الأوامر

توفّر صفحة الجهاز لوحة **الأوامر** لإرسال أوامر عن بُعد إلى جهاز مُدار. تعتمد الأوامر المتاحة على النظام الأساسي (Android أو Apple) وحالة الجهاز.

لا يمكن إرسال الأوامر إلا إلى جهاز مسجّل حاليًا. على جهاز غير مسجّل، وعلى جهاز ADE لم يُسجّل بعد، وعلى السجل التاريخي لتسجيل سابق، تعرض اللوحة سجل الأوامر فقط.

> إذا لم يكن الجهاز متصلًا بالإنترنت حاليًا، فسيُسلّم الأمر ويُنفّذ بمجرد اتصال الجهاز بالإنترنت. وبالنسبة لأوامر Android، يمكنك ضبط معلمة **الصلاحية** لتحديد المدة التي يظل فيها الأمر غير المُسلّم صالحًا.

أوامر Android (AMAPI)

بالنسبة لأجهزة Android، تتضمن لوحة الأوامر حقل **الصلاحية** (القيمة + الوحدة) ومحدد **الأمر**. وتتطلب بعض الأوامر معلمات إضافية تظهر ديناميكيًا عند تحديد الأمر.

المعلمات الشائعة

- **الصلاحية**: المدة التي يظل فيها الأمر صالحًا إذا تعذر تنفيذه فورًا.
- **الأمر**: اختر الإجراء الذي تريد إرساله إلى الجهاز.

أوامر بدون حقول إضافية

- **قفل الجهاز**: يقفل الجهاز.
- **إعادة تشغيل الجهاز**: يعيد تشغيل الجهاز. يتطلب Android 7.0 أو أحدث.
- **تعطيل وضع الفقدان**: يُخرج الجهاز من وضع الفقدان.
- **التخلي عن الملكية**: يزيل ملف العمل وجميع السياسات من جهاز مملوك للشركة يعمل بنظام Android 8.0 أو أحدث، ويترك للاستخدام الشخصي. تُحفظ تطبيقات الملف الشخصي وبياناته. يُخذف الجهاز من الخادم بعد إقراره بتنفيذ الأمر. لا يمكن التراجع عن ذلك.

الأوامر ذات الحقول الإضافية

- **إعادة تعيين كلمة المرور**: يتطلب **كلمة مرور جديدة** و**تأكيد كلمة المرور الجديدة**. وتتضمن مفاتيح التبديل الاختيارية **القفل الآن** و**طلب الإدخال** و**عدم طلب بيانات الاعتماد عند التشغيل**.
- **مسح بيانات التطبيق**: يتطلب **اسم الحزمة** الهدف.
- **تفعيل وضع الفقدان**: يتطلب **رسالة وضع الفقدان** ويدعم حقول اتصال اختيارية (عنوان الشارع، المؤسسة، رقم الهاتف، البريد الإلكتروني). عندما يُبلَّغ الجهاز بذلك، تصبح حالته **مفقود**، وتعرض صفحة الجهاز شريطاً ويُخفى هذا الأمر حتى يُعطّل وضع الفقدان.
- **محو الجهاز**: يدعم **رسالة سبب المحو** (تُعرض للمستخدمين على الأجهزة الشخصية) وعلامات محو اختيارية، بما في ذلك **محو شرائح eSIM**.

> تتوفر أوامر eSIM (**إضافة eSIM**، **إزالة eSIM**، **طلب EID**) في لوحة **إدارة شرائح SIM** المخصصة.

سجل الأوامر

أسفل أدوات التحكم بالإرسال، تعرض لوحة التحكم جدول سجل أوامر. والجدول قابل للفرز ويدعم ترقيم الصفحات. ويمكن توسيع بعض الصفوف لعرض معلمات إضافية أو تفاصيل التنفيذ.

أعمدة سجل Android

- **تاريخ الإنشاء**
- **الأمر**
- **الصلاحية**
- **الحالة**
- **الخطأ**
- **تاريخ التنفيذ**

أوامر Apple (MDM)

بالنسبة لأجهزة Apple، توفر لوحة الأوامر محدد **الأمر**. وتتطلب بعض الأوامر مدخلات إضافية. وكما هو الحال مع Android، يظهر أدناه جدول سجل الأوامر.

الأوامر ذات الحقول الإضافية

- **تثبيت التطبيق**: يتطلب **معرّف الحزمة** للتطبيق.
- **إرسال إشعار**: يتطلب **رسالة الإشعار** (الحد الأقصى للطول 200 حرف).

على أجهزة iPhone وiPad، يصل **إرسال إشعار** والتتبّع المباشر إلى الجهاز عبر تطبيق **Cerberus Enterprise**: يكون مطلوبًا حتى يُثبّت التطبيق ويسجّل للإشعارات (راجع حقل

تطبيق Cerberus Enterprise). عند بدء التتبّع المباشر تظهر رسالة «تم إرسال طلب التتبّع المباشر إلى الجهاز»: يبدأ التتبّع عندما يرسل الجهاز موقعه الأول. قد يؤخّر iOS الطلب أو الوصله، مثلاً في وضع الطاقة المنخفضة أو دون اتصال بالشبكة: إذا لم يصل أي موقع خلال دقيقتين، اطلب من المستخدم فتح التطبيق مرة واحدة. عندما يفشل طلب، توضّح الرسالة السبب، مثلاً أن التطبيق لم يسجّل بعد، أو أن مفتاح إشعار الخادم مفقود، أو أن رمز إشعار الجهاز لم يعد صالحاً.

إجراءات الجهاز

تُدرج فقط الأوامر التي يدعمها الجهاز: بعضها يتطلب جهاز iPhone أو iPad خاضعاً للإشراف، وبعضها غير متاح على Mac. وتطلب الأوامر المسبوقة للتعطيل تأكيداً.

- **قفل الجهاز**: يقفل الشاشة، مع رسالة اختيارية ورقم هاتف. يُعاد تشغيل Mac ويُقفل برمز PIN من ستة أرقام، يُعرض مرة واحدة بعد إرسال الأمر وفي تفاصيل الأمر. يعرض iPhone العنوان «iPhone مفقود» فوق رسالتك، رغم أن هذا الأمر لا يفعّل وضع الفقدان.
- **تفعيل وضع الفقدان** (iPhone وiPad خاضعان للإشراف): يقفل الجهاز ويعرض رسالتك ورقم هاتفك والحاشية على شاشة القفل. وأثناء تفعيل وضع الفقدان، تعرض الصفحة شريطاً والأوامر **تحديد موقع الجهاز** (يظهر الموقع على خريطة الموقع)، و**تشغيل صوت** ، و**تعطيل وضع الفقدان**.
- يُبلَّغ الجهاز من يحمله بأنه تم تحديد موقعه: بعد **تحديد موقع الجهاز**، تعرض شاشة القفل **تم تحديد موقع iPhone** مع الوقت واسم الخادم الذي تلقى الموقع، وزر **متابعة**. يعرض iOS هذا الإشعار ولا يمكن إيقافه.
- **مسح رمز المرور**: يزيل رمز مرور جهاز iPhone أو iPad، على سبيل المثال عندما ينساه المستخدم. وإذا كانت السياسة تتطلب رمز مرور، يُطلب من المستخدم تعيين رمز جديد.
- **تحديث معلومات الجهاز**: يطلب من الجهاز معلوماته (الإشراف، إصدار نظام التشغيل، حالة الأمان، شهادة MDM) وجرده.
- **إعدادات الجهاز**: يفتح نافذة لتغيير اسم الجهاز، واسم المضيف لجهاز Mac، وBluetooth، وتواجد البيانات، ونقطة الاتصال الشخصية، والمنطقة الزمنية، والخلفية، وما إذا كان قفل التنشيط مسموحاً، وعلى iPad مشترك إعداداته (انظر أدناه). تُرسل الإعدادات التي تغيّرها فقط؛ الإعدادات التي لا يدعمها الجهاز تكون معطّلة مع السبب. قد يقرّ الجهاز بتواجد البيانات أو نقطة الاتصال الشخصية دون تطبيقها (مثلاً عندما لا تتضمن خطة SIM نقطة اتصال شخصية)، لذلك يعيد Cerberus Enterprise قراءتها بعد نحو 30 ثانية ويكتب تحذيراً في سجلات النظام إذا لم يتغير.
- **إعادة تشغيل الجهاز وإيقاف تشغيل الجهاز**: إعادة تشغيل الجهاز أو إيقاف تشغيله فوراً، بعد تأكيد.
- **محو الجهاز**: يمحو جميع المحتويات والإعدادات ويزيل الجهاز من الإدارة. على iPhone وiPad يمكن الاحتفاظ بخطة بيانات eSIM وتخطي إعداد القرب؛ ويحصل Mac على رمز PIN من ستة أرقام.
- **الإرجاع إلى الخدمة** (خيار **محو الجهاز**، iPhone وiPad مع iOS 17 أو أحدث): بعد المحو، يعدّ الجهاز نفسه مجدداً، دون أن يلمسه أحد، ويسجّل مرة أخرى بسيسته ومستخدمه وملكيته الحالية. اختر شبكة Wi-Fi من سياسة الجهاز للإعداد، إلا إذا كان الجهاز يستخدم Ethernet أو بيانات خلوية: فلا يمكن استخدام سوى الشبكات الشخصية (بكلمة مرور، دون شهادات)، لأن الجهاز ليس لديه مستخدم أو شهادة بعد. ويجب أن يكون قفل التنشيط

متوقفاً.

- **تحديث خطط البيانات الخلوية** (iPhone وiPad الخلوي، iOS 13 أو أحدث، وليس تسجيل المستخدم): أدخل **عنوان URL لخادم eSIM الخاص بمشغّل الاتصالات** الذي يقدمه المشغّل (عنوان https://، أو اسم مضيف، أو رمز تفعيل LPA، والذي يُستخدم منه سوى الخادم) وسيُنزّل الجهاز خطط eSIM التي ربطها المشغّل بمعرّف EID الخاص به. ويظهر معرّف EID للجهاز أسفل الحقل لإرساله إلى المشغّل. راجع صفحة **إدارة شرائح SIM**.
- **الاحتفاظ بخطة بيانات eSIM** عند إيقاف تشغيلها يزيل جميع شرائح eSIM عند المحو. وينطبق قيد السياسة **الاحتفاظ بـ eSIM عند محو الجهاز** (الأجهزة الخاضعة للإشراف، iOS 17.2 أو أحدث) على عمليات المحو التي تبدأ على الجهاز (محاولات كثيرة فاشلة لرمز المرور، محو كل المحتوى والإعدادات): والوثوق Apple تأثيره على هذا الأمر.
- **تسجيل خروج المستخدم** (iPad مشترك): يسجّل خروج المستخدم الحالي ويعود إلى شاشة تسجيل الدخول. وتبقى البيانات التي لم تتم مزامنتها مع iCloud بعد على iPad.

iPad مشترك

يُستخدم iPad مشترك من قبل عدة أشخاص، لكل منهم حساب Managed Apple Account خاص به، أو من قبل ضيوف بجلسات مؤقتة. ويُعدّ باستخدام ملف تعريف ADE يفعّل iPad مشترك (راجع صفحة **Apple Automated Device Enrollment**)، ويعرض حقل **نوع التسجيل** قيمة **iPad مشترك**.

- **مستخدمو iPad المشترك**: مستخدمو iPad، مع المستخدم المسجّل الدخول، والتخزين الذي يستخدمونه، وما إذا كانت بعض البيانات لم تتم مزامنتها مع iCloud بعد. استخدم **تحديث** لطلب القائمة من iPad مرة أخرى. ويمكن حذف مستخدم مع بياناته، باستثناء المستخدم المسجّل الدخول (سجّل خروجه أولاً)؛ ويتطلب **حذف كل المستخدمين** نظام iPadOS 14 أو أحدث. وعندما لا تكون البيانات متزامنة بعد، يحذّر التأكيد من أنها ستُفقد.
- **إعدادات الجهاز**: التخزين لكل مستخدم، والعدد المتوقع للمستخدمين، ومدة عدم النشاط التي بعدها يتم تسجيل خروج المستخدمين وجلسات الضيوف، وجلسات الضيوف فقط، ونطاقات Managed Apple Account المقترحة على شاشة تسجيل الدخول، وعدد الأيام التي يمكن للمستخدم فيها تسجيل الدخول دون التحقق من كلمة المرور عبر الإنترنت، وتخطي إعداد اللغة والمنطقة للمستخدمين الجدد. وتحتفظ الحقول الفارغة بقيمتها الحالية؛ والإعدادات التي تحتاج إلى إصدار أحدث من iPadOS تكون معطّلة.

مستخدمو Mac

على Mac، تسرد لوحة **مستخدمو Mac** المستخدمين المسجّلين في الإدارة، وعادةً المستخدم الذي سجّل الـ Mac. وتُثبّت حسابات السياسة في جلساتهم. ولكل مستخدم، تعرض متى تم تسجيله، وآخر تقرير عن جلسته، وحالة الحساب: **محدّث**، أو **في انتظار المستخدم** (يثبّتها الـ Mac عند تسجيل دخول المستخدم)، أو **لم يُطبّق** مع الأسباب التي يبلغ عنها الـ Mac، أو **الا توجد حسابات** عندما لا تكون للسياسة أي حسابات. استخدم **إعادة التحميل** لقراءة القائمة مرة أخرى.

قفل التنشيط

يوضح حقل **قفل التنشيط** ما إذا كان قفل التنشيط مفعّلاً. وعند تفعيله، يمكن إعداد جهاز مُدار باستخدام حساب Apple الخاص بالمستخدم أو رمز التجاوز الخاص بالجهاز. ولتعطيل القفل في **إعدادات الجهاز**، يجب توفير رمز التجاوز الخاص بالجهاز من أجهزة الخادم للإشراف على التنشيط إلى الجهاز، مع ترك حساب Apple فارغاً. وتخزّن Cerberus Enterprise رمز التجاوز الخاص بها وتستخدم **إظهار رمز التجاوز** في قائمة الحقل عرضه (يمكن للمسؤولين فقط، ويُسجّل كل عرض في سجل النظام)، ثم أدخله كلمة مرور على شاشة قفل التنشيط في الجهاز، معترك حساب Apple فارغاً.

قفل الاستيراد وكلمة مرور البرنامج الثابت (Mac)

يعرض Mac المزوّد بشريحة Apple Silicon حقل **قفل الاستيراد**، ويعرض Mac المزوّد بمعالج Intel حقل **كلمة مرور البرنامج الثابت**. ويحمي كلاهما الـ Mac عند بدء التشغيل: مع قفل الاستيراد، يطلب recoveryOS كلمة المرور؛ ومع كلمة مرور البرنامج الثابت، يطلبها الـ Mac للبدء من قرص آخر أو من وضع الاستيراد. ويعرض الحقل ما إذا كان الـ Mac يبلغ عن كلمة مرور، وفي تلميحه، متى خزّنتها Cerberus Enterprise ومتى تم التحقق منها آخر مرة.

- **تعيين كلمة المرور أو تغييرها**: تنشئ Cerberus Enterprise كلمة مرور من 20 حرفاً (من 8 تقع على المفاتيح نفسها في أي تخطيط لوحة مفاتيح، أو يكتب المسؤول واحدة) لتسلّمها إلى المستخدم. ويمكن للأدوار الأخرى إنشاء واحدة فقط، لأنها تستطيع رؤية كلمات المرور المخزّنة). وتُخزّن كلمة المرور مشفّرة قبل إرسالها، والـ تحل محل المخزّنة إذا عندما يؤكدها الـ Mac. وإذا كان الـ Mac لديه كلمة مرور معيّنة خارج Cerberus Enterprise بالفعل، فاكتبها كلمة المرور الحالية: وتُستخدم مرة واحدة والـ تُخزّن.
- **التحقق من كلمة المرور**: يسأل الـ Mac عما إذا كانت كلمة المرور المخزّنة صحيحة. وتظهر النتيجة في التلميح وفي سجل النظام.
- **إظهار كلمة المرور**: يمكن للمسؤولين فقط رؤية كلمة المرور المخزّنة، ويُسجّل كل عرض في سجل النظام. وتُعرض كلمات المرور المُنشأة في مجموعات من أربعة أحرف: اكتبها دون مسافات.
- **مسح كلمة المرور**: يزيل كلمة المرور من الـ Mac.

يُعاد تشغيل Mac المزوّد بمعالج Intel لتطبيق تغيير كلمة مرور البرنامج الثابت: وإلى ذلك الحين، تظل كلمة المرور السابقة مطلوبة (يسردها إظهار كلمة المرور)، ولا يمكن إرسال تغيير آخر. وتقبل Apple أيضاً أمراً واحداً فقط لكلمة مرور البرنامج الثابت كل 30 ثانية. وتكون كلمات المرور مخفية في سجل الأوامر.

عندما يخرج Mac من الإدارة (إلغاء التسجيل، أو الإزالة بواسطة المستخدم، أو المحو)، يزيل macOS قفل الاستيراد من تلقاء نفسه وتُسقط Cerberus Enterprise كلمة مرور قفل الاستيراد المخزّنة؛ وتفعل الشيء نفسه عندما يبلغ الـ Mac أنه لا يوجد لديه قفل استيراد، على سبيل المثال بعد إعادة تسجيله. وعند إلغاء تسجيل Mac (أو حذف سياسته)، تُمسح كلمة مرور البرنامج الثابت المخزّنة أولاً، ويُعاد تشغيل الـ Mac ثم يخرج من الإدارة. وإذا فشل المسح، يخرج الـ Mac من

الإدارة على أي حال وتبقى كلمة المرور مخزّنة حتى تتمكن من رؤيتها. ويحتفظ Mac الذي أزالهُ المستخدم من الإدارة، أو الذي مُحي، بكلمة مرور البرنامج الثابت: وتحتفظ بها Cerberus Enterprise أيضاً. ويؤدي حذف سجل الجهاز إلى حذف كلمة المرور المخزّنة، لذا يُطلب منك تأكيد ذلك أولاً: دوّن كلمة المرور، لأنه بدونها لا يمكن إزالتها إلا بواسطة Apple.

FileVault (Mac)

يعرض حقل **FileVault** ما إذا كان قرص Mac مشفّراً، ويعرض في تلميحه ما إذا كان Cerberus Enterprise يخزّن مفتاح الاسترداد الشخصي الخاص به. يرسل Mac المفاتح عندما يكون FileVault مشغّلاً بعد أن يتلقى إعداد FileVault من سياسته (راجع صفحة **macOS** في سياسات Apple).

- **إظهار مفتاح الاسترداد**: يمكن للمسؤولين فقط رؤية المفاتح، ويُسجّل كل عرض في سجل النظام. استخدمه في نافذة تسجيل الدخول في الـ Mac لإعادة تعيين كلمة مرور المستخدم، أو في وضع الاسترداد لفتح القرص. ويظل متاحاً بعد خروج الـ Mac من الإدارة؛ ويؤدي حذف سجل الجهاز إلى حذفه.
- **تغيير مفتاح الاسترداد**: يستبدل الـ Mac مفتاح الاسترداد الشخصي الخاص به ويرسل المفاتح الجديد مشفّراً؛ ويتوقف المفتاح القديم عن العمل. ولا يكون ذلك ممكناً إلا عندما يمكن قراءة المفاتح المخزّن: يكون الـ Mac مفتوحاً به، ولا حاجة إلى كلمة مرور مستخدم. ويُخفى المفتاح المخزّن في سجل الأوامر ويُزال من الخادم بمجرد أن يجيب الـ Mac (أو بعد 7 أيام دون إجابة).

Bootstrap Token (Mac)

يرسل Mac المزوّد بـ macOS 10.15 أو أحدث رمز **Bootstrap Token** إلى خادم الإدارة عندما يسجّل مستخدم لديه رمز مميز آمن الدخول. ويحتفظ الخادم به ويعيده إلى ذلك الـ Mac فقط، الذي يستخدمه لمنح المستخدمين الجدد رمزاً مميزاً آمناً، وعلى Mac المزوّد بشريحة Apple Silicon، لتثبيت تحديثات البرامج والموافقة على إضافات kernel دون طلب كلمة مرور مسؤول. ولا يمكن لأحد رؤية الرمز المميز، في لوحة التحكم أو في أي مكان آخر. ويعرض حقل **Bootstrap Token** حالته:

- **محتجَز بأمان**: يحتفظ الخادم بالرمز المميز؛ ويظهر التلميح متى أرسله الـ Mac.
- **تم حفظه مسبقاً**: أُرسل الرمز المميز المخزّن قبل آخر عملية تسجيل أو تجديد لشهادة MDM لهذا الـ Mac. بعد التجديد يكون ذلك متوقعاً: يبقى الرمز ولا يرسله الـ Mac مرة أخرى. بعد عملية تسجيل جديدة قد لا يظل صالحاً: نفّذ `sudo profiles install -type bootstraptoken` في Terminal على الـ Mac.
- **غير محتجَز بأمان**: لم يرسل الـ Mac رمزاً مميزاً بعد. لإرساله الآن، يشغّل مسؤول الـ Mac الأمر `sudo profiles install -type bootstraptoken` في Terminal (ويوضح `sudo profiles status -type bootstraptoken` ما إذا كان محتجَزاً بأمان).

يوضح التلميح أيضاً ما إذا كان الـ Mac يسمح بالرمز المميز للمصادقة. وتسمح به أجهزة Mac المعدّة باستخدام Automated Device Enrollment تلقائياً؛ وعلى أجهزة Mac الأخرى المزوّدة بشريحة Apple Silicon، يمكن للمستخدم السماح به في Startup Security Utility في recoveryOS. ولا يمكن لأجهزة Mac المزوّدة بمعالج Intel استخدام الرمز المميز للمصادقة (**غير مدعوم**)، لكن الرمز المميز المحتجَز بأمان يمنح المستخدمين الجدد رمزاً مميزاً آمناً. وفي كل مرة يرسل فيها الـ Mac رمزه

المميز أو يزيله أو يطلبه، يُسجّل ذلك في سجل النظام.

حالة الجهاز وتحديثات نظام التشغيل

تعرض لوحة **حالة الجهاز** ما يبلغ به الجهاز عن نفسه: إصدار نظام التشغيل وبنائه، وتقدّم تحديث برنامج (الإصدار المعلّق، الموعد النهائي، ما بدأه، حالات الفشل)، وما إذا كان رمز المرور معيّنًا ويتوافق مع السياسة، وFileVault على Mac، وصحة البطارية، والحسابات المكوّنة على الجهاز.

تعرض قائمة **التحديثات المتاحة** تحديثات نظام التشغيل التي يمكن للجهاز تثبيتها، وهي تُجمع عند التسجيل وأسبوعيًا. استخدم **التحقق من التحديثات** لطلبه الآن، و**تثبيت** لتثبيت تحديث فوري (يُعاد تشغيل الجهاز بعد تأكيد) أو لتنزيله فقط وترك المستخدم يثبّته. يعمل هذا على أجهزة iPhone وiPad الخاضعة للإشراف وعلى أجهزة Mac، حتى iOS وiPadOS وmacOS 26: في الإصدارات اللاحقة، ولتحديث أجهزة كثيرة، استخدم التحديثات المطلوبة في السياسة (راجع صفحة [تحديثات البرامج](#) في سياسات Apple).

الـ Mac المزوّد بشريحة Apple Silicon يثبّت تحديثًا دون طلب كلمة مرور مسؤول إذا عندما يسمح باستخدام Bootstrap Token الخاص به للمصادقة ويكون الرمز المميز محتجَزًا بأمان (راجع Bootstrap Token أعلاه). وبخلاف ذلك، يفيد التأكيد بأنه قد يتعين على المستخدم إدخال كلمة مرور مسؤول قبل تثبيت التحديث.

التطبيقات والجرد

تسرد لوحة **التطبيقات** كل تطبيق على الجهاز في جدول واحد. وتبلغ حالة تثبيت التطبيقات المثبّتة بواسطة السياسة أو بأمر مباشرةً من الجهاز؛ بينما تأتي الإصدارات والأحجام والتطبيقات المثبّتة بواسطة المستخدم من قائمة التطبيقات الأخيرة، التي تُجمع عند التسجيل وأسبوعيًا. استخدم **اسأل الجهاز** لطلبها الآن.

- **الإدارة**: **السياسة** للتطبيقات المثبّتة بواسطة سياسة الجهاز، **مُدار** للتطبيقات المثبّتة بأمر مثل **تثبيت التطبيق**، **غير مُدار** للتطبيقات التي يثبّتها المستخدم. يحمل تطبيق Cerberus Enterprise شريحة **مثبّت بواسطة Cerberus**.
- **يحتاج إلى انتباه**: التطبيقات التي فشل تثبيتها، أو رفضها المستخدم أو أزالها، أو التي تنتظر المستخدم. افتح صفًا لعرض الخطأ؛ ويمكن إعادة تثبيت تطبيقات السياسة الفاشلة باستخدام زر إعادة المحاولة. ولا تُحتسب التطبيقات المدمجة وتطبيقات App Store التي يبلغ الجهاز بأنها غير متحققٍ منها.
- **إزالة التطبيق**: يمكن إزالة التطبيقات المُدارة، مع بياناتها. لإزالة تطبيق مثبّت بواسطة السياسة، أزله من السياسة. وترسل السياسة هذا الأمر أيضًا من تلقاء نفسها عندما تُزال حزمة Mac مثبّتة كتطبيق مُدار من السياسة.

تعرض لوحة **ملفات التعريف والشهادات والأمان** ملفات تعريف التكوين والشهادات وحالة الأمان (رمز المرور، التشفير، FileVault والجدار الناري على Mac) التي يبلغ عنها الجهاز.

>

> على الأجهزة المملوكة شخصيًا، لا تُجمع التطبيقات المثبّتة بواسطة المستخدم، وتُدرج فقط ملفات التعريف والشهادات التي تديرها Cerberus Enterprise.

تعرض لوحة **تغييرات الجرد** ما تغيّر بين قائمتين يرسلهما الجهاز: تطبيقات مثبّتة أو مُزالة أو محدّثة (مع الإصدارين القديم والجديد)، وملفات تعريف مثبّتة أو مُزالة أو محدّثة، وشهادات مضافة أو مُزالة. ويُكتشف التغيير عندما يرسل الجهاز قائمة جديدة، أسبوعيًا للتطبيقات وملفات التعريف، ويوميًا للشهادات، أو عندما تستخدم **أسأل الجهاز**: والتاريخ المعروض هو وقت اكتشافه، وقد حدث التغيير بين القائمة السابقة وتلك القائمة. وتُسجّل القائمة الأولى للجهاز، والأولى بعد تسجيل جديد أو تغيير ملكية، فقط كنقطة بداية. ابحث حسب الاسم أو المعرّف، وصفِّ حسب النوع والتغيير. ويُحتفظ بالتغييرات لمدة 365 يومًا.

> عندما يستبدل تحديث نظام التشغيل العديد من تطبيقات Apple دفعة واحدة، تُعرض في سطر واحد (على سبيل المثال "تم تحديث 23 تطبيقًا من Apple") يمكنك توسيعه. ويُعرض تجديد شهادة MDM كـ **تم تجديد شهادة MDM**. وعلى الأجهزة المملوكة شخصيًا، تُعرض فقط تغييرات العناصر التي تديرها Cerberus Enterprise.

أعمدة سجل Apple

- **تاريخ الإنشاء**
- **الأمر**
- **الحالة**: **تم الإرسال** (في انتظار الجهاز، ويُسلّم بمجرد اتصاله)، **نجاح**، **تم الرد** (افتح الصف لرؤية النتيجة)، **في انتظار الجهاز** (الجهاز يمكنه تنفيذ الأمر الآن)، **فشل** (افتح الصف لرؤية السبب) أو **ملغى** (تم مسح قائمة انتظار أوامر الجهاز، مثلًا عند إعادة تسجيله).
- **تاريخ التنفيذ**

تحديث

استخدم إجراء التحديث في لوحة الأوامر لإعادة تحميل سجل الأوامر.

Revision #58
Created 2025-12-17 09:32:44 UTC by Admin
Updated 2026-11-12 09:53:30 UTC by Admin