حالة الجهاز

- نظرة عامة على الجهاز
- خريطة الموقع
- إدارة شرائح SIM
- الأوامر

نظرة عامة على الجهاز

افتح جهازاً من **لوحة التحكم** ← **الأجهزة** بالنقر على صف الجهاز. يعرض عنوان الصفحة **طراز** الجهاز (عند توفره) و**معرّف** الجهاز الداخلي.

البيانات التاريخية مقابل التسجيل الحالي

عندما يكون للجهاز عمليات تسجيل متعددة، يمكن لـ Cerberus Enterprise عرض سجل تاريخي للقراءة فقط. في هذه الحالة، تعرض الصفحة شريط **بيانات تاريخية** وزراً للعودة إلى بيانات التسجيل الحالي.

الحقول العلوية

يلخّص القسم العلوي هوية الجهاز وإسناده وحالة إدارته. بعض الحقول خاصة بالنظام الأساسي وتظهر فقط لأجهزة Android أو Apple.

- **المعرّف** و**الطراز**: معرّفات للقراءة فقط.
- **المستخدم**: يعرض المستخدم المعيّن حالياً (إن وُجد). ومن قائمة المستخدم يمكنك **فتح المستخدم** أو **تغيير المستخدم**، أو تعيين مستخدم عندما لا يكون هناك مستخدم.
- **وضع الإدارة** و**الملكية**: يُعرضان مع تلميحات في واجهة المستخدم.
- **الحالة**: حالة الجهاز الحالية (مع تفاصيل الأيقونة والتلميح). يعرض الجهاز في وضع الفقدان **مفقود** على Android وApple معاً، ويوضّح شريط في أعلى الصفحة ما يجب فعله بعد ذلك.
- **ملف تعريف ADE** (Apple فقط): يعرض ملف تعريف التسجيل التلقائي للأجهزة المعيّن (إن وُجد) ويتيح لك فتحه أو تغييره.
- **السياسة**: تعرض السياسة المعيّنة وتتيح لك فتحها أو تغييرها، أو تعيين سياسة عندما لا تكون هناك سياسة.
- **حالة الامتثال للسياسة** (عند تعيين سياسة): تشير إلى ما إذا كان الجهاز ممتثلاً.
- **إصدار السياسة** (عند تعيين سياسة): يشير إلى ما إذا كان الجهاز قد طبّق أحدث إصدار من السياسة.
- **تطبيق Cerberus Enterprise** (iPhone وiPad فقط): حالة تطبيق Cerberus Enterprise الذي يثبّته Cerberus على الجهاز. **غير متاح** (iOS أو iPadOS أقدم من 18.4، أو لا يوجد رقم تسلسلي على جهاز تابع للشركة، أو لا يوجد Managed Apple Account على جهاز شخصي)؛ **غير متاح على الأجهزة الشخصية بعد**؛ **في انتظار معلومات الجهاز**؛ **في انتظار**

ترخيص المستخدم لحساب Managed Apple Account (الأجهزة الشخصية، بينما تؤكد Apple الترخيص)؛ **غير مثبّت** (التطبيق ليس في مكتبة Apple Business لديك أو لم يتم إعداد Apps and Books، عُد إلى **إعدادات الحساب**)؛ **مثبّت · يحتاج Apps and Books إلى انتباه** (انتهت صلاحية الرمز المميز أو غادر التطبيق مكتبتك: يبقى التطبيق مثبّتاً)؛ **الإعداد غير متاح**؛ **جارٍ التثبيت…** (إذا لم يرسل الجهاز تقرير حالة لمدة 30 دقيقة، يقترح التلميح التحقق من اتصاله بالإنترنت وإعادة تشغيله، مما يبدأ التثبيت عادةً من جديد)؛ **في انتظار موافقة المستخدم**؛ **رفض المستخدم** و**فشل التثبيت** (كلاهما مع **إعادة المحاولة**، الذي يسأل الجهاز مرة أخرى)؛ **مثبّت · في انتظار بدء التطبيق** (لم يُفتح التطبيق بعد)؛ **مثبّت · لم يُقبل الإعداد**؛ وبعد تسجيل التطبيق، إصداره وآخر تواصل له وما إذا كانت الإشعارات مفعّلة.

- **تاريخ التسجيل** و**آخر تقرير حالة**: الطوابع الزمنية للتسجيل وآخر حالة تم الإبلاغ عنها.
- **تاريخ إلغاء التسجيل**: يُعرض عندما يتم إلغاء تسجيل الجهاز.

> لا تتوفر بعض البيانات واللوحات إلا عندما تكون الفئة المقابلة مُمكّنة في سياسة الجهاز. لمزيد من المعلومات، اقرأ صفحتي **الإبلاغ عن الحالة** و**الموقع والأسيجة الجغرافية**.

اللوحات

تُنظّم صفحة الجهاز في أقسام قابلة للتوسيع. وفقًا للنظام الأساسي والحالة، قد ترى واحدًا أو أكثر من اللوحات التالية:

- **خريطة الموقع**: لوحة ذات علامات تبويب تتضمن سجل **الموقع** للجهاز الحالي، وعلى أجهزة Android وأجهزة iPhone وiPad، علامة تبويب **السياج الجغرافي** لعمليات الانتقال عبر السياج الجغرافي.
- **إدارة شرائح SIM**: EID الجهاز وشرائح SIM وeSIM المثبتة. على Android أيضًا أوامر eSIM وسجلها؛ وعلى أجهزة iPhone المملوكة للشركة أو أجهزة iPad الخلوية أيضًا التجوال على البيانات ونقطة الاتصال الشخصية و**تحديث الخطط الخلوية**. راجع صفحة **إدارة شرائح SIM** المخصصة.
- **الأوامر**: أرسل أوامر إلى الجهاز واعرض سجل الأوامر (حسب النظام الأساسي).
- **الوضع الأمني**: الحالة الأمنية للجهاز ومخاطره. على Android أيضًا نتيجة Play Integrity. حتى يُبلّغ الجهاز بذلك، تظهر **غير محدد**، أو **لم يُبلّغ بعد** على جهاز Android لم يرسل أي بيانات أمنية.
- **سبب عدم امتثال الجهاز**: يُعرض فقط عندما يكون الجهاز غير ممتثل، مع أيقونة تنبيه حمراء؛ افتح لرؤية الأسباب. على Android يسرد إعدادات السياسة غير الممتثلة؛ وعلى Apple يوضّح أيضًا ما إذا كانت قاعدة امتثال قد حجبت الجهاز.
- **حالة الجهاز** (Apple فقط): إصدار نظام التشغيل، وتقدّم تحديث البرنامج، ورمز المرور، وFileVault، والبطارية والحسابات التي أبلغ عنها الجهاز، وتحديثات نظام التشغيل المتاحة له. راجع صفحة **الأوامر**.

- **التطبيقات** (Android): التطبيقات المثبّتة وتقارير المخالفات والأخطاء الخاصة بها.
- **التطبيقات** (Apple فقط): التطبيقات المثبتة بواسطة السياسة، والتطبيقات المثبتة بالأوامر، والتطبيقات المثبتة بواسطة المستخدم، مع حالة تثبيتها والأخطاء والإجراءات (إعادة المحاولة، الإزالة). على أجهزة Mac، تسرد أيضًا الحزم المثبتة بواسطة السياسة، مع حالتها و**إعادة التثبيت**؛ والحزم المثبتة كتطبيقات مُدارة شارة **مُدارة**، ويوضح ملاحظة متى تُثبّتت حزمة دون إدارة ولماذا، أو متى لم يُعثر على تطبيقها بعد ساعة من التنزيل. على أجهزة iPhone وiPad، يحمل تطبيق Cerberus Enterprise شارة **مثبّت بواسطة Cerberus**؛ وهو غير مدرج ضمن عامل التصفية **السياسة**. ويحمل التطبيق الذي لم يقبل الجهاز تكوينه المُدار شارة **لم يتم قبول التكوين**. على أجهزة iPhone وiPad الشخصية (تسجيل مستخدم)، يعرض سطر حساب Managed Apple Account الذي يستخدم ترخيص المستخدم الخاص به تطبيقات App Store، وتعرض التطبيقات التي تنتظر ترخيصها **بانتظار ترخيص مستخدم** أو **فشل ترخيص المستخدم**، ويعرض التطبيق الذي ألغى المستخدم مطالبة تثبيته **بانتظار موافقة المستخدم على التثبيت**، ويطلب **طلب مرة أخرى** من Apple الترخيص مرة أخرى أو يعرض المطالبة مرة أخرى. راجع صفحة **الأوامر**.
- **الملفات الشخصية والشهادات والأمان** (Apple فقط): ملفات التكوين والشهادات وحالة الأمان التي أبلغ عنها الجهاز.
- **تغييرات المخزون** (Apple فقط): مخطط زمني للتطبيقات والملفات الشخصية والشهادات المثبتة أو المزالة أو المحدّثة على الجهاز، قابل للبحث ومفلتر حسب النوع والتغيير. راجع صفحة **الأوامر**.
- **مستخدمو iPad المشترك** و**مستخدمو Mac** (Apple فقط): مستخدمو iPad المشترك ومستخدمو Mac. راجع صفحة **الأوامر**.
- **تقارير الحالة**: بيانات إضافية يبلغ عنها الجهاز، تُعرض كشجرة من الفئات والقيم.
- **سجل التسجيل**: عمليات التسجيل السابقة لنفس الجهاز الفعلي، تُعرض كقائمة.

علامات تبويب لوحة الموقع

تستخدم لوحة **خريطة الموقع** علامات تبويب لفصل سجل الموقع وانتقالات النطاقات الجغرافية.

- **الموقع**: يعرض عوامل تصفية السجل، وبحثًا بنطاق تاريخ، وعلامات الموقع، ودائرة الدقة، وعناصر التحكم في التتبع المباشر للجهاز الحالي.
- **السياج الجغرافي** (Android وiPhone وiPad): يعرض سجل الانتقال عبر السياج الجغرافي على خريطة مخصصة، مع عوامل تصفية للفترة، ومفتاح اختياري للأسوار الجغرافية المؤرشفة، وقائمة جانبية للانتقالات. وعلى أجهزة iPhone وiPad، يخبرك سطر حالة أيضًا عندما يتعذّر عمل السياج الجغرافي على الجهاز.

للاطلاع على السلوك الكامل لعلامات التبويب هذه، راجع **خريطة الموقع**.

الإجراءات

في أسفل الصفحة، يمكنك تحديث البيانات وتنفيذ إجراءات حسب النظام الأساسي وحالة الجهاز وحالة الترخيص.

- **تحديث البيانات**: إعادة تحميل سجل الجهاز.
- **تعطيل الجهاز / تمكين الجهاز** (Android فقط): متاح في الحالات المدعومة.
- **إلغاء تسجيل الجهاز**: يزيل الإدارة من الجهاز. يعتمد السلوك الدقيق على النظام الأساسي والملكية (على سبيل المثال، قد يمسح Android ملف تعريف العمل أو يعيد ضبط الجهاز إلى إعدادات المصنع).
- **حذف الجهاز**: متاح عندما يكون الجهاز ملغى التسجيل بالفعل ويمكن إزالة سجله.

خريطة الموقع

توثّق هذه الصفحة أدوات الموقع الخاصة بالجهاز والمتاحة في **نظرة عامة على الجهاز**. وتحتوي اللوحة على علامة تبويب **الموقع** لسجل المواقع، وعلى أجهزة Android وأجهزة iPhone وiPad، علامة تبويب **السياج الجغرافي** لانتقالات الأسيجة الجغرافية.

المتطلبات الأساسية

على Android، لا تُعرض بيانات موقع الجهاز إلا عندما يكون الإبلاغ عن الموقع ممكّناً في سياسة الجهاز. لتمكينه، افتح السياسة وشغّل **الموقع والأسيجة الجغرافية ← الإبلاغ عن الموقع**. لمزيد من التفاصيل، راجع **الموقع والأسيجة الجغرافية**.

على أجهزة iPhone وiPad، يأتي الموقع من تطبيق Cerberus Enterprise، بعد أن يسمح به المستخدم، أو من أمر **تحديد موقع الجهاز** أثناء وجود الجهاز في وضع الفقدان. لا تُبلِّغ أجهزة Mac وأجهزة Apple الأخرى عن مواقعها.

> على الأجهزة غير المُدارة بالكامل، قد تظل بيانات الموقع تعتمد على امتلاك تطبيق Cerberus Enterprise لأذونات الموقع المطلوبة وعلى تفعيل خدمات الموقع على الجهاز.

> على الأجهزة الشخصية (تسجيل المستخدم)، يتوفر الموقع والأسيجة الجغرافية فقط عندما يكون خيار **الموقع والأسيجة الجغرافية على الأجهزة الشخصية** مفعّلاً في سياسة Apple، وفقط إذا سمح المستخدم بالموقع لتطبيق Cerberus Enterprise. وبخلاف ذلك، لا تعرض صفحة جهازه إجراءات الموقع أو التتبع المباشر. ولا يتوفر وضع الفقدان أبداً على الأجهزة الشخصية.

> للخريطة العامة متعددة الأجهزة المتاحة من لوحة التحكم، راجع **خريطة الموقع في لوحة التحكم**.

حالة التحميل وعدم وجود بيانات

- أثناء تحميل بيانات الموقع، تعرض اللوحة طبقة تحميل على الخريطة.
- إذا لم تتوفر بيانات موقع للجهاز، تعرض اللوحة رسالة تنص على **لا تتوفر بيانات موقع**. على Android تضيف تذكيراً بتفعيل الإبلاغ عن الموقع في السياسة المعيّنة،

عندما يكون معطّلاً. على Apple توضّح مصدر الموقع، أو أن هذا النوع من الأجهزة لا يُبلِّغ عنه.
- إذا كان عامل تصفية التاريخ نشطاً ولم تتطابق معه أي عينات، تعرض اللوحة **لا تتوفر بيانات في نطاق التاريخ المحدد**.

علامة تبويب الموقع

افتح علامة تبويب **الموقع** لفحص السجل الخاص بجهاز واحد. وتشمل عوامل التصفية المتاحة آخر موقع معروف، ونطاقات السجل الأخيرة، ونطاق تاريخ مخصص، والتتبع المباشر.

- **الأخير**: يعرض آخر موقع معروف.
- **اليوم**، و**آخر 7 أيام**، و**آخر 30 يوماً**: عرض المواقع المسجّلة للفترة المحددة.
- **بحث**: يتيح لك اختيار نطاق تاريخ مخصص.
- **مباشر**: يبدأ أو يوقف التتبع المباشر للجهاز الحالي.

> تُحفظ المواقع لمدة **90 يوماً**: وتُحذف المواقع الأقدم تلقائياً كل ليلة. ويُحفظ دائماً آخر موقع لكل جهاز مسجّل، لذا يظل الجهاز على الخرائط حتى عندما لا يُبلغ عن موقعه منذ مدة طويلة. أما الأجهزة المُزالة والتسجيلات السابقة، فتُحذف جميع مواقعها الأقدم من 90 يوماً. ولهذا السبب لا يمكن أن يبدأ نطاق تاريخ **البحث** قبل أكثر من 90 يوماً.

تفاصيل العلامة

عند النقر على علامة موقع، تُفتح نافذة معلومات تتضمن:

- الطابع الزمني لسجل الموقع.
- الدقة **المُبلغ عنها** (بالأمتار).
- السرعة **المُبلغ عنها**، عندما يوفّرها الجهاز.
- الاتجاه **المُبلغ عنه** أو الميل، عندما يوفّره الجهاز.

دائرة الدقة

عندما تكون نافذة المعلومات مفتوحة، تُعرض دائرة الدقة حول العلامة. يتطابق نصف قطر الدائرة مع الدقة المُبلغ عنها (بالأمتار). يؤدي إغلاق نافذة المعلومات إلى إخفاء الدائرة.

التتبع المباشر

في عرض سجل الجهاز، يؤدي تحديد عامل التصفية **مباشر** إلى بدء طلب تتبع في الوقت الفعلي لهذا الجهاز تحديداً. يطلب Cerberus Enterprise تأكيداً قبل بدء الطلب.

- يستمر التتبع المباشر لمدة تصل إلى **15 دقيقة**.
- أثناء تفعيل التتبع المباشر، تعرض أجهزة Android إشعاراً، وتعرض أجهزة iPhone وiPad مؤشر الموقع.
- أثناء تفعيل التتبع المباشر، تستمر اللوحة في تحديث أحدث موقع ويبقى مؤشر التتبع المباشر ظاهراً.
- يتيح لك تحديد عامل التصفية المباشر مرة أخرى إيقاف التتبع المباشر قبل انتهاء المهلة.
- على **iPhone وiPad**، يعمل التتبع المباشر عبر تطبيق Cerberus Enterprise، مع ضبط الوصول إلى الموقع على **Always**. عادةً ما يوقظ الطلب التطبيق حتى عندما لا يكون مفتوحاً، ثم يرسل التطبيق المواقع طوال الجلسة. لا يضمن iOS هذه الطلبات: فقد يؤخّرها أو يوصلها، على سبيل المثال في وضع الطاقة المنخفضة أو دون اتصال بالشبكة. إذا لم يصل أي موقع خلال دقيقتين، تلغي لوحة التحكم الطلب: اطلب من المستخدم فتح التطبيق مرة واحدة، ثم أعد المحاولة.

علامة تبويب السياج الجغرافي

على أجهزة Android وأجهزة iPhone وiPad، تعرض علامة التبويب الثانية عمليات الانتقال عبر السياج الجغرافي الناتجة عن الأسوار الجغرافية المحددة في السياسة المعيّنة.

- تعرض الخريطة مناطق السياج الجغرافي الحالية إلى جانب نقاط الانتقال المسجّلة.
- تتيح لك قائمة الانتقالات على اليمين فحص أحداث **الدخول** و**الخروج**.
- عوامل التصفية المتاحة هي **اليوم**، و**آخر 7 أيام**، و**آخر 30 يوماً**، وبحث مخصص بنطاق تاريخ.
- **تضمين المؤرشف** يعرض أيضاً عمليات الانتقال المرتبطة بتعريفات الأسوار الجغرافية القديمة التي لم تعد موجودة في السياسة الحالية.
- تُحفظ انتقالات الأسيجة الجغرافية لمدة **90 يوماً** وتُحذف الانتقالات الأقدم تلقائياً كل ليلة، لذا لا يمكن أن يبدأ البحث بنطاق تاريخ مخصص قبل أكثر من 90 يوماً.

على أجهزة iPhone وiPad، عندما تحتوي السياسة على أسوار جغرافية نشطة، يعرض سطر حالة في أعلى علامة التبويب ما إذا كان السياج الجغرافي يعمل على الجهاز. ويخبرك عندما لا يستطيع العمل: إذا لم يتصل تطبيق Cerberus Enterprise بالخادم أو وجب تحديثه، أو إذا لم يكن الوصول إلى الموقع مضبوطاً على **Always**، أو كان **الموقع الدقيق** أو **تحديث التطبيقات في الخلفية** متوقفاً، أو كان **وضع الطاقة المنخفضة** قيد التشغيل عندما أبلغ التطبيق آخر مرة عن إعداداته (حينها قد تتأخر أحداث السياج الجغرافي والتغييرات لساعات)، أو إذا لم يطبّق التطبيق أحدث الأسوار الجغرافية بعد. وعندما يعمل كل شيء، يعرض عدد الأسوار الجغرافية التي يراقبها التطبيق.

تفاصيل الانتقال عبر السياج الجغرافي

يؤدي تحديد انتقال إلى فتح تفاصيله على الخريطة وإبراز الإدخال المقابل في القائمة. وعندما تتوفر، يعرض Cerberus Enterprise أيضاً إحداثيات الجهاز والدقة المُبلغ عنها لذلك الانتقال.

إدارة شرائح SIM

توفّر صفحة الجهاز لوحة **إدارة شرائح SIM**. على أجهزة Android تدير شرائح SIM وملفات eSIM المثبّتة على الجهاز، وتضيف ملفات eSIM أو تزيلها، وتعرض سجل أوامر eSIM المرسلة إلى الجهاز. على أجهزة iPhone المملوكة للشركة وأجهزة iPad العاملة بالشبكة الخلوية، تعرض شرائح SIM وخطط eSIM التي يبلّغ عنها الجهاز وتتيح للجهاز تنزيل خطط eSIM التي أعدّتها شركة الاتصالات: راجع **iPhone وiPad** أدناه.

> تُبلغ الأجهزة المُدارة بالكامل عن معلومات SIM عندما يكون الإبلاغ عن **معلومات الشبكة** ممكّناً في سياسة الجهاز (هذا الخيار ممكّن دائماً بواسطة Cerberus Enterprise). راجع صفحة **الإبلاغ عن الحالة**.

EID الجهاز

يحدد EID (معرّف eUICC) جهاز eSIM في الجهاز. يستخدمه مشغّل الشبكة لربط ملفات تعريف eSIM بالجهاز، لذلك فإن استرجاعه وعادةً الخطوة الأولى في سير عمل تزويد eSIM.

- **الأجهزة المملوكة للشركة** (Android 13 وما فوق): يُبلَّغ عن EID تلقائياً مع حالة الجهاز ولا يلزم أي تفاعل من المستخدم.
- **الأجهزة المملوكة شخصياً** (Android 13 وما فوق): استخدم زر **طلب EID**. سيرى المستخدم إشعاراً على الجهاز يطلب مشاركة EID، ويمكنه الموافقة على الطلب أو رفضه. لا يظهر EID إلا إذا وافق المستخدم. وبينما الطلب معلّق، يبقى الزر معطّلاً.

> يؤدي إرسال طلب EID إلى عرض مربع حوار تأكيد أولاً، لأن المستخدم سيرى إشعاراً على الجهاز.

شرائح SIM المثبتة

يسرد جدول **شرائح SIM المثبتة** شرائح SIM المعروفة حالياً للجهاز، بما في ذلك شرائح SIM الفعلية وملفات تعريف eSIM. على الأجهزة المملوكة شخصياً، تُعرض ملفات تعريف eSIM المثبتة بأمر **إضافة eSIM** حتى عندما لا يبلغ الجهاز عن معلومات SIM.

- **مشغّل الشبكة**: اسم مشغّل الشبكة المرتبط بشريحة SIM (عند الإبلاغ عنه).
- **رقم الهاتف**: رقم الهاتف المرتبط بشريحة SIM (عند الإبلاغ عنه).
- **ICCID**: معرّف بطاقة الدائرة المتكاملة لشريحة SIM.

- **حالة التنشيط**: ما إذا كانت eSIM منشّطة أم لا. يُبلَّغ عنها فقط لشرائح eSIM على Android 15 وما فوق.
- **وضع التكوين**: ما إذا كان قد تم تكوين eSIM بواسطة المسؤول أو المستخدم. يُبلَّغ عنه فقط لشرائح eSIM على Android 15 وما فوق.
- **نوع SIM**: يعرض ما إذا كان الجهاز يبلغ عن الإدخال كـ eSIM.

> تعرض شرائح eSIM التي لديها أمر إزالة قيد التنفيذ أو منفّذ (غير فاشل) حالة تنشيط مؤقتة **قيد الإزالة**. يختفي الإدخال من القائمة عندما يبلغ الجهاز عن قائمة SIM المحدّثة. وأثناء تنفيذ الإزالة، لا يتوفر زر الإزالة، لتجنب إرسال الأمر نفسه مرتين.

إزالة eSIM

استخدم زر الإزالة بجانب eSIM مثبتة لإزالة ملف تعريفها من الجهاز. يطلب منك مربع حوار تأكيد تأكيد ICCID الخاص بـ eSIM المطلوب إزالتها قبل إرسال الأمر. إزالة eSIM مدعومة على Android 15 وما فوق.

إضافة eSIM

يثبّت قسم **إضافة eSIM** ملف تعريف eSIM جديداً على الجهاز (مدعوم على Android 15 وما فوق). ويتطلب:

- **الصلاحية**: المدة التي يظل الأمر صالحاً خلالها إذا تعذّر تنفيذه فوراً.
- **رمز التنشيط**: رمز التنشيط لملف تعريف eSIM، الذي يوفره مشغّل الشبكة. يمكنك إدخال الرمز الكامل، أو عنوان SM-DP+ فقط للسماح للجهاز باكتشاف ملف تعريف ربطه مشغّل الشبكة بالفعل بـ EID الخاص به.
- **حالة التنشيط**: ما إذا كان يجب تنشيط ملف تعريف eSIM تلقائياً بعد التنزيل، أو تركه غير منشّط ليقوم المستخدم بتنشيطه يدوياً.

سجل الأوامر

أسفل قسم إضافة eSIM، تعرض اللوحة سجل أوامر eSIM المرسلة إلى الجهاز: **إضافة eSIM**، و**إزالة eSIM**، و**طلب EID**. يمكن فرز الجدول ويدعم ترقيم الصفحات. ويمكن توسيع بعض الصفوف لعرض معطيات الأمر (على سبيل المثال رمز التنشيط أو ICCID) وحالة التنفيذ، بما في ذلك تفاصيل خطأ eSIM عندما تفشل عملية على الجهاز.

- **تاريخ الإنشاء**
- **الأمر**
- **الصلاحية**
- **الحالة**

- **الخطأ**: يعرض حالة خطأ eSIM (على سبيل المثال □□□ □□□□□□□□ ، أو □□□ □□□□□ □□□ □□□□ ، أو □□ □□□ □□□□□□ □□□ *ICCID*) عندما يبلّغ تنفيذ الأمر عنه.
- **تاريخ التنفيذ**

مسح شرائح eSIM عند المسح وإلغاء التسجيل

عند مسح الجهاز من لوحة الأوامر، يتحكم خيار **مسح شرائح eSIM** في ما إذا كانت ملفات تعريف eSIM تُزال مع المسح. على الأجهزة المملوكة شخصياً التي لديها ملف تعريف عمل، يكون هذا الخيار ممكّناً افتراضياً (تُزال شرائح eSIM المُدارة، ولا تتأثر شرائح eSIM المملوكة شخصياً). ويتوفر الخيار نفسه في مربع حوار تأكيد **إلغاء تسجيل الجهاز**.

iPhone وiPad

تُعرض اللوحة لأجهزة iPhone ولأجهزة iPad التي أبلغت عن بيانات خلوية (جهاز iPad الذي يدعم Wi-Fi فقط ليس لديه أي منها)، وذلك فقط عندما يكون الجهاز مملوكاً للشركة وليس تسجيل مستخدم. يُطلب من الجهاز معلوماته الخلوية مع معلومات الجهاز: عند التسجيل، وكل يوم، ومع **تحديث معلومات الجهاز**، وعندما تصبح ملكيته مملوكة للشركة، وبعد بضع دقائق من **تحديث الخطط الخلوية**.

- **EID الجهاز**: EID المُبلغ عنه مع شرائح SIM، مع زر لنسخه لمشغّل الشبكة. وإذا لم يبلغ عنه الجهاز، يجده المستخدم في الإعدادات > عام > حول.
- **تم الإبلاغ**، و**التجوال على البيانات**، و**نقطة الاتصال الشخصية**، و**برنامج المودم الثابت**: متى أجاب الجهاز والحالة التي أبلغ عنها. يمكن تغيير التجوال على البيانات ونقطة الاتصال الشخصية عبر **إعدادات الجهاز** في لوحة الأوامر، التي تعرض الحالة الحالية أيضاً.
- **شرائح SIM**: صف واحد لكل شريحة SIM أو خطة eSIM (الأجهزة ذات الشريحتين لديها صفان)، مع الفتحة كما يبلغ عنها الجهاز، وتسميتها ونوعها (**eSIM** عندما يبلغ الجهاز عن EID معها، و**بطاقة SIM** بخلاف ذلك)، ومشغّل الشبكة (مشغّل الشبكة الرئيسي في تلميح عندما يكون الجهاز على شبكة أخرى أثناء التجوال)، ورقم الهاتف، وICCID، وEID، وIMEI، وشريحة SIM المستخدمة للبيانات والمكالمات، والتجوال. وتُعرض فتحة eSIM بدون خطة باللون الرمادي على أنها **لا توجد خطة**.
- **لم يبلغ هذا الجهاز عن أي شريحة SIM** يعني أن الجهاز أجاب دون أي شريحة SIM؛ و**لا توجد معلومات خلوية بعد** يعني أنه لم يجب بعد: استخدم **تحديث معلومات الجهاز**.

> تحدد أرقام الهاتف وICCID وIMEI وEID الشخص والخط: ولا تُطلب أبداً من الأجهزة المملوكة شخصياً أو تسجيلات المستخدم. وعندما يصبح الجهاز مملوكاً شخصياً، تُزال المعلومات

> فوراً وتُخفى في نتائج أوامر معلومات الجهاز القديمة في سجل الأوامر. والـ تُصدَّر والـ تُكتب في سجلات النظام.

تحديث الخطط الخلوية

الـ يمكن لأجهزة iPhone وiPad تثبيت eSIM من رمز تنشيط. يربط مشغّل الشبكة (يحجز) خطة eSIM بـ EID الخاص بالجهاز على خادم eSIM الخاص به (SM-DP+) ويمنحك عنوان ذلك الخادم؛ بعد ذلك يطلب **تحديث الخطط الخلوية** من الجهاز تنزيل الخطط التي تنتظره. ويحدد زر **تحديث الخطط الخلوية** في الـ لوحة الأمر في لوحة الأوامر، حيث تُدخل **عنوان URL لخادم eSIM الخاص بمشغّل الشبكة**:

- **عنوان https://**، يُرسل كما هو. الـ تُقبل العناوين التي تحتوي على http://، أو اسم مستخدم أو كلمة مرور، أو جزء #.
- **اسم مضيف**، على سبيل المثال *smdp.carrier.example*، يُرسل كـ https://smdp.carrier.example.
- **رمز تنشيط LPA** (LPA:1$server$code، نص رمز QR لـ eSIM): يُستخدم الخادم فقط، لأن الأمر الـ يمكنه حمل الرمز. ويجب أن يكون مشغّل الشبكة قد ربط الخطة بـ EID الخاص بالجهاز، وإلا فلن يجد الجهاز ما ينزّله.

يثبّت الجهاز الخطة وينشّطها دون سؤال المستخدم، حتى عندما الـ يكون خاضعاً للإشراف. النجاح في سجل الأوامر يعني أن الجهاز قبل الطلب، وليس أنه تم تثبيت خطة: فقد يستغرق التثبيت حتى ثلاث دقائق، ويطلب Cerberus Enterprise من الجهاز شرائح SIM مرة أخرى بعد نحو ثلاث دقائق، فتظهر الخطة الجديدة في اللوحة. وتُشرح الأخطاء 36001 (تعذّر على الجهاز الوصول إلى نظامه الخلوي)، و36002 (الـ يوجد دعم لـ eSIM)، و36003 (النظام الخلوي مشغول، أعد المحاولة الحقاً) في سجلات النظام. والـ يمكن تنزيل خطة نُزِّلت مرة أخرى: إذا فشل التثبيت، فاتصل بمشغّل الشبكة. ويتوفر الأمر أيضاً لعدة أجهزة في وقت واحد في قائمة **إجراءات أجهزة Apple** في صفحة الأجهزة.

ما الـ تسمح به Apple

- **إضافة eSIM** من رمز تنشيط: غير ممكن، استخدم **تحديث الخطط الخلوية** مع خطة مرتبطة بـ EID.
- **إزالة eSIM**: الـ يمكن إزالة eSIM عن بُعد واحدة تلو الأخرى. يؤدي مسح الجهاز مع إيقاف **الاحتفاظ بخطة بيانات eSIM** إلى إزالة جميع شرائح eSIM. لإيقاف خطة واحدة، اطلب من مشغّل الشبكة إلغاء تنشيطها: تبقى الخطة على الجهاز ولكنها الـ تستطيع الاتصال.
- **طلب EID**: غير مطلوب، إذ يأتي EID مع شرائح SIM الخاصة بالأجهزة المملوكة للشركة.
- **أجهزة Mac** ليس لديها إدارة خلوية أو إدارة eSIM.

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، ويتركه للاستخدام الشخصي. تُحفظ تطبيقات الملف الشخصي وبياناته. يُخرج 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 **اسأل 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** (لا يمكن للجهاز 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.