تزويد الأجهزة - Apple

- نظرة عامة على تجهيز Apple
- تسجيل Apple اليدوي (ملف تعريف التسجيل)
- Apple Automated Device Enrollment (ADE)
- تسجيل Apple الموجّه بالحساب

نظرة عامة على تجهيز Apple

يدعم Cerberus Enterprise تسجيل أجهزة iPhone وiPad وMac وإداراتها. يتطلب تزويد Apple شهادة APNs ويمكن تنفيذه بطرق تسجيل مختلفة.

الشرط المسبق: إعداد Apple Management (APNs)

قبل تسجيل أي جهاز Apple، أكمل **إعداد Apple Management (APNs)**.

اختر طريقة التسجيل

التسجيل اليدوي (ملف تعريف التسجيل)

توفر هذه الطريقة عنوان URL للتسجيل وملف تعريف تهيئة (mobileconfig) تثبّته على الجهاز. اقرأ **التسجيل اليدوي لأجهزة Apple**.

التسجيل التلقائي للأجهزة (ADE)

تتكامل هذه الطريقة مع Apple Business لأتمتة تسجيل الأجهزة المملوكة للشركة. اقرأ **التسجيل التلقائي للأجهزة من Apple (ADE)**.

التسجيل المدفوع بالحساب (تسجيل الدخول بحساب عمل)

يسجّل المستخدمون أجهزة iPhone أو iPad أو Mac الخاصة بهم عبر تسجيل الدخول بحساب Apple المُدار في إعدادات الجهاز: تسجيل المستخدم للأجهزة الشخصية، وتسجيل الجهاز لأجهزة الشركة

غير الموجودة في Apple Business. اقرأ **التسجيل المدفوع بالحساب من Apple**.

على أجهزة iPhone وiPad الشخصية المسجّلة بتسجيل المستخدم، تُثبّت تطبيقات App Store الخاصة بالسياسة باستخدام ترخيص مستخدم لحساب Apple المُدار، الذي يعيّنه Cerberus تلقائيًا؛ ويُطلب من المستخدم تثبيت كل تطبيق. يجب أن تنتمي حسابات Apple المُدارة ورمز Apps and Books إلى المؤسسة نفسها في Apple Business. اقرأ **التطبيقات على الأجهزة الشخصية**.

تطبيق Cerberus Enterprise على iPhone وiPad

بعد التسجيل، يثبّت Cerberus تطبيقه **Cerberus Enterprise** على أجهزة iPhone وiPad التي تعمل بـ **iOS أو iPadOS 18.4 أو أحدث**، مع سياسة أو دونها. يشارك التطبيق موقع الجهاز ويتلقى الإشعارات وطلبات التتبّع المباشر؛ على الأجهزة الشخصية (تسجيل المستخدم) يتلقى الرسائل ويشارك الموقع فقط إذا شغّلت السياسة خيار **الموقع والأسيجة الجغرافية على الأجهزة الشخصية** وسمح المستخدم بذلك. يتطلب خطوة لمرة واحدة: أضف التطبيق المجاني إلى مكتبة Apple Business لديك (**Apps and Books** ← **App Store**، وابحث عن «Cerberus Enterprise»، ثم اختر **إضافة** لجميع الوحدات التنظيمية الحالية والمستقبلية). تثبّت الأجهزة الخاضعة للإشراف التطبيق بصمت؛ وفي الأجهزة الأخرى يُطلب من المستخدم تثبيته. إذا كان المستخدم قد ثبّته بالفعل من App Store، يطلب الجهاز السماح لمؤسستك بإدارة التطبيق، ويحتفظ التطبيق ببياناته وأذوناته. إذا رفض المستخدم، استخدم **إعادة المحاولة** في صفحة الجهاز. لا يمكن للمستخدم حذف التطبيق، ويبقى مثبّتًا إذا انتهت صلاحية رمز Apps and Books. لا تحصل أجهزة Mac على التطبيق.

> يمكنك استخدام التسجيل اليدوي وADE بالتوازي، وفقًا لمجموعة أجهزتك وعملية الشراء لديك.

تسجيل Apple اليدوي (ملف تعريف التسجيل)

يدعم Cerberus Enterprise التسجيل اليدوي لأجهزة Apple باستخدام رمز QR أو عنوان URL للتسجيل أو ملف تعريف تسجيل.

> يتوفر التسجيل اليدوي عند تكوين Apple Management (APNs). إذا لم تكمل إعداد APNs بعد، فاقرأ **إعداد Apple Management (APNs)**.

> يمكن للمستخدمين أيضاً تسجيل أجهزة iPhone أو iPad أو Mac الخاصة بهم دون ملف تعريف، عن طريق تسجيل الدخول بحساب العمل في إعدادات الجهاز. اقرأ **تسجيل Apple الموجّه بالحساب**.

رموز التسجيل

لكل رمز تسجيل عنوان URL للتسجيل ورمز QR خاصان به، ويعيّن هذه الإعدادات للأجهزة التي تسجّل به:

- **السياسة**: تُطبّق على الجهاز بمجرد تسجيله.
- **المستخدم**: يُعيّن للجهاز. وبدون مستخدم في الرمز المميز، لا يكون للجهاز مستخدم.
- **الملكية**: مملوك للشركة أو مملوك شخصياً. عند عدم ضبطها، تُضبط الأجهزة الخاضعة للإشراف كمملوكة للشركة والأجهزة الأخرى كمملوكة شخصياً. أجهزة iPhone وiPad المسجّلة يدوياً ليست خاضعة للإشراف؛ أما أجهزة Mac فهي كذلك، لذا تُضبط كمملوكة للشركة.
- **انتهاء الصلاحية**: بعد هذا اليوم يتوقف عنوان URL للتسجيل عن العمل. ولا يزال من الممكن تثبيت ملف تعريف نُزّل قبل ذلك.
- **عمليات التسجيل المسموح بها**: عدد الأجهزة التي يمكنها التسجيل بالرمز المميز. اتركه فارغاً لعدم وجود حد.

لإنشاء رمز مميز، افتح قسم **التسجيل** في لوحة التحكم، وحدد علامة التبويب **تسجيل Apple اليدوي (ملف تعريف التسجيل)** وانقر **رمز تسجيل جديد**. اضبط الاسم والإعدادات، ثم انقر **إنشاء الرمز**: تعرض صفحة الرمز المميز عنوان URL للتسجيل ورمز QR وزر **تنزيل ملف تعريف التسجيل**.

يعرض جدول الرموز المميزة، لكل رمز، **الحالة** (نشط، منتهي الصلاحية أو مستنفد)، و**تاريخ الانتهاء**، و**عمليات التسجيل** المنجزة من العدد المسموح، و**آخر استخدام**، وهو آخر مرة سجّل فيها جهاز باستخدامه. ثم يأتي **السياسة**، و**المستخدم** (مرّر المؤشر فوقه لرؤية البريد الإلكتروني)، و**المالكية**، و**تاريخ الإنشاء** (مرّر المؤشر فوقه لرؤية من أنشأ الرمز). تظهر أحدث الرموز أولًا، ويمكنك الفرز حسب أي عمود. فرز حسب **آخر استخدام** للعثور على الرموز النشطة التي لم يعد أحد يستخدمها، واحذفها حتى يتوقف عنوان URL الخاص بالتسجيل عن العمل. يظهر أي سياسة أو مستخدم حُذف بعد حفظ الرمز على أنه **سياسة محذوفة** أو **مستخدم محذوف** مع أيقونة تحذير: حرّر الرمز لاختيار آخر.

> تُطبَّق التغييرات على الرمز المميز على عمليات التسجيل التالية: وتحتفظ الأجهزة المسجّلة بالفعل بسياساتها ومستخدمها. وعندما يُحذف رمز مميز أو تنتهي صلاحيته أو يبلغ عمليات التسجيل المسموح بها، يتوقف عنوان URL للتسجيل الخاص به عن العمل.

التسجيل بدون رمز مميز

تعرض لوحة **التسجيل بدون رمز مميز** في علامة التبويب نفسها عنوان URL للتسجيل الخاص بمؤسستك. والأجهزة المسجّلة به لا تحصل على سياسة ولا مستخدم: عيّنهما من صفحة الجهاز.

تعتمد سياسة الجهاز ومستخدمه على كيفية تسجيله: سياسة الرمز المميز ومستخدمه مع رمز تسجيل؛ وسياسة ملف تعريف ADE مع Automated Device Enrollment، مع الاحتفاظ بالمستخدم المعيّن في صفحة الجهاز؛ ولا سياسة ولا مستخدم مع عنوان URL للتسجيل أو رمز QR أو ملف التعريف بدون رمز مميز (حتى إذا كان للجهاز ملف تعريف ADE). والجهاز الذي يعيد التسجيل لا يحتفظ بسياسة تسجيله السابق ومستخدمه: إذا تعرضهما صفحة الجهاز فقط إذا عيّنتهما عملية التسجيل الجديدة. ولا يعيد التسجيل بسياساته ومستخدمه الحاليين إلا جهاز مُمحى باستخدام **إعادة الخدمة**.

الحصول على عنوان URL للتسجيل وملف التعريف

- افتح الرمز المميز في علامة التبويب **تسجيل Apple اليدوي (ملف تعريف التسجيل)** من قسم **التسجيل**، أو وسّع **التسجيل بدون رمز مميز**.
- انسخ **عنوان URL للتسجيل**، أو استخدم إجراء الإرسال بالبريد الإلكتروني.
- امسح **رمز QR** المعروض بجوار عنوان URL للتسجيل باستخدام كاميرا iPhone أو iPad: فهو يفتح عنوان URL نفسه للتسجيل على الجهاز. على Mac، استخدم عنوان URL للتسجيل أو ملف التعريف.
- نزّل **ملف تعريف التسجيل** (ملف mobileconfig).

كيفية تسجيل iPhone أو iPad

iOS/iPadOS 15.0+

أولًا، نزّل ملف تعريف التسجيل على الجهاز باستخدام إحدى الطرق التالية:

الطريقة 1: رمز QR

افتح تطبيق □□□□□□□□ على الجهاز ووجّهه نحو رمز QR الظاهر بجانب عنوان URL للتسجيل، ثم اضغط الرابط الذي يظهر. يفتح Safari عنوان URL للتسجيل ويطلب السماح بتنزيل ملف تعريف التهيئة: اضغط □□□□□□ .

الطريقة 2: عنوان URL للتسجيل

أرسل عنوان URL للتسجيل إلى المستخدم (على سبيل المثال باستخدام إجراء الإرسال بالبريد الإلكتروني) وافتحه في *Safari* على الجهاز، ثم اضغط □□□□□□ لتنزيل ملف تعريف التهيئة.

الطريقة 3: ملف تعريف التسجيل

نزّل ملف تعريف التسجيل (*enroll.mobileconfig*) وأرسله إلى الجهاز، على سبيل المثال كمرفق بريد إلكتروني أو عبر AirDrop، ثم افتحه على الجهاز.

ثم أكمل التسجيل على الجهاز:

1. على الجهاز، افتح □□□□□□□□ → □□ □□□□□ □□□□□ □□□□□□ → □□□□□ ، ثم اتبع التعليمات.
2. بعد التسجيل، يمكنك التحقق من الحالة في □□□□□□□□ → □□□ → *VPN* □□□□□□ □□□□□□□ (أو □□□□□□□ □□□□□□□ □□□□□□ □□□□□□□).

> بعد التسجيل، تحصل أجهزة iPhone وiPad التي تعمل بنظام iOS أو iPadOS 18.4 أو أحدث على تطبيق **Cerberus Enterprise**. على الجهاز المسجّل يدويًا (غير الخاضع للإشراف)، يُطلب من المستخدم تثبيته، أو السماح لمؤسستك بإدارته إذا كان مثبتًا مسبقًا من App Store. إذا رفض المستخدم، استخدم **إعادة المحاولة** في صفحة الجهاز. يجب أن يكون التطبيق في مكتبة Apple Business لديك مرة واحدة (راجع **إعدادات الحساب**).

> على أجهزة iPhone وiPad، يزيل الجهاز ملف تعريف تم تنزيله ولم يُثبّت خلال 8 دقائق. في هذه الحالة، نزّله مرة أخرى.

كيفية تسجيل Mac

macOS 13.0+

يعمل رمز QR على أجهزة iPhone وiPad فقط. نزّل ملف تعريف التسجيل على Mac باستخدام إحدى الطرق التالية:

الطريقة 1: عنوان URL للتسجيل

أرسل عنوان URL للتسجيل إلى المستخدم (على سبيل المثال باستخدام إجراء الإرسال بالبريد الإلكتروني) وافتحه في *Safari* على Mac، ثم اسمح بالتنزيل إذا طُلب منك ذلك. إذا لم يُفتح ملف التعريف تلقائيًا، فافتح ملف *enroll.mobileconfig* الذي نزّلته.

الطريقة 2: ملف تعريف التسجيل

نزّل ملف تعريف التسجيل (*enroll.mobileconfig*) وأرسله إلى Mac، على سبيل المثال كمرفق بريد إلكتروني أو عبر AirDrop، ثم افتحه على Mac.

فتح ملف التعريف يضيفه فقط إلى ملفات التعريف التي تم تنزيلها. ثم أكمل التسجيل على Mac بعد تسجيل الدخول بصفتك المستخدم الرئيسي له:

1. افتح □□□□□□□ □□□□□□ → □□□ → □□□□□ □□□□□□□ (على macOS 13 و14: □□□□□□□ □□□□□□□ → □□□□□ □□□□□□□). في قسم □□ □□□□□□□ ، انقر نقرًا مزدوجًا على □□□ □□□□□ □□□□□□□ ، وانقر على □□□□□ (أو □□□□□) واتّبع التعليمات. أدخل اسم وكلمة مرور مسؤول على Mac إذا طُلب منك ذلك.
2. بعد التسجيل، يظهر □□□ □□□□□ □□□□□□□ في المكان نفسه. في *Terminal*، يعرض `profiles status -type enrollment` النتيجة *MDM enrollment: Yes (User Approved)*.

> أجهزة Mac المسجّلة يدويًا خاضعة للإشراف، ويظهر المستخدم الذي يثبّت ملف التعريف في لوحة **Mac ومستخدمو** في صفحة الجهاز. لا تحصل أجهزة Mac على تطبيق Cerberus Enterprise. إذا لم يعد ملف التعريف في قسم □□ □□□□□□□ ، فنزّله مرة أخرى.

> ثبّت فقط ملفات تعريف التسجيل التي حصلت عليها من لوحة تحكم Cerberus Enterprise.

Apple Automated Device Enrollment (ADE)

يتكامل Automated Device Enrollment (ADE) مع Apple Business (المعروف سابقًا باسم Apple Business Manager) لتسجيل أجهزة iPhone وiPad وMac المملوكة للشركة تلقائيًا عند تشغيلها لأول مرة (أو بعد إعادة ضبط المصنع).

> يتطلب ADE تكوين Apple Management (APNs) أولًا. وإذا لزم الأمر، فاقرأ **إعداد Apple Management (APNs)**.

كيفية تسجيل الأجهزة تلقائيًا

1. أضف الأجهزة إلى حساب Apple Business لديك وعيّنها لخدمة إدارة أجهزة Cerberus Enterprise: في Apple Business، افتح **الأجهزة** ← **المخزون**، وحدد الأجهزة وانقر **تعيين إدارة الأجهزة**، أو عيّن الأجهزة الجديدة تلقائيًا من **الأجهزة** ← **خدمات الإدارة** ← **تعيين الجهاز الافتراضي**. راجع إدارة موردي الأجهزة وإضافة الأجهزة باستخدام Apple Configurator.
2. بعد إضافة أجهزة جديدة إلى حساب Apple Business، زامنها في Cerberus Enterprise من قسم **الأجهزة** باستخدام إجراء **مزامنة من Apple Business**. لا تستهلك الأجهزة المزامنة ترخيصًا إلا بعد تسجيلها.
3. أنشئ ملف تعريف ADE في لوحة التحكم من **التسجيل** ← **Apple Automated Device Enrollment (ADE)** ← **ملف تعريف ADE جديد**.
4. عيّن ملف تعريف ADE لجهاز من صفحة تفاصيل الجهاز باستخدام حقل **ملف تعريف ADE**.

> بعد التسجيل، تحصل أجهزة iPhone وiPad التي تعمل بـ iOS أو iPadOS 18.4 أو أحدث على تطبيق **Cerberus Enterprise**. الأجهزة المسجّلة عبر ADE خاضعة للإشراف، لذا يُثبّت التطبيق دون سؤال المستخدم؛ ولا يُنظر الإعداد تثبيته. يجب أن يكون التطبيق في مكتبة Apple Business لديك مرة واحدة (راجع **إعدادات الحساب**). لا تحصل أجهزة Mac على التطبيق.

إعدادات ملف تعريف ADE (نظرة عامة)

يتحكم ملف تعريف ADE في كيفية تسجيل الجهاز وسلوك مساعد الإعداد. وفي Cerberus Enterprise، يتضمن ملف تعريف ADE اسمًا وسياسة أولية اختيارية وخيارات تسجيل ولوحات مساعد الإعداد المرادة تخطيها وجهات اتصال الدعم والشهادات الموثوقة.

اسم الملف التعريفي

اسم مقروء لملف التعريف (على سبيل المثال، □□□ □□□□□ *ADE* □□□□□□□□□).

السياسة

السياسة المطبّقة على الأجهزة عند تسجيلها بـ Automated Device Enrollment (مساعد الإعداد). أما أجهزة الملف التعريفي المسجّلة بعنوان URL للتسجيل أو رمز QR فتحصل على سياسة رمز التسجيل الخاص بها بدلًا من ذلك، أو لا تحصل على سياسة بدون رمز. وتغيير السياسة فقط يبقي ملف التعريف كما هو.

خيارات التسجيل

- **قابلية إزالة MDM**: يتحكم في ما إذا كان يمكن إزالة حمولة MDM من الجهاز.
- **السماح بالاقتران**: يتحكم في ما إذا كان الاقتران مسموحًا (أهملته Apple في iOS 13).
- **التقدّم التلقائي في الإعداد**: يتقدّم بمساعد الإعداد تلقائيًا عبر شاشاته (Mac بنظام macOS 11 أو أحدث وApple TV).
- **انتظار تكوين الجهاز**: ينتظر مساعد الإعداد حتى تُطبّق سياسة ملف تعريف ADE، ليبدأ المستخدمون بتطبيقاتهم وإعداداتهم جاهزة. ثم يتيح Cerberus Enterprise للجهاز المتابعة، في موعد أقصاه 4 دقائق بعد التسجيل.
- **إلزامي**: يمنع تخطي تطبيق ملف التعريف أثناء الإعداد.
- **متعدد المستخدمين (Shared iPad)**: يكوّن الجهاز وضع Shared iPad.
- **خاضع للإشراف**: يطلب الإشراف على الجهاز.

مساعد الإعداد

- **القسم، هاتف الدعم وبريد الدعم الإلكتروني** (اختياري): يُرسَل إلى Apple مع ملف التعريف. وقد لا يعرضه الجهاز.
- **اللوحات المراد تخطيها**: لا يعرض مساعد الإعداد اللوحات المحددة (على سبيل المثال Apple Account أو Siri أو Screen Time). يعرض كل جهاز لوحات نظامه فقط (بعضها، مثل

FileVault أو iCloud Documents and Desktop، موجود على أجهزة Mac فقط)؛ و**تخطي الكل** و **إظهار الكل** يحدّدان جميع اللوحات أو يلغيانه.
- **Apple TV**: اللغة والمنطقة لـ Apple TV مع التقدّم التلقائي في الإعداد.
- **الشهادات الموثوقة**: مطلوبة فقط إذا كان الخادم يستخدم شهادة ال تثق بها الأجهزة، على سبيل المثال من جهة إصدار شهادات خاصة. استورد الشهادة في صفحة الشهادات أولاً.

قائمة ملفات تعريف ADE

تعرض القائمة اسم كل ملف تعريف، وسياسته، وأجهزته، ومعرّفه (Id)، وهو المعرّف الذي تمنحه Apple لملف التعريف. تشير علامة القفل بعد الاسم إلى ملف تعريف إلزامي ال يمكن لمستخدمي الإدارة إزالته. يشير **ال توجد سياسة** أو **تم حذف السياسة** إلى أن الأجهزة المسجّلة بملف التعريف لن تحصل على سياسة أولية.

يحصي عمود **الأجهزة** الأجهزة المسجّلة لملف التعريف، وبجانبها الأجهزة المنتظرة: المعيّنة لملف التعريف في Apple Business ولكنها غير مسجّلة بعد. ال تُحتسب الأجهزة المزالة.

تغيير ملف التعريف

ال تسمح Apple بتغيير ملف تعريف ADE. وعند تغيير أحدها (باستثناء السياسة فقط)، يحدد Cerberus Enterprise ملف تعريف جديداً بالاسم نفسه ويعيّنه لأجهزة الملف التعريفي القديم؛ والى يبقى ملف التعريف القديم مدرجاً بمجرد أال يستخدمه أي جهاز. وتستخدم الأجهزة التي أكملت مساعد الإعداد بالفعل ملف التعريف الجديد في المرة التالية التي تُمحى فيها.

يمكن حذف أي ملف تعريف ال يستخدمه أي جهاز، مسجّلاً كان أو منتظراً، من قائمة ملفات تعريف ADE. ال تسمح Apple بحذف ملف تعريف، لذا يبقى في Apple Business دون استخدام.

> بعد تعيين ملف تعريف ADE لجهاز، يصبح جاهزاً للتسجيل التلقائي.

تسجيل Apple الموجّه بالحساب

باستخدام التسجيل الموجّه بالحساب، يسجّل المستخدمون أجهزة iPhone أو iPad أو Mac الخاصة بهم عن طريق تسجيل الدخول بحساب العمل (**حساب Managed Apple**، على سبيل المثال *name@company.com*) في إعدادات الجهاز. الملف التعريفي للتنزيل والرمز QR: يعثر Cerberus Enterprise على المستخدم ويطبّق السياسة ويضبط الملكية بنفسه.

وضعان

- **تسجيل المستخدم** (الأجهزة الشخصية): تتم إدارة تطبيقات العمل والحسابات والبيانات فقط، في منطقة منفصلة على الجهاز. لا يمكن لـ Cerberus رؤية البيانات الشخصية أو مسح الجهاز أو تحديد موقعه أو قراءة رقمه التسلسلي. ويُضبط الجهاز على أنه مملوك شخصيًا. يتطلب iOS وiPadOS 15 أو macOS 14 أو أحدث.
- **تسجيل الجهاز** (أجهزة الشركة غير الموجودة في Apple Business): تتم إدارة الجهاز بالكامل، كما في التسجيل اليدوي. يكون جهاز Mac المسجّل بهذه الطريقة خاضعًا للإشراف؛ أما iPhone أو iPad فلا. ويُضبط الجهاز على أنه مملوك للشركة. يتطلب iOS وiPadOS 17.1 أو macOS 14.1 أو أحدث.

> تختار الوضع لأجهزة iPhone وiPad وبشكل منفصل لأجهزة Mac: على سبيل المثال تسجيل المستخدم لأجهزة iPhone الشخصية وتسجيل الجهاز لأجهزة Mac. ويمكنك تغيير ملكية الجهاز لاحقًا في صفحة الجهاز.

> يتوفر التسجيل الموجّه بالحساب عند تكوين Apple Management (APNs). إذا لم تكمل إعداد APNs بعد، فاقرأ **إعداد Apple Management (APNs)**.

إعداد Apple Business

يسجّل المستخدمون الدخول بحسابات Managed Apple، التي تُنشأ في Apple Business. قبل أن تبدأ:

1. **تحقّق من نطاقك** (على سبيل المثال *company.com*) في Apple Business، ضمن نطاقات مؤسستك.

2. **أنشئ حسابات Managed Apple** للمستخدمين لديك، أو ارابط Apple Business بـ Google Workspace أو Microsoft Entra ID: عندئذٍ يكون حساب كل مستخدم عنوان بريده الإلكتروني للعمل ويسجّل الدخول بكلمة مروره.
3. لتسجيل المستخدم، تحقّق في إعدادات إدارة الوصول من أن حسابات Managed Apple يمكنها تسجيل الدخول على **الأجهزة الشخصية**: عندما يمكنها تسجيل الدخول على الأجهزة الخاضعة للإشراف فقط، يفشل تسجيل المستخدم.
4. فقط لخيار **Apple Business** أدناه: افتح **الأجهزة** ← **خدمات الإدارة** ← **تعيين الجهاز الافتراضي** (تعديل) واختر خدمة إدارة أجهزة Cerberus Enterprise لأجهزة iPhone وiPad وMac.

> احتفظ بخدمة إدارة أجهزة Cerberus Enterprise ورمزها المميز في Apple Business ما دامت الأجهزة مسجّلة بحسابات Managed Apple: فقد تؤدي إزالتها إلى توقف عمل الحسابات على الأجهزة.

إعداد Cerberus Enterprise

افتح قسم **التسجيل** في لوحة التحكم وحدد علامة التبويب **تسجيل الدخول بحساب Apple**. وتعرض قائمة تحقق في الأعلى ما إذا كان يلزم اتخاذ إجراء. ولا يمكن إلا للمسؤولين تغيير الإعدادات.

- **السماح بالتسجيل عن طريق تسجيل الدخول بحساب عمل**: يفعّل أو يعطّل التسجيل الموجّه بالحساب للمؤسسة بأكملها.
- **النطاقات**: نطاقات حسابات المستخدمين لديك (على سبيل المثال *company.com*)، حتى 20 نطاقاً. ولا يمكن إلا لحسابات هذه النطاقات التسجيل، وذلك فقط بعد التحقق من النطاق (انظر أدناه).
- **iPhone وiPad وMac**: إيقاف أو تسجيل المستخدم أو تسجيل الجهاز لكل فئة أجهزة.
- **السياسة** لكل وضع: تُطبّق على الأجهزة بمجرد تسجيلها. وبدون سياسة، تسجّل الأجهزة دونها. وتُطبّق السياسة المتغيّرة على عمليات التسجيل التالية.
- **المستخدمون**: [redacted] (يجب أن يتطابق عنوان البريد الإلكتروني للمستخدم في Cerberus Enterprise مع الحساب المكتوب على الجهاز)، أو [redacted].

> تتم مطابقة الحساب المكتوب على الجهاز مع حقل **حساب Managed Apple** الخاص بالمستخدمين، ثم مع عنوان بريده الإلكتروني. ويُرسل الرمز دائماً إلى عنوان البريد الإلكتروني للمستخدم. ويمكن لحساب Managed Apple المعيّن للمستخدم التسجيل حتى عندما لا يكون نطاقه متحققاً منه في Cerberus، على سبيل المثال حساب من النطاق المحجوز *org.appleid.com* الخاص بـ Apple Business. ومع اكتشاف خدمة Apple Business، يكتب المستخدمون دائماً حساب Managed Apple الخاص بهم.

التحقق من النطاقات

بعد حفظ الإعدادات، يعرض قسم **التحقق من النطاق** سجل TXT لكل نطاق. أضفه إلى DNS الخاص بالنطاق، ثم انقر **تحقّق**. قد تستغرق تغييرات DNS بعض الوقت لتظهر. ويبقى النطاق المتحقق منه متحققاً: يمكنك إزالة السجل بعد ذلك. ولا يمكن لمستخدمي نطاق غير متحقق منه التسجيل.

اكتشاف الخدمة: كيف تجد الأجهزة Cerberus Enterprise

عند تسجيل أحد المستخدمين، يسأل الجهاز نطاق الحساب (على سبيل المثال *https://company.com*) عن الخادم الذي يديره. أعدّ واحداً على الأقل من هذه الخيارات الثلاثة. ويعرض قسم **اكتشاف الخدمة** في علامة التبويب عنوان URL للاكتشاف الخاص بمؤسستك والنص الدقيق المراد نسخه لكل خيار.

الخيار 1: Apple Business (موصى به)

انقر **التسجيل في Apple Business**: يخزّن Cerberus Enterprise عنوان URL للاكتشاف في مؤسسة Apple Business لديك ولا يلزم نشر أي شيء على نطاقاتك. ويعرض **التحقق في Apple Business** عنوان URL الذي لدى Apple Business الآن، ويؤدي **الإزالة من Apple Business** إلى إزالته.

- يتطلب iOS وiPadOS 18.2 أو macOS 15.2 أو أحدث. وتحتاج الأجهزة الأقدم إلى الخيار 2 أو 3.
- يتطلب ربط Apple Business في Cerberus Enterprise (رمز خدمة Automated Device Enrollment)، وتعيين الجهاز الافتراضي الموضح أعلاه.
- لا يسأل الجهاز Apple Business إلا عندما لا يجيب نطاقك: يجب أن يكون العنوان *https://company.com/.well-known/com.apple.remotemanagement* موجوداً (خطأ مثل "not found"). وإذا أجاب موقعك الإلكتروني عنه بصفحة ويب، تتوقف الأجهزة عند ذلك. استخدم **التحقق من التكوين** لمعرفة ما يجيب عنه.

> يحتفظ Apple Business بعنوان URL واحد للاكتشاف لكل مؤسسة: فتسجيله يوجّه كل حساب Managed Apple في المؤسسة إلى مؤسسة Cerberus Enterprise هذه. لا تسجّله من مؤسستي Cerberus Enterprise تستخدمان مؤسسة Apple Business نفسها.

الخيار 2: إعادة التوجيه من موقعك الإلكتروني

على خادم الويب لكل نطاق، أعِد توجيه */.well-known/com.apple.remotemanagement* إلى عنوان URL للاكتشاف الخاص بمؤسستك، مع **الاحتفاظ بسلسلة الاستعلام** (فهي تحمل الحساب الذي كتبه المستخدم). يعمل هذا مع كل إصدار نظام تشغيل يدعم التسجيل الموجّه بالحساب،

ويمكن أن يكون الوضع مختلفاً لأجهزة iPhone وMac. انسخ النص الخاص بـ Apache أو nginx من عالمة التبويب؛ ويبدو هكذا، مع مفاتيح مؤسستك:

Apache (.htaccess أو المضيف الظاهري):

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx:

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

على خوادم أو خدمات ويب أخرى (IIS، Cloudflare، لوحات التحكم في الاستضافة)، أنشئ قاعدة إعادة توجيه (302) من المسار نفسه إلى عنوان URL للاكتشاف باستخدام الخيار الذي يحتفظ بسلسلة الاستعلام أو يمررها.

الخيار 3: ملف ثابت على موقعك الإلكتروني

إذا تعذّر عليك إضافة إعادة توجيه، فانشر ملفاً على *https://company.com/.well-known/com.apple.remotemanagement* (دون امتداد ملف)، يُقدَّم مع *Content-Type: application/json*. انسخ محتواه من عالمة التبويب. والخيار الثابت يمكن للملف الواحد: فهو يستخدم الوضع نفسه لأجهزة iPhone وiPad وMac. ولتسجيل المستخدم يبدو هكذا:

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/byod"}]}
```

ولتسجيل الجهاز:

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/adde"}]}
```

> يجب أن يكون وضع الملف أيضاً هو الوضع المضبوط في عالمة التبويب لفئة الجهاز، وإلا يُرفض التسجيل.

التحقق من التكوين

في **التحقق من التكوين**، اختر نطاقًا وجهازًا (iPhone أو Mac) وانقر **تحقّق**: يسأل Cerberus Enterprise النطاق ما الذي سيسأله الجهاز ويعرض الإجابة، وكل إعادة توجيه، وحكمًا. ويعني أن النطاق يشير إلى Cerberus Enterprise أن الخيارين 2 أو 3 يعملان؛ وإجابة خطأ (مثل "not found") مقبولة للخيار 1؛ أما صفحة ويب أو ملف يشير إلى مكان آخر فيوقف الأجهزة. ويحذر الفحص أيضًا عندما تُسقط إعادة التوجيه سلسلة الاستعلام أو عندما لا يُقدّم الملف كـ *application/json*.

مفتاح التسجيل

يحتوي عنوان URL للاكتشاف والتسجيل على مفتاح لمؤسستك. وإذا نُشرت عنوانين URL بالخطأ، فانقر **إعادة إنشاء المفتاح**: تتوقف عنوانين URL القديمة فورًا، لذا حدّث عمليات إعادة التوجيه والملفات الثابتة على مواقعك الإلكترونية. ويسجّل Cerberus Enterprise عنوان URL الجديد في Apple Business بنفسه عند استخدام الخيار 1.

كيف يسجّل المستخدمون

1. iPhone وiPad: افتح □□□□□□□□ ← □□□ ← *VPN* □□□□□□ □□□□□□□ ← □□□□□ □□□□□□ □□□ □□□□ □□□□□ □□ □□□□□□□ . على Mac: □□□□□□□ □□□□□□ ← □□□ ← □□□□□ □□□□□□□ ← □□□□□ □□□□□□ (على macOS 14: □□□□□□□ □□□□□□□ ← □□□□□ □□□□□□□ ← □□□□□ □□□□□□).
2. اكتب حساب Managed Apple، أو عنوان البريد الإلكتروني للعمل للمستخدم في Cerberus (على سبيل المثال *name@company.com*). وعندما يختلف حساب Managed Apple الخاص بالمستخدم عما تم كتابته، يطلب الجهاز بعد ذلك تسجيل الدخول بذلك الحساب.
3. تُفتح صفحة Cerberus Enterprise: اضغط □□□□□ □□□□□ ، ثم أدخل الرمز المكوّن من 6 أرقام الذي وصلك عبر البريد الإلكتروني. تنتهي صلاحية الرمز بعد 10 دقائق؛ وبعد 5 رموز خاطئة، يجب على المستخدم إغلاق الصفحة وتسجيل الدخول مرة أخرى.
4. سجّل الدخول بكلمة مرور حساب Managed Apple (أو بصفحة تسجيل الدخول الخاصة بالشركة عندما يكون Apple Business مرتبطًا بـ Google Workspace أو Microsoft Entra ID)، ثم اسمح بإدارة الجهاز.

> تعرض الحسابات التي لا يمكنها التسجيل (نطاق غير متحقق منه، أو عدم وجود مستخدم مطابق عندما لا يتم إنشاء المستخدمين تلقائيًا، أو وجود عدة مستخدمين بعنوان البريد الإلكتروني نفسه) الرسالة "هذا الحساب غير مُعدّ للتسجيل. اتصل بمسؤول تكنولوجيا المعلومات لديك." وتظهر الأحداث في سجلات النظام في لوحة التحكم.

بعد التسجيل

- تعرض صفحة الجهاز **حساب Managed Apple** المستخدم للتسجيل ونوع التسجيل (تسجيل المستخدم أو تسجيل الجهاز الموجّه بالحساب). وفي قائمة الأجهزة، تعرض أجهزة تسجيل المستخدم "تسجيل المستخدم".
- على أجهزة تسجيل المستخدم، لا تُعرض الأوامر وإعدادات السياسة التي لا تسمح بها Apple (المسح، الموقع، وضع الفقدان، تحديثات نظام التشغيل، العديد من القيود) أو لا تُرسل. وتستخدم تطبيقات App Store في السياسة ترخيص مستخدم بدلًا من ترخيص جهاز (راجع **التطبيقات على الأجهزة الشخصية** أدناه).
- على أجهزة تسجيل المستخدم، تظهر مقاطع الويب على الشاشة الرئيسية ولكنها لا تُدرج في □□□□□□□□□ → □□□ → *VPN* □□□□□□ □□□□□□□ .
- لا تُجدّد شهادة MDM لهذه الأجهزة تلقائيًا ولا تتوفر **إعادة الخدمة**: قبل انتهاء صلاحية شهادة MDM (بعد سنة من التسجيل، راجع صفحة الجهاز)، اطلب من المستخدم إعادة تسجيل الجهاز.
- لمغادرة الإدارة، يسجّل المستخدم الخروج من حساب العمل في المكان نفسه من الإعدادات، أو تلغي تسجيل الجهاز من Cerberus Enterprise. ومع تسجيل المستخدم، تُزال تطبيقات العمل والحسابات والبيانات فقط؛ وتبقى البيانات الشخصية. ويظهر الجهاز الذي يعيد التسجيل جهازًا جديدًا.

> بعد التسجيل مباشرة، قد يُبلَّغ عن بعض ملفات تعريف السياسة (الشهادات وشبكات Wi-Fi ومقاطع الويب) بأنها فشلت بسبب خطأ غير معروف، وقد يظهر الجهاز **غير ممتثل** لفترة. يعيد الجهاز محاولتها من تلقاء نفسه وتُثبَّت بعد فترة، دون الحاجة إلى أي إجراء. لا تحفظ السياسة مجددًا أو تسجّل الجهاز مجددًا بسبب ذلك.

التطبيقات على الأجهزة الشخصية

لا تملك أجهزة iPhone وiPad المسجّلة بتسجيل المستخدم رقمًا تسلسليًا، لذا لا يمكن لـ Apps and Books منحها ترخيص جهاز. ويمنح Cerberus Enterprise تطبيقات App Store في سياستها **ترخيص مستخدم** بدلًا من ذلك: يذهب الترخيص إلى حساب Managed Apple المسجّل الدخول على الجهاز. لا يتغير شيء في السياسة: فالسياسة نفسها تخدم أجهزة الشركة والأجهزة الشخصية، ويختار Cerberus نوع الترخيص لكل جهاز.

- **تلقائي**: عند أول تسجيل، يسجّل Cerberus حساب Managed Apple لدى Apps and Books، ثم يطلب من Apple ترخيصًا لكل تطبيق App Store في السياسة. وتحتاج التطبيقات المجانية إلى ترخيص أيضًا؛ وتمنحها Apple تراخيص غير محدودة. ويستخدم التطبيق المدفوع ترخيصًا واحدًا لكل حساب Managed Apple، تشترك فيه جميع الأجهزة الشخصية لذلك الحساب.

- **المؤسسة نفسها**: يجب أن تنتمي حسابات Managed Apple ورموز Apps and Books الخاص بـ Cerberus Enterprise إلى مؤسسة Apple Business نفسها، ويجب أن تكون التطبيقات في مكتبة موقع الرمز المميز.
- **الترخيص أولاً**: لا يُرسل التطبيق إلى الجهاز إلا بعد أن تؤكد Apple ترخيصه، عادةً خلال بضع دقائق. وحتى ذلك الحين، تعرضه لوحة **التطبيقات** للجهاز على أنه **بانتظار ترخيص مستخدم**، مع السبب.
- **طلب التثبيت**: الأجهزة الشخصية لا تكون خاضعة للإشراف أبدًا، لذلك يسأل iOS المستخدم قبل تثبيت كل تطبيق، بما في ذلك تطبيق **Cerberus Enterprise**، الذي يثبّته Cerberus على هذه الأجهزة أيضًا (**تثبيت** أو **إلغاء**)؛ لا حاجة لتسجيل الدخول إلى Apple Account. إذا ألغى المستخدم، يعرض التطبيق **في انتظار موافقة المستخدم على التثبيت**: استخدم **اطلب مرة أخرى** في صفحة الجهاز لإظهار الطلب مجددًا. لا يمكن للمستخدم حذف التطبيقات المثبّتة بصفتها **مطلوبة**.
- **التطبيقات المثبتة قبل التسجيل**: لا تسمح Apple للمؤسسة بالاستيلاء على تطبيق ثبّته المستخدم شخصيًا على جهاز مسجّل بتسجيل المستخدم. اطلب من المستخدم حذف نسخته قبل التسجيل، أو احذفها ثم استخدم **طلب مرة أخرى** في صفحة الجهاز: عندئذٍ تثبّت المؤسسة النسخة المُدارة.
- **مغادرة الإدارة**: عندما يُلغى تسجيل الجهاز، يزيل iOS التطبيقات المُدارة وبياناتها. ويُحرَّر الترخيص عندما لا يحتاجه أي جهاز مسجّل آخر لحساب Managed Apple نفسه، على سبيل المثال عندما يغادر التطبيق السياسة أو يُلغى تسجيل آخر جهاز؛ وتُحرَّر التراخيص التي لم يعد أحد يحتاجها بواسطة الفحص اليومي خلال يوم.

> عندما يتعذّر على Apple تعيين ترخيص، على سبيل المثال لأن تطبيقًا مدفوعًا لم يعد لديه ترخيص متاح، يعرض التطبيق **فشل ترخيص المستخدم** مع رسالة Apple. أضف تراخيص في Apple Business، ثم استخدم **طلب مرة أخرى** في صفحة الجهاز؛ ويحاول Cerberus أيضًا مرة أخرى بنفسه في الفحص اليومي. ويعرض السطر أعلى قائمة التطبيقات حساب Managed Apple وحالة مستخدم Apps and Books الخاص به؛ والحالة نفسها موجودة في صفحة المستخدم.

> تُستخدم تراخيص المستخدم على أجهزة iPhone وiPad فقط: على أجهزة Mac المسجّلة بتسجيل المستخدم، لا تُثبّت تطبيقات App Store الخاصة بالسياسة. الكتب وحسابات Apple الشخصية غير مدعومة.