --forget <identifier>` لنسيان إيصال الحزمة.

- **الحالة على الجهاز**: تعرض لوحة التطبيقات في جهاز Mac كل حزمة في السياسة على أنها في قائمة الانتظار، أو مقبولة (قبل جهاز Mac الأمر)، أو تم تنزيلها، أو مثبّتة (فقط للحزم التي تحتوي على تطبيقات، عندما يتم العثور على التطبيقات على جهاز Mac)، أو فاشلة (مع الخطأ). الـ يُبلغ macOS عن تثبيت حزمة أُرسلت بالأمر، لذا فإن «تم تنزيلها» هي الحالة الأخيرة للحزم بدون تطبيقات. تصبح الحزمة المثبّتة كتطبيق مُدار «فاشلة» أيضًا عندما يُبلغ macOS بأن التطبيق تعذّر تثبيته أو أُزيل من جهاز Mac. **التثبيت مرة أخرى** يرسل الحزمة إلى جهاز Mac مرة أخرى.
- **الحالة مع الإعلان**: تعرض الحزم المسلّمة كإعلان شريحة **الإعلان (Declaration)** والحالة التي يُبلغ عنها جهاز Mac: في قائمة الانتظار، أو متاحة (حزمة اختيارية لم يثبّتها المستخدم)، أو في انتظار المستخدم، أو قيد التنزيل، أو قيد التثبيت، أو مثبّتة، أو فاشلة (مع السبب، مثلًا فشل تنزيل أو تثبيت، أو إعلان رفضه جهاز Mac). تشير شريحة **الملفات المُزالة مع السياسة** إلى الحزم التي يحذف جهاز Mac يعمل بنظام macOS 27 ملفاتها عند خروجها من السياسة. الـ يظهر **التثبيت مرة أخرى** إلا بعد الفشل ويطلب من جهاز Mac إعادة المحاولة؛ والـ يُعرض عندما يرفض جهاز Mac الإعلان.

الحسابات

تتيح لكل لوحة **الحسابات** تكوين حسابات تُطبّق على الأجهزة المُدارة. وتتضمن أيضًا مفتاح تبديل قيد لتعديل الحسابات.

القيد

- **السماح بتعديل الحساب**: عند تعطيله، لا يمكن للمستخدمين تعديل حسابات مثل حسابات Apple وحسابات الإنترنت.

إضافة حسابات

استخدم **إضافة حساب Google** أو **إضافة حساب بريد** لإضافة حمول الحسابات إلى السياسة. يظهر كل حساب كبطاقة تحتوي على حقول التكوين الخاصة به.

بيانات اعتماد الحساب من المستخدمين

توفّر بطاقات حسابات Google والبريد كلتاهما مفتاح تبديل **بيانات اعتماد الحساب من المستخدمين**. عند تفعيله، يطبّق النظام بيانات اعتماد الحساب على أساس كل مستخدم.

وعند تعطيله، تُدخل هوية الحساب في السياسة.

حقول حساب Google

- **الاسم المرئي**: الاسم المعروض للمستخدم للحساب.
- **عنوان بريد Google الإلكتروني**: عنوان البريد الإلكتروني للمستخدم.
- **الاسم الكامل**: الاسم الكامل للمستخدم.

حقول حساب البريد

تتضمن حسابات البريد حقول الهوية إضافة إلى تكوين خادم البريد الوارد/الصادر. أسماء المضيف مطلوبة.

- **الاسم المرئي**: الاسم المعروض للمستخدم لحساب البريد.
- **عنوان البريد الإلكتروني**: عنوان البريد الإلكتروني للمستخدم.
- **الاسم الكامل**: الاسم الكامل للمستخدم.

الخادم الوارد

- **نوع الخادم**: بروتوكول البريد (مثلاً IMAP أو POP).
- **طريقة المصادقة**: طريقة المصادقة للخادم.
- **بادئة مسار IMAP**: تُعرض فقط عندما يكون نوع الخادم IMAP.
- **اسم المضيف**: مطلوب.
- **المنفذ**: منفذ الخادم (1–65535).

الخادم الصادر

- **طريقة المصادقة**
- **اسم المضيف**: مطلوب.
- **المنفذ**: منفذ الخادم (1–65535).

خيارات S/MIME

بالنسبة لحسابات البريد، يمكنك أيضاً تكوين سلوك تشفير S/MIME وتوقيعه.

التشفير

- **تشفير S/MIME**
- **هوية قابلة للتجاوز من المستخدم**
- **مفتاح لكل رسالة مفعّل**
- **قابل للتجاوز من المستخدم**

التوقيع

- **توقيع S/MIME**
- **هوية قابلة للتجاوز من المستخدم**
- **قابل للتجاوز من المستخدم**

> تتضمن خيارات الحساب والقيد تلميحات في لوحة التحكم توثّق المتطلبات المسبقة وإصدارات أنظمة التشغيل المدعومة.

وضع الكشك والشاشة الرئيسية

يثبّت قسم **وضع الكشك والشاشة الرئيسية** في محرّر سياسة Apple الأجهزة على تطبيق واحد، ويختار التطبيقات التي يمكن فتحها، ويرتّب الشاشة الرئيسية ويضيف رموز مواقع الويب. يُثبّت كل إعداد على الأجهزة كملف تعريف تكوين.

> تطبّق Apple معظم هذه الإعدادات على أجهزة iPhone وiPad الخاضعة للإشراف فقط (الأجهزة المسجّلة عبر Automated Device Enrollment أو المُعدّة باستخدام Apple Configurator). لا تحصل الأجهزة الأخرى عليها. تعمل مقاطع الويب أيضًا على أجهزة iPhone وiPad غير الخاضعة للإشراف. لا تحصل أجهزة Mac على أي من هذه الإعدادات.

اختيار التطبيقات

تُعرّف التطبيقات بمعرّف الحزمة (bundle ID) الخاص بها. اكتب اسم تطبيق لاختياره من تطبيقات Apple المضمّنة وتطبيقات السياسة، أو اكتب أي معرّف حزمة، مثلًا `com.example.app`.

وضع التطبيق الواحد

يشغّل الجهاز التطبيق المختار فقط: لا يمكن للمستخدمين العودة إلى الشاشة الرئيسية أو فتح تطبيقات أخرى. ثبّت التطبيق بالسياسة أولًا. يخرج الجهاز من وضع التطبيق الواحد عند إيقاف الإعداد أو إزالة التطبيق.

- **الخيارات**: عطّل شاشة اللمس أو التدوير أو أزرار مستوى الصوت أو مفاتيح الرنين/الصامت أو الزر الجانبي أو القفل التلقائي، وفعّل ميزات الوصول مثل VoiceOver أو Zoom.
- **ميزات الوصول التي يمكن للمستخدم تفعيلها**: ميزات يمكن للمستخدم تفعيلها بالنقر ثلاث مرات على الزر الجانبي.

التطبيقات المسموح بها والمحظورة

- **التطبيقات المحظورة**: تخفي الأجهزة هذه التطبيقات والا تفتحها. `com.apple.webapp` يحظر جميع مقاطع الويب. لا يمكن حظر الإعدادات، والا تطبيق Phone على iPhone.
- **السماح ببعض التطبيقات فقط**: تعرض الأجهزة هذه التطبيقات فقط. اترك القائمة فارغة للسماح بجميع التطبيقات. يضيف **تطبيقات السياسة** التطبيقات المثبّتة بواسطة السياسة؛ ويسمح معرّف `com.apple.webapp` بكل مقاطع الويب.
- **التطبيقات التي يمكنها بدء وضع التطبيق الواحد**: تطبيقات يمكنها قفل الجهاز على نفسها أثناء حاجتها إليه، مثلاً أثناء اختبار.

> مع **السماح ببعض التطبيقات فقط**، يختفي من الأجهزة كل تطبيق غير موجود في القائمة، بما في ذلك تطبيقات السياسة. تبقى الإعدادات دائماً، وكذلك تطبيق Phone على iPhone.

تخطيط الشاشة الرئيسية

رتّب الـ Dock وصفحات الشاشة الرئيسية. أضف التطبيقات ومجلدات التطبيقات ومقاطع الويب الخاصة بالسياسة، واختر الموضع عبر **إضافة إلى**، واسحب الرموز لنقلها بين الـ Dock والصفحات. انقر على مجلد لتغيير اسمه وتطبيقاته.

لا يمكن للمستخدمين نقل الأيقونات أو إزالة التطبيقات من الشاشة الرئيسية. تنتقل التطبيقات غير الموجودة في التصميم إلى الصفحات التي تلي الصفحات التي حدّدتها. يعرض iPhone أربع أيقونات في الـ Dock. لا يزال بإمكان المستخدمين حذف التطبيقات غير المطلوبة في شاشة التخزين في الإعدادات. لمنع ذلك، أوقف **السماح بإزالة التطبيقات** في إدارة التطبيقات.

مقاطع الويب

مقطع الويب هو رمز على الشاشة الرئيسية يفتح موقع ويب. حدّد التسمية وعنوان URL، واختياريًا صورة (PNG أو JPEG، مقصوصة إلى مربع).

- **يمكن للمستخدمين إزالته**: عطّله للإبقاء على الرمز على الأجهزة.
- **ملء الشاشة**: يُفتح موقع الويب كتطبيق ويب، دون شريط عنوان Safari. كما يفتح **البقاء بملء الشاشة على مواقع أخرى** الروابط المؤدية إلى مواقع أخرى في تطبيق

الويب.

- **الفتح باستخدام هذا التطبيق**: تطبيق يفتح عنوان URL بدلاً من Safari.

إعدادات الإشعارات

اختر كيفية عرض الأجهزة لإشعارات بعض التطبيقات: ما إذا كانت مسموحاً بها، وأين تظهر (شاشة القفل، مركز الإشعارات، CarPlay)، والشارات، والأصوات، والتنبيهات الحرجة، ونمط الشريط، والتجميع، والمعاينات. لا يمكن للمستخدمين تغيير هذه الإعدادات.

رسالة شاشة القفل

رسالة تُعرض أسفل شاشة القفل، مثلاً بمن يجب الاتصال إذا عُثر على الجهاز، ووسم أصل. يمكن أن يحتوي كل هام على المتغيرات $EMAIL$ و$USERNAME$ و$FULLNAME$ و$SERIAL$ و$UDID$: يُترك المتغير الذي ليس له قيمة للجهاز فارغاً.

رمز المرور

يتحكم قسم **إعدادات رمز المرور** في متطلبات رمز مرور الجهاز وقواعد الأمان ذات الصلة (على سبيل المثال، الحد الأدنى للطول والتعقيد). على Mac (macOS 13 أو أحدث، وليس مع تسجيل المستخدم) تنطبق القواعد على كلمة مرور تسجيل الدخول للمستخدمين.

الخيارات

في محرّر سياسة Apple، تُكوّن خيارات رمز المرور باستخدام مزيج من مفاتيح التبديل والحقول الرقمية. تتضمن حقول كثيرة تلميحات تشير إلى إصدارات أنظمة التشغيل المدعومة ومتطلبات الإشراف.

مفاتيح تبديل رمز المرور

- **التغيير عند المصادقة التالية**: فرض إعادة تعيين رمز المرور في المرة التالية التي يصادق فيها المستخدم.
- **اشتراط رمز مرور أبجدي رقمي**: اشتراط حرف أبجدي واحد على الأقل ورقم واحد.
- **اشتراط رمز مرور معقّد**: اشتراط رمز مرور «معقّد» (دون أنماط متكررة أو متتابعة، ومع حرف واحد على الأقل غير أبجدي رقمي).
- **اشتراط رمز المرور**: اشتراط رمز مرور دون متطلبات إضافية للطول أو الجودة. ملاحظة: تعيين مفاتيح أخرى لرمز المرور يستلزم ضمنًا رمز مرور.

الحقول الرقمية

- **إعادة تعيين المحاولات الفاشلة (دقائق)**: الدقائق قبل إعادة تعيين عدّاد المحاولات الفاشلة (يتطلب الحد الأقصى للمحاولات الفاشلة).
- **الحد الأقصى للمحاولات الفاشلة**: المحاولات الفاشلة المسموح بها قبل محو جهاز iPhone أو iPad، أو قفل جهاز Mac (النطاق: 2–11).
- **الحد الأقصى لفترة السماح (دقائق)**: المدة التي يمكن فيها إبقاء الجهاز مفتوحًا دون طلب رمز المرور (0 = بلا حد).
- **الحد الأقصى للخمول (دقائق)**: مدة الخمول قبل قفل الجهاز (النطاق: 0–15).
- **الحد الأقصى لعمر رمز المرور (أيام)**: الحد الأقصى لعمر رمز المرور قبل تغييره قسرًا (النطاق: 0–730).
- **الحد الأدنى للأحرف المعقّدة**: الحد الأدنى لعدد الأحرف «المعقّدة» (النطاق: 0–4).
- **الحد الأدنى للطول**: الحد الأدنى لطول رمز المرور (النطاق: 0–16).
- **حد إعادة استخدام رمز المرور**: طول سجل رموز المرور لمنع إعادة استخدام رموز قديمة (النطاق: 1–50).

القيود

تتحكّم أقسام القيود في ميزات نظام التشغيل المسموح بها على أجهزة Apple المُدارة. في محرّر سياسة Apple، تُعرض هذه الخيارات كلوحات مجمّعة بها عدة مفاتيح تبديل.

توُصف مفاتيح التبديل في لوحتي **إدارة التطبيقات** و**الشبكات** في صفحتي التطبيقات وملفات التعريف والشبكات في سياسات Apple.

> تدعم إصدارات معينة من أنظمة التشغيل كثيرًا من القيود فقط، وقد تتطلب أجهزة خاضعة للإشراف. استخدم التلميحات في لوحة التحكم لمعرفة المتطلبات المعتمدة.

> على أجهزة تسجيل المستخدم (الأجهزة الشخصية المسجّلة بتسجيل الدخول بحساب عمل)، لا تُرسل القيود التي لا تسمح بها Apple هناك. إذا لم ينطبق أي من قيود السياسة، فلا تتلقى هذه الأجهزة ملف تعريف قيود. يعرض محرّر السياسة عدد القيود التي لا تنطبق على أجهزة تسجيل المستخدم.

الأمان

- **السماح بالفتح التلقائي**
- **السماح ببصمة الإصبع للفتح**
- **السماح بتعديل بصمة الإصبع**
- **السماح بمحو المحتوى والإعدادات**
- **السماح بتمكين القيود**
- **السماح بتثبيت ملفات التعريف بواسطة المستخدمين**
- **السماح بالاقتران مع المضيف**
- **السماح بإرسال البيانات التشخيصية**
- **السماح بتعديل إرسال البيانات التشخيصية**
- **السماح بالإعلانات الشخصية من Apple**
- **السماح بتعديل Remote Management**

الوسائط المتعددة

- **السماح بالكاميرا**
- **السماح بتعديل مشاركة الملفات**
- **السماح لتطبيق الملفات بالوصول إلى محركات USB**

- **السماح بتسجيل المكالمات**
- **السماح بـ AirPrint**
- **السماح بتخزين بيانات اعتماد AirPrint**
- **السماح باكتشاف iBeacon الخاص بـ AirPrint**

الشبكة الخلوية

- **السماح بتعديل بيانات الشبكة الخلوية للتطبيقات**
- **السماح بتعديل خطة الشبكة الخلوية**
- **السماح بتعديل eSIM**
- **السماح بعمليات نقل eSIM الصادرة**
- **الاحتفاظ بشريحة eSIM عند محو الجهاز**
- **السماح بالجلب في الخلفية أثناء التجوال**

APN للشبكة الخلوية

APN للشبكة الخلوية يعيّن اسم نقطة الوصول (APN) الذي منحك إياه مشغّلك، مثلاً لشبكة جوال خاصة أو تجارية. عيّن **اسم نقطة الوصول** وإذا طلب المشغّل ذلك، المصادقة (PAP أو CHAP)، واسم المستخدم (المتغيرات مثل $EMAIL$ مسموح بها)، وكلمة المرور، وإصدارات IP (أيضاً عند التجوال)، وخادم وكيل مع منفذه وXLAT464. فعّل **إرفاق APN** فقط إذا منحك المشغّل APN منفصلاً للاتصال بالشبكة.

- لا تتلقاه إلا أجهزة iPhone وiPad المزوّدة بشريحة اتصال خلوي، حتى دون إشراف. لا تتلقاه الأجهزة المسجّلة بتسجيل المستخدم (الأجهزة الشخصية).
- ينطبق على شريحة SIM المستخدمة لبيانات الجوال فقط. لا يثبّت الجهاز الذي لديه ملف تعريف APN مثبّت بطريقة أخرى.
- تُحمى كلمة المرور مثل كلمات مرور الشبكة الأخرى: لا يُرسل ملف التعريف إلا إلى الجهاز المعدّله، ولا تُكتب كلمة المرور في السجلات.

> قد يترك APN خاطئ الأجهزة دون بيانات جوال: جرّب الإعدادات على جهاز اختبار بشريحة SIM من المشغّل أولاً.

النظام وواجهة المستخدم

- **السماح بـHandoff**
- **السماح بالتصحيح التلقائي**
- **السماح بالتعتيم التلقائي**
- **السماح بشاشة التوقف التلقائية**

- السماح بلوحة مفاتيح QuickPath
- السماح بالبحث عن التعريفات
- السماح بتعديل اسم الجهاز
- السماح بسكون الجهاز
- السماح بـiPhone Mirroring
- السماح بأدوات iPhone على Mac
- السماح باختصارات لوحة المفاتيح

تطبيقات Apple وخدماتها

- السماح بـiMessage
- السماح بـGame Center
- السماح بإضافة أصدقاء Game Center
- السماح بـFind My للجهاز
- السماح بـFind My للأصدقاء
- السماح بتعديل Find My للأصدقاء
- السماح بـBook Store
- السماح بمحتوى Book Store للبالغين
- السماح بالنسخ الاحتياطي لكتب المؤسسة
- السماح بمزامنة بيانات كتب المؤسسة الوصفية
- السماح بـiTunes Store
- السماح بالمحتوى الصريح

Apple Intelligence وSiri

- السماح بـSiri
- السماح بمحتوى Siri الذي ينشئه المستخدم
- السماح بـSiri أثناء القفل
- السماح بالإملاء
- السماح بعمليات تكامل الذكاء الخارجي
- السماح بتسجيل الدخول إلى الذكاء الخارجي
- السماح بـGenmoji
- السماح بـImage Playground
- السماح بـImage Wand

iCloud

- السماح بدفتر عناوين iCloud

- **السماح بنسخ iCloud الاحتياطي**
- **السماح بإشارات iCloud المرجعية**
- **السماح بتقويم iCloud**
- **السماح بسطح مكتب iCloud والمستندات**
- **السماح بمزامنة مستندات iCloud**
- **السماح بـ iCloud Freeform**
- **السماح بمزامنة سلسلة مفاتيح iCloud**
- **السماح ببريد iCloud**
- **السماح بـ iCloud Notes**
- **السماح بمكتبة صور iCloud**
- **السماح بـ iCloud Private Relay**
- **السماح بتذكيرات iCloud**

الحسابات (قيد)

تحتوي لوحة الحسابات على قيد وإعداد الحسابات (اختياريًا). يتحكم مفتاح القيد في ما إذا كان المستخدم يستطيع تعديل حسابات النظام.

- **السماح بتعديل الحسابات**

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 تبث أسماءها).
- **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 المعدّة له: يجب أن يوقّع الجهاز طلبه بشهادة الإدارة الخاصة به. لا تُكتب كلمات المرور والشهادات في السجلات.

تحديثات البرامج

يحافظ قسم **تحديثات البرامج** في محرر سياسة Apple على تحديث الأجهزة: يمكنه فرض إصدار نظام تشغيل معين بحلول موعد نهائي، والتحكم في كيفية تنزيل الأجهزة للتحديثات وتثبيتها.

تحديثات نظام التشغيل المطلوبة

انقر على **إضافة تحديث مطلوب** لفرض إصدار نظام تشغيل. ينزّل الجهاز التحديث، ويُبلغ المستخدم بالموعد النهائي، ويثبّته عند حلول الموعد إذا لم يكن قد فعله من قبل. تتجاهله الأجهزة التي تعمل بالفعل بهذا الإصدار أو بإصدار أحدث. يتطلب iOS وiPadOS 17 أو macOS 14.

- **ينطبق على** (مطلوب): iPhone وiPad، أو Mac. لكل نظام تشغيل أرقام إصدارات خاصة به، لذا أضف تحديثاً مطلوباً واحداً لكل منها.
- **إصدار نظام التشغيل**: الإصدار المراد تثبيته، مثل 18.5 أو 15.4.1.
- **البنية** (اختياري): بنية محددة، مثل نسخة تجريبية أو تحسين أمان في الخلفية.
- **التثبيت بحلول**: الموعد النهائي، بالتوقيت المحلي لكل جهاز. يجعل تاريخ في الماضي الأجهزة تثبّت التحديث في أقرب وقت ممكن.
- **رابط التفاصيل** (اختياري): صفحة ويب حول التحديث تُعرض للمستخدم.

> يُبلغ الجهاز عن تقدّم التحديث (التنزيل، التثبيت، الأعطال) في لوحة **حالة الجهاز** في صفحة الجهاز.

إعدادات تحديثات البرامج

عبّئ **إعدادات تحديثات البرامج لـ iPhone وiPad** أو **إعدادات تحديثات البرامج لـ Mac** للتحكم في التحديثات على تلك الأجهزة. عندما يكون أحد المفاتيح متوقفاً، تحتفظ الأجهزة بإعداداتها الخاصة. يتطلب iOS وiPadOS 18 أو macOS 15: تتجاهل الأجهزة الأقدم هذه الإعدادات.

- **تأجيل التحديثات**: لا تُعرض التحديثات الجديدة للمستخدم إلا بعد عدد الأيام المحدد (من 1 إلى 90). على Mac، يمكنك تعيين فترات مختلفة للتحديثات الرئيسية والتحديثات الثانوية وتحديثات النظام الأخرى.

- **التحديثات المعروضة للمستخدم** (iPhone وiPad): عندما يتوفر أكثر من تحديث، اعرضها كلها، أو أقدم تحديث ثانوي فقط، أو الأحدث فقط.
- **يمكن للمستخدمين العاديين تثبيت التحديثات** (Mac): يمكن للمستخدمين دون حقوق مسؤول تثبيت تحديثات macOS.
- **إبلاغ المستخدم بالتحديثات المطلوبة**: اعرض الإشعارات المتعلقة بالتحديثات المطلوبة ومواعيدها النهائية.
- **التنزيل التلقائي**، و**التثبيت التلقائي**، و**تحديثات الأمان التلقائية**: اترك القرار للمستخدم (الوضع الافتراضي في Apple)، أو أبقِها مفعّلة دائماً أو متوقفة دائماً.
- **تحسينات الأمان في الخلفية**: قدّم إصلاحات الأمان السريعة من Apple للمستخدم، واختر ما إذا كان يمكنه إزالتها.
- **برامج النسخ التجريبية**: اسمح للمستخدم بالانضمام إلى برامج Apple التجريبية، أو أزل الجهاز منها واحظرها (على iPhone وiPad، للأجهزة الخاضعة للإشراف فقط).

تثبيت تحديث من صفحة الجهاز

تسرد لوحة **حالة الجهاز** لأي جهاز التحديثات المتاحة له. استخدم **التحقق من التحديثات** لطلب القائمة من الجهاز، و**تثبيت** لتثبيت أحدها الآن أو لتنزيله وترك المستخدم يثبّته. يعمل هذا على أجهزة iPhone وiPad الخاضعة للإشراف وعلى أجهزة Mac. تزيل Apple هذه الأوامر في iOS وiPadOS وmacOS 27: في تلك الإصدارات استخدم التحديثات المطلوبة في السياسة.

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، والامتدادات النظام والنواة المسموح بتحميلها. كما يثبّت ملفات تكوين خدمات النظام والمهام الخلفية. لا تتلقى الأجهزة الأخرى في السياسة هذه الإعدادات. فعّل إعداداً 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 معتمداً 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 لاحقاً، يتلقى جهاز Mac هذه الإعدادات تلقائياً.

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، مشفّراً بمفتاح يخص مؤسستك فقط. يُعرض المفتاح ويُعيّر من حقل **FileVault** في صفحة الجهاز (راجع أوامر الجهاز). يتطلب الإعداد macOS 13 أو أحدث وMDM معتمداً 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 افتراضياً، إذا يعرف المفتاح المسؤولون فقط، من صفحة الجهاز.
- **منع إيقاف FileVault**: مفعّل افتراضياً.
- **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، مثلاً 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.

الموقع والأسيجة الجغرافية

يحدّد قسم **الموقع والأسيجة الجغرافية** في محرّر سياسة Apple مناطق، على سبيل المثال موقع أو مستودع. تبلّغ أجهزة iPhone وiPad التي عليها تطبيق Cerberus Enterprise عند دخولها إحدى هذه المناطق أو خروجها منها، ويمكن لقواعد الأحداث الاستجابة لذلك: إرسال بريد إلكتروني، أو قفل الجهاز أو تعطيله، أو تمكينه مرة أخرى. لا تستخدم أجهزة Mac الأسيجة الجغرافية.

حقول السياج الجغرافي

استخدم **إضافة سياج جغرافي** لإنشاء إدخال جديد. يمكن أن تحتوي السياسة على ما يصل إلى **10 سياجات جغرافية**، ويجب أن تكون أسماؤها فريدة داخل السياسة. يحتوي كل سياج جغرافي على هذه الحقول:

- **الاسم**: مطلوب وفريد.
- **خط العرض** و**خط الطول**: مركز المنطقة. يمكنك أيضًا النقر على الخريطة لتعيينه.
- **نصف القطر (م)**: مطلوب، من **200** إلى **10000** متر.
- **الوصف**: ملاحظات اختيارية للمسؤولين.
- **الإبلاغ عن الدخول** و**الإبلاغ عن الخروج**: اختر الأحداث التي تُنشأ. يجب أن يبقى واحد على الأقل مفعّلًا.
- **نشط**: يفعّل السياج الجغرافي أو يعطّله دون حذفه.

لكل سياج جغرافي معاينة خريطة. مركز السياج الجغرافي المحفوظ ونصف قطره مقفلان: استخدم زر القفل على الخريطة لتغييرهما. أما الأزرار الأخرى فتُوسّط الخريطة على المنطقة أو على موقعك الحالي.

عند حفظ السياسة، يطلب Cerberus Enterprise من أجهزة iPhone وiPad التابعة للسياسة الحصول على السياجات الجغرافية الجديدة. يستغرق هذا عادة بضع دقائق، لكن iOS قد يؤخّره، مثلًا في وضع الطاقة المنخفضة أو دون اتصال بالشبكة. تعرض صفحة الجهاز متى لم يطبّق التطبيق أحدث السياجات الجغرافية بعد.

المتطلبات

تعمل السياجات الجغرافية على أجهزة iPhone وiPad التي لديها تطبيق Cerberus Enterprise. تتجاهلها أجهزة Mac. على الجهاز:

- يكون تطبيق Cerberus Enterprise مثبّتًا (يثبّته Cerberus) وقد فتح المستخدم مرة واحدة على الأقل؛
- يكون الوصول إلى الموقع للتطبيق مضبوطًا على **دائمًا**؛

- يكون **الموقع الدقيق** مفعّلًا للتطبيق؛
- يكون **تحديث التطبيقات في الخلفية** مفعّلًا.

> **الموقع والسياجات الجغرافية على الأجهزة الشخصية**، في أعلى القسم، معطّل افتراضيًا. وبينما هو معطّل، لا يجمع Cerberus موقع الأجهزة الشخصية (تسجيل المستخدم)، ولا تُنشأ أحداث سياجاتها الجغرافية، ولا تقدّم صفحة جهازها خيار «تحديد الموقع» أو التتبّع المباشر. عند تفعيله، تشارك الأجهزة الشخصية في السياسة موقعها وأحداث سياجاتها الجغرافية مثل أجهزة الشركة، لكن فقط إذا سمح المستخدم بالوصول إلى الموقع لتطبيق Cerberus Enterprise؛ ويوضّح التطبيق ذلك للمستخدم قبل أن يطلب iOS الإذن. مؤسستك مسؤولة عن إبلاغ المستخدمين وعن الالتزام بالقوانين المحلية بشأن موقع الموظفين. لا يتوفر وضع الفقدان وطلب الموقع عبر MDM أبدًا على الأجهزة الشخصية (لا تسمح Apple بهما).

في **وضع الطاقة المنخفضة** تستمر السياجات الجغرافية في العمل، لكن iOS يُبلغ عن مغادرة منطقة لاحقًا وبموقع أقل دقة، ويمكنه تأخير الحصول على سياجات جغرافية جديدة بعد تغيير السياسة لساعات، حتى يعمل التطبيق مرة أخرى (مثلًا عند العبور التالي، أو عندما يفتحه المستخدم).

كيفية وصول الأحداث

يراقب iOS المناطق للتطبيق ويوقظه عندما يعبر الجهاز حدًا، حتى عندما لا يكون التطبيق مفتوحًا. قد تصل الأحداث بعد بضع دقائق من العبور، وقد تُوفّت منطقة صغيرة أو زيارة قصيرة: يحتاج iOS إلى أن يتحرّك الجهاز مسافة معينة بعد الحد وأن يبقى هناك لبعض الوقت.

إذا تعذّر على التطبيق العمل، مثلًا بعد إعادة تشغيل قبل فتح قفل الجهاز، يكتشف الخادم العبور أيضًا من المواقع التي يرسلها التطبيق، لاحقًا. كل عبور يفعّل قواعد الأحداث مرة واحدة، سواء اكتشفه التطبيق أو الخادم.

عندما لا يتصل التطبيق بالخادم لعدة ساعات، يطلب الخادم من iOS إيقاظه ليتمكّن من فحص سياجاته الجغرافية مرة أخرى. لا يضمن iOS هذه الطلبات.

صفحة الجهاز

في صفحة الجهاز، تعرض علامة التبويب **السياج الجغرافي** في لوحة **خريطة الموقع** انتقالات الجهاز. عندما تحتوي السياسة على سياجات جغرافية نشطة، يوضّح سطر حالة ما إذا كانت السياجات الجغرافية تعمل على الجهاز، أو سبب تعذّر ذلك: لم يتصل التطبيق بالخادم أو يجب تحديثه، أو أن الوصول إلى الموقع ليس **دائمًا**، أو أن **الموقع الدقيق** أو **تحديث التطبيقات في الخلفية** معطّل، أو أن **وضع الطاقة المنخفضة** كان مفعّلًا عندما أبلغ التطبيق عن إعداداته آخر مرة، أو أن التطبيق لم يطبّق أحدث السياجات الجغرافية بعد.

تُحفظ انتقالات الأسيجة الجغرافية والمواقع لمدة **90 يومًا** وتُحذف البيانات الأقدم تلقائيًا كل ليلة. ويُحفظ دائمًا آخر موقع لكل جهاز مسجّل، لذا يظل الجهاز على الخرائط.

القيود

- نسخ سياسة ال ينسخ سياجاتها الجغرافية: أضفها مرة أخرى في النسخة.
- أحداث السياجات الجغرافية على أجهزة iPhone وiPad تُنفّذ قدر الإمكان: يقرّر iOS متى يمكن للتطبيق العمل.

للتفاعل مع أحداث السياجات الجغرافية، أنشئ قاعدة حدث لـ **دخول الجهاز إلى سياج جغرافي** أو **خروج الجهاز من سياج جغرافي**. راجع **قواعد الأحداث**.

الحسابات

يضيف قسم **الحسابات** في محرر سياسة Apple حسابات البريد وExchange وGoogle والتقويم وجهات الاتصال والدليل إلى أجهزة iPhone وiPad وMac. انقر على **إضافة حساب** واختر النوع. ويحتوي القسم أيضاً على قيد **السماح بتعديل الحساب** (الأجهزة الخاضعة للإشراف).

> على جهاز Mac (macOS 13 أو أحدث)، تُثبّت الحسابات في جلسة المستخدمين المسجّلين في الإدارة، وعادةً المستخدم الذي سجّل جهاز Mac، عند تسجيل دخولهم. وتُدرج صفحة الجهاز هؤلاء المستخدمين ضمن **مستخدمو Mac**، مع حالة حساباتهم. أما الحسابات التي تأخذ عنوان البريد الإلكتروني من مستخدم الجهاز فتستخدم المستخدم المعيّن لجهاز Mac في Cerberus Enterprise.

الإعدادات الشائعة

- **اسم مستخدم الجهاز وبريده الإلكتروني** (Mail وExchange وGoogle): يستخدم كل جهاز اسم مستخدمه وعنوان بريده الإلكتروني كما هو محدد في صفحة المستخدمين (وبالنسبة إلى Google، حساب Google الخاص بالمستخدم). أما الأجهزة التي ليس لها مستخدم، أو التي ليس لمستخدمها عنوان بريد إلكتروني، فلا تحصل على الحساب. وفي غير ذلك، عيّن عنوان بريد إلكتروني واسماً كاملاً ثابتين.
- **اسم الحساب** (اختياري): اسم الحساب في الإعدادات وفي التطبيقات.
- **اسم المستخدم وكلمة المرور** (اختياري): يمكن أن يحتوي اسم المستخدم على المتغيرات $EMAIL$ و$USERNAME$ و$FULLNAME$ و$SERIAL$ و$UDID$. اترك كلمة المرور فارغة ليُدخلها المستخدم على الجهاز، أو اترك كليهما فارغين ليُدخلهما المستخدم.
- **ينطبق على**: قصر الحساب على أنواع معينة من الأجهزة.

أنواع الحسابات

- **حساب البريد**: خادم وارد IMAP أو POP وخادم صادر، مع منافذهما ومصادقتهما. يمكن للخادم الصادر استخدام اسم المستخدم وكلمة المرور نفسيهما المستخدمين في الخادم الوارد.
- **حساب Exchange** (Exchange ActiveSync): الخادم، أو اتركه فارغاً لاستنتاجه من عنوان البريد الإلكتروني. اختر الخدمات (البريد وجهات الاتصال والتقويمات والتذكيرات والملاحظات) وما إذا كان يمكن للمستخدم تغييرها. مع **المصادقة الحديثة (OAuth)**، يسجّل المستخدم الدخول عبر صفحة مزوّد الهوية لديك، مثل Microsoft 365. وتصادق **شهادة المصادقة** (iOS 17 أو أحدث) على الجهاز باستخدام شهادة.
- **حساب Google**: يسجّل المستخدم الدخول إلى حساب Google بعنوان البريد الإلكتروني المحدد.

- **حساب التقويم (CalDAV)** و**حساب جهات الاتصال (CardDAV)**: الخادم والمنفذ والمسار.
- **الدليل (LDAP)**: الخادم والمنفذ، وعمليات البحث (قاعدة البحث والنطاق والوصف) المستخدمة للبحث عن جهات الاتصال.
- **تقويم مشترك**: عنوان URL للتقويم (https أو http أو webcal).

S/MIME

يمكن لحسابات البريد وExchange توقيع الرسائل وتشفيرها باستخدام S/MIME (iOS 17 أو أحدث). ولكل حساب، اختر الشهادة: إحدى الشهادات من صفحة الشهادات، أو شهادة مستخدم الجهاز، أو شهادة تُطلب من خادم SCEP. يمكنك السماح للمستخدم بإيقافها واختيار شهادة أخرى، وبالنسبة إلى التشفير، عرض مفتاح لكل رسالة.

الأمان

ليست كلمات المرور والشهادات جزءاً من الإعدادات المرسلة إلى الأجهزة: إذ يُنزّل كل جهاز بيانات اعتماده من Cerberus Enterprise، ويوقّع الطلب بشهادة إدارته. وهي لا تُكتب في السجلات.

قواعد الامتثال

يحدّد قسم **قواعد الامتثال** في محرّر سياسة Apple متطلبات لأجهزة السياسة. الجهاز الذي يخالف قاعدة يصبح غير ممتثل فورًا: تعرض صفحة الجهاز السبب في **لماذا الجهاز غير ممتثل**، وتُظهره قائمة الأجهزة على أنه غير ممتثل. يكون الجهاز أيضًا غير ممتثل عندما يتعذّر تطبيق أحد إعدادات السياسة عليه.

القواعد

- **رمز المرور**: الجهاز لديه رمز مرور، وهو يستوفي إعدادات رمز المرور في السياسة.
- **الحد الأدنى لإصدار نظام التشغيل**: لأجهزة iPhone وiPad، أو لأجهزة Mac. لتحديث الأجهزة، أضف تحديثًا مطلوبًا في «تحديثات البرامج».
- **جهاز خاضع للإشراف**: الأجهزة المسجّلة بملف تعريف التسجيل أو بتسجيل المستخدم ليست خاضعة للإشراف.
- **FileVault مفعّل (Mac)**: قرص جهاز Mac مشفّر باستخدام FileVault. لا تتأثر الأجهزة الأخرى.

تُفحص القاعدة عندما يرسل الجهاز حالته، وعند حفظ السياسة، وكل ساعة. الجهاز الذي تكون حالته غير معروفة (مثلًا جهاز Mac لم يُبلغ عن FileVault بعد) لا يخالف القاعدة.

حظر الجهاز

فعّل **حظر الجهاز إذا ظل غير ممتثل** وحدّد عدد الأيام بعدها (القيمة 0 تحظر فورًا). تنقل أجهزة iPhone وiPad الخاضعة للإشراف إلى وضع الفقدان مع الرسالة التي تحددها. تُقفل الأجهزة الأخرى مرة واحدة؛ ويعيد جهاز Mac التشغيل ويطلب رمز PIN، يظهر في تفاصيل الأمر في سجل الأوامر.

- **إلغاء الحظر**: عندما يصبح الجهاز ممتثلًا مرة أخرى، يُعطّل وضع الفقدان تلقائيًا.
- **إيقاف وضع الفقدان بنفسك**: لا يُحظر الجهاز مرة أخرى حتى يصبح ممتثلًا ويخالف قاعدة مجددًا. استخدم هذا لتمكين المستخدم من إصلاح الجهاز.

> **الجهاز يصبح غير ممتثل**: لتلقّي إشعار، أو للتفاعل بطرق أخرى، أنشئ قاعدة حدث لـ تحصل أيضًا على الأسباب.