# دليل مستخدم HP Sure Admin

**ملخص**

يتيح HP Sure Admin لمسؤولي تكنولوجيا المعلومات إدارة إعدادات البرامج الثابتة الحساسةٍ الخاصة بالجهاز بشكل آمن باستخدام الشهادات وتشفير المفاتيح العامة لكل من الإدارة البعيدة والمحلية للإعدادات بدلاً من كلمة المرور.

# المعلومات القانونية





برامج الكمبيوتر السرية. يجب توافر ترخيص صالح من HP لأغراض الحيازة أو الاستخدام أو النسخ. واستنادًا إلى FAR 12.211 و FAR 12.212، يتم ترخيص برامج الكمبيوتر التجارية ووثائق برامج الكمبيوتر والبيانات الفنية للحاجات التجارية لحكومة الولايات المتحدة بموجب الترخيص التجاري القياسي للبائع.

المعلومات الواردة في هذا الدليل عرضة للتغيير دون إشعار مسبق. وتقتصر الضمانات الخاصة بمنتجات وخدمات شركة HP على تلك المنصوص عليها في بيانات الضمان الصريح المرفق بتلك المنتجات والخدمات. ولا يوجد هنا ما يمكن تفسيره على أنه يشكل ضمانًا إضافيًا. وتخلي شركة HP مسؤوليتها عن أي أخطاء فنية أو تحريرية أو أي أخطاء ناتجة عن السهو والإغفال وردت في هذا المستند.

الإصدار الثاني: أكتوبر 2021

الإصدار الأول: ديسمبر 2019

الرقم المرجعي للمستند: L83995-172

# جدول المحتويات

# ١ بدء التشغيل

يتيح HP Sure Admin لمسؤولي تكنولوجيا المعلومات إدارة إعدادات البرامج الثابتة الحساسة الخاصة بالجهاز بشكل آمن باستخدام الشهادات وتشفير المفاتيح العامة لكل من الإدارة البعيدة والمحلية للإعدادات بدلاً من كلمة المرور.

يتكون HP Sure Admin من القطع التالية:

- **جهاز الكمبيوتر المستهدف:** الأنظمة الأساسية لإدارة ذلك تدعم "وضع مصادقة BIOS المحسنة".
- **HP Manageability Integration Kit (MIK):** المكوِّن الإضافي لـ System Center Configuration Manager (SCCM) أو HP BIOS Configuration Utility (BCU) لإدارة إعدادات BIOS عن بُعد.
- **HP Sure Admin Local Access Authenticator:** تطبيق هاتف يستبدل كلمة المرور ليتيح الوصول إلى إعداد BIOS عن طريق المسح الضوئي لرمز استجابة سريعة للحصول على رقم تعريف شخصي لمرة واحدة.

## استخدام HP Sure Admin

يصف هذا القسم عملية استخدام HP Sure Admin.

١. افتح المكوِّن الإضافي HP Sure Admin داخل المكوِّن الإضافي HP Manageability Integration Kit (MIK) لـ System Configuration Manager (SCCM) أو Enhanced BIOS Configuration Utility (BCU).

٢. قم بتنزيل تطبيق الهاتف HP Sure Admin إما من متجر Google Play™ أو متجر Apple App®.

٣. قم بإنشاء زوج مفاتيح يتم استخدامه من قبل الجهاز المستهدف وتطبيق الهاتف HP Sure Admin للحصول على رقم تعريف شخصي لمرة واحدة لإلغاء قفل BIOS.

## تعطيل HP Sure Admin

يصف هذا القسم خيارات تعطيل HP Sure Admin.

- من إعداد BIOS F10، حدد **Restore Security settings to Factory Defaults** (استعادة إعدادات الأمان إلى افتراضيات المصنع).

**ملاحظة:** يتطلب ذلك وجودًا فعليًا عن طريق تقديم مصادقة رقم التعريف الشخصي بواسطة تطبيق الهاتف HP Sure Admin للوصول إلى إعدادات F10.

- استخدم الأمر BCU لطلب WMI الخاص بـ **Restore Security settings to Factory Defaults** (استعادة إعدادات الأمان إلى افتراضيات المصنع) عن بُعد.

**ملاحظة:** للحصول على مزيد من المعلومات، راجع دليل مستخدم HP BIOS Configuration Utility (BCU).

- من صفحة MIK Security Provisioning (توفير الأمان لـ MIK)، حدد **Deprovision** (إزالة).

# ٢ إنشاء المفاتيح وإدارتها

إكمال توفير الأمان ضمن MIK قبل تمكين "وضع مصادقة BIOS المحسّن". يتعين تمكين "وضع مصادقة BIOS المحسّن" لإنشاء المفاتيح وتصديرها. لتمكين وضع مصادقة BIOS:

▲ افتح المكوّن الإضافي HP Sure Admin وحدد **Enhanced BIOS Authentication Mode** (وضع مصادقة BIOS المحسّن) لإنشاء المفاتيح وتصديرها.

## إنشاء المفاتيح وتصديرها

هناك 3 طرق مختلفة لإنشاء أزواج مفاتيح للوصول المحلي، وقم بتمكين تطبيق الهاتف HP Sure Admin للوصول إلى المفتاح.

- إنشاء مفتاح وتصديره بالتوزيع اليدوي في صفحة ٢
- إنشاء مفتاح وتصديره باستخدام Azure AD Revocation في صفحة ٣
- إنشاء مفتاح وإرساله إلى Azure AD Group OneDrive في صفحة ٣

### إنشاء مفتاح وتصديره بالتوزيع اليدوي

استخدم هذا الخيار لتصدير مفتاح مصادقة الوصول المحلي، ثم قم بتوزيعه يدويًا على تطبيق الهاتف HP Sure Admin من خلال البريد الإلكتروني أو طريقة أخرى.

**ملاحظة:** لا يتطلب هذا الخيار الوصول إلى شبكة تطبيقات الهواتف HP Sure Admin للحصول على رقم تعريف شخصي لمرة واحدة.

١. قم بتسمية مفتاحك في مربع الإدخال **Key Name** (اسم المفتاح).

٢. أدخل عبارة المرور في مربع الإدخال **Passphrase** (عبارة المرور).

**ملاحظة:** يتم استخدام عبارة مرور لحماية المفتاح الذي تم تصديره ويتعين تقديمها كي يتمكن مستخدم تطبيق الهاتف HP Sure Admin من استيراد المفتاح.

٣. حدد **Browse** (استعراض)، واختر مكان تصدير المسار في النظام.

٤. حدد **Create Key** (إنشاء مفتاح). تم إنشاء مفتاحك بنجاح عِند ظهور أيقونة إعلام بجوار الزر **Create key** (إنشاء مفتاح) مع الرسالة **Key successfully created** (تم إنشاء المفتاح بنجاح).

٥. اختر **التالي**. تعرض صفحه الملخص إعدادات HP Sure Admin التي أدخلتها.

٦. حدد **Save Policy** (حفظ النهج). يتم حفظ النهج عند ظُهور الرسالة **Saved successfully** (تم الحفظ بنجاح).

٧. انتقل إلى المجلد الذي قمت بحفظ المفتاح فيه وقم بتوزيعه إلى مستخدم تطبيق الهاتف HP Sure Admin مستخدمًا طريقة متوفرة لذلك المستخدم على هذا الجهاز، مثل البريد الإلكتروني. سيحتاج هذا المستخدم أيضًا إلى عبارة مرور لاستيراد المفتاح. توصي HP باستخدام آليات توزيع مختلفة للمفتاح وعبارة المرور.

**ملاحظة:** وعند إرسال رمز الاستجابة السريعة، أرسله بحجمه الأصلي. لا يمكن للتطبيق قراءه الصورة بشكل صحيح إذا كانت أصغر من 800 × 600 من حيث الحجم.

## إنشاء مفتاح وتصديره باستخدام Azure AD Revocation

استخدم هذا الخيار لتوصيل مفتاح الوصول المحلي بمجموعة Active Directory Azure محددة، علمًا بأنه يتطلب تطبيق الهاتف HP Sure Admin لطلب مصادقة المستخدم لـ Azure Active Directory وتأكيد أن المستخدم عضو في المجموعة المحددة قبل توفير رقم تعريف شخصي للوصول المحلي. تتطلب هذه الطريقة أيضًا التوزيع اليدوي لمفتاح مصادقة الوصول المحلي إلى تطبيق الهاتف من خلال البريد الكتروني أو طريقة أخرى.

**ملاحظة:** يتطلب هذا الخيار تطبيق الهاتف HP Sure Admin للوصول إلى الشبكة للحصول على رقم تعريف شخصي لمرة واحدة.

١. قم بتسمية مفتاحك في مربع الإدخال **Key Name** (اسم المفتاح).

٢. أدخل عبارة المرور في مربع الإدخال **Passphrase** (عبارة المرور).

**ملاحظة:** يتم استخدام عبارة مرور لحماية المفتاح الذي تم تصديره ويتعين تقديمها كي يتمكن مستخدم تطبيق الهاتف HP Sure Admin من استيراد المفتاح.

٣. حدد **Azure AD Login** (تسجيل الدخول إلى Azure AD) وسجل الدخول.

٤. حدد اسم المجموعة من المربع المنسدل **Azure AD Group Name** (اسم مجموعة Azure AD). يتعين أن يكون عضوًا في المجموعة لتتمكن من الوصول إلى المفتاح.

٥. حدد **Browse** (استعراض)، واختر مكان تصدير المسار في النظام.

٦. حدد **Create Key** (إنشاء مفتاح). تم إنشاء مفتاحك بنجاح عند ظهور أيقونة إعلام بجوار الزر **Create key** (إنشاء مفتاح) مع الرسالة **Key successfully created** (تم إنشاء المفتاح بنجاح).

٧. اختر **التالي**. تعرض صفحه الملخص إعدادات HP Sure Admin التي أدخلتها.

٨. حدد **Save Policy** (حفظ النهج). يتم حفظ النهج عند ظُهور الرسالة **Saved successfully** (تم الحفظ بنجاح).

٩. انتقل إلى المجلد الذي قمت بحفظ المفتاح فيه وقم بتوزيعه إلى مستخدم تطبيق الهاتف HP Sure Admin مستخدمًا طريقة متوفرة لذلك المستخدم على هذا الجهاز، مثل البريد الإلكتروني. سيحتاج هذا المستخدم أيضًا إلى عبارة مرور لاستيراد المفتاح. توصي HP باستخدام آليات توزيع مختلفة للمفتاح وعبارة المرور.

**ملاحظة:** وعند إرسال رمز الاستجابة السريعة، أرسله بحجمه الأصلي. لا يمكن للتطبيق قراءه الصورة بشكل صحيح إذا كانت أصغر من 800 × 600 من حيث الحجم.

## إنشاء مفتاح وإرساله إلى Azure AD Group OneDrive

(مستحسن) استخدم هذا الخيار لتجنب تخزين مفتاح مصادقة الوصول المحلي على الهاتف. عند اختيارك هذا الخيار، سيقوم MIK بتخزين مفتاح مصادقة الوصول المحلي إلى المجلد OneDrive المحدد الذي لا يمكن الوصول

إليه إلا من خلال المجموعة المعتمدة فقط. سيتعين على مستخدم تطبيق الهاتف HP Sure Admin مصادقة الوصول إلى Azure AD في كل مرة يلزم فيها رقم تعريف شخصي.

١. قم بتسمية مفتاحك في مربع الإدخال **Key Name** (اسم المفتاح).

٢. أدخل عبارة المرور في مربع الإدخال **Passphrase** (عبارة المرور).

٣. حدد **Azure AD Login** (تسجيل الدخول إلى Azure AD) وسجل الدخول.

٤. حدد اسم المجموعة من المربع المنسدل Azure AD Group Name (اسم مجموعة Azure AD).

**ملاحظة:** يتعين أن يكون عضوًا في المجموعة لتتمكن من الوصول إلى المفتاح.

٥. أدخل اسم مجلد OneDrive الذي تريد حفظ المفتاح إليه في مربع الإدخال **OneDrive**.

٦. حدد **Browse** (استعراض)، واختر مكان تصدير المسار في النظام.

٧. حدد **Create Key** (إنشاء مفتاح).

**ملاحظة:** تتم إضافة مفتاحك بنجاح إلى مجلد OneDrive المحدد وتصديره إلى المجلد المحلي المعيّن عند ظهور أيقونة إعْلام بجوار الزر **Create Key** (إنشاء مفتاح) مع الرسالة **Key successfully created** (تم إنشاء المفتاح بنجاح).

٨. اختر **التالي**. تعرض صفحه الملخص إعدادات HP Sure Admin التي أدخلتها.

٩. حدد **Save Policy** (حفظ النهج). يتم حفظ النهج عند ظُهور الرسالة **Saved successfully** (تم الحفظ بنجاح).

**ملاحظة:** في هذا السيناريو، لا توجد حاجة إلى إرسال أي شيء إلى تطبيق الهاتف HP Sure Admin لتقديمه. يتم تقديم أجهزه الكمبيوتر المستهدفة للإشارة إلى موقع OneDrive المضمّن في رمز الاستجابة السريعة. يستخدم تطبيق الهاتف HP Sure Admin هذا المؤشر للوصول إلى موقع OneDrive إذا كان المستخدم جزءًا من المجموعة المعتمدة وتمت مصادقته بنجاح.

# ٣ إعداد الهاتف

قم بتنزيل تطبيق الهاتف HP Sure Admin إما من متجر Google Play أو متجر Apple App.

- قم بتنزيل HP Sure Admin من متجر Google لهواتف Android.
- قم بتنزيل HP Sure Admin من متجر Apple لهواتف iOS.

## استخدام HP Sure Admin لإلغاء قفل BIOS

يستبدل تطبيق الهاتف HP Sure Admin استخدام كلمة مرور BIOS للوصول المحلي إلى إعداد BIOS عن طريق تقديم رقم التعريف الشخصي لمرة واحدة الذي تم الحصول عليه عن طريق المسح الضوئي لرمز الاستجابة السريعة المعروض من قبل الجهاز المستهدف.

اتبع هذه الخطوات لحفظ المفتاح محليًا على الهاتف في سيناريو يتم إرسال المفتاح فيه إلى مستخدم تطبيق الهاتف. في المثال التالي، يتم إرسال المفتاح عبر البريد الإلكتروني إلى مستخدم تطبيق HP Sure Admin عبر الهاتف، ويفتح المستخدم البريد الإلكتروني على الهاتف.

١. افتح البريد الإلكتروني الذي يحتوي على المفتاح.

٢. عندما يتم عرض صفحة **Enrollment** (التسجيل)، أدخل العبارة في مربع الإدخال **Enter passphrase** (إدخال عبارة مرور) وعنوان البريد الإلكتروني في مربع الإدخال **Enter your email address** (إدخال عنوان بريدك الإلكتروني) لفك تشفير المفتاح وإضافته إلى تطبيق HP Sure Admin. يتم عرض رقم التعريف الشخصي لإلغاء القفل في الصفحة **Your PIN** (رقم التعريف الشخصي الخاص بك).

**ملاحظة:** تحفظ هذه الخطوة المفتاح في الجهاز المحمول وتستكمل التسجيل. في هذه المرحلة، يمكنك استخدام تطبيق الهاتف HP Sure Admin للوصول إلى أي جهاز تم تقديمه للوصول إليه بواسطة هذا المفتاح. ولا يلزم عنوان بريد إلكتروني إلا إذا طلبه المسؤول فقط.

٣. أدخل رقم التعريف الشخصي في مربع الإدخال **BIOS Enter Response Code** (إدخال رمز الاستجابة السريعة لـ BIOS).

### للتمكن من الوصول إلى إعداد BIOS بعد التسجيل

للتمكن من الوصول إلى إعداد BIOS على جهاز مستهدف بعد التسجيل:

١. أدخل إعداد BIOS عند التمهيد على الجهاز المستهدف.

٢. حدد **Scan QR Code** (المسح الضوئي لرمز الاستجابة السريعة) من تطبيق الهاتف، وامسح رمز الاستجابة السريعة ضوئيًا على الجهاز المستهدف.

٣. إذا تمت المطالبة بمصادقة المستخدم، فقم بتقديم بيانات اعتمادك.

٤. يتم عرض رقم التعريف الشخصي لإلغاء القفل في الصفحة **Your PIN** (رقم التعريف الشخصي الخاص بك).

٥. أدخل رقم التعريف الشخصي في مربع الإدخال **BIOS Enter Response Code** (إدخال رمز الاستجابة السريعة لـ BIOS) على الجهاز المستهدف.

## قم بإلغاء تأمين BIOS باستخدام Azure AD Group OneDrive

لاستخدام HP Sure Admin لإلغاء قفل BIOS باستخدام Azure AD Group OneDrive:

١. حدد **Scan QR Code** (مسح رمز الاستجابة السريعة ضوئيًا)، ثم امسح رمز الاستجابة السريعة لـ BIOS.

**ملاحظة:** يعرض تطبيق HP Sure Admin صفحة تسجيل الدخول إلى Azure AD.

٢. تسجّل الدخول إلى حساب Azure الخاص بك.

٣. أدخل رقم التعريف الشخصي في مربع الإدخال **BIOS Enter Response Code** (إدخال رمز الاستجابة السريعة لـ BIOS).

**ملاحظة:** لا يحفظ تطبيق HP Sure Admin المفتاح محليًا في هذا السيناريو. يتعين أن يتوفر لتطبيق الهاتف HP Sure Admin إمكانية الوصول إلى الشبكة، كما يتعين أن يصادق المستخدم في كل مرة تكون فيها حاجة إلى رقم التعريف الشخصي لمرة واحدة.

# ٤ رموز الخطأ الخاصة بـ HP Sure Admin

استخدم الجدول في هذا القسم لمشاهدة رموز الأخطاء وأنواعها وأوصافها الخاصة بـ HP Sure Admin و KMS Admin Console.

**جدول ٤-١ رموز وأنواع وأوصاف تطبيق HP Sure Admin**

| رمز الخطأ | نوع الخطأ | الوصف |
|---|---|---|
| 100 | QRCodeUnknownError | خطأ عام. |
| 101 | QRCodeDeserialization | يتعذر قراءة JSON لرمز الاستجابة السريعة. إما أن السلسلة ليست ملف JSON صالح أو أن البيانات غير صالحة. |
| 102 | QRCodeInvalidImage | صورة رمز الاستجابة السريعة الممسوحة ضوئيًا غير صالحة. تتعذر قراءة ملف صورة رمز الاستجابة السريعة. |
| 103 | QRCodeNoLoad | صورة رمز الاستجابة السريعة الممسوحة ضوئيًا غير صالحة. لا تحتوي ملفات الصور على حمولة JSON. |
| 104 | QRCodeInvalid | تتعذر قراءة سلسلة JSON لرمز الاستجابة السريعة. إما أن السلسلة ليست JSON صالحة أو أن صورة رمز الاستجابة السريعة غير صالحة. |
| 105 | QRCodeInvalidKeyIdHash | رمز الشباك للمفتاح العام في سلسلة JSON لرمز الاستجابة السريعة لا يتطابق مع رمز الشباك للمفتاح العام لحزمة التسجيل (بيانات معرِّف المفتاح). |
| 106 | QRCodeTampered | صورة رمز الاستجابة السريعة الممسوحة ضوئيًا عُبِث بها أو غير صالحة. |
| 107 | QRCodeTamperedOrInvalidPassrase | يتم العبث بصورة رمز الاستجابة السريعة التي تم مسحها ضوئيا أو أنها غير صالحة، أو تكون كلمة المرور التي تم إدخالها غير صحيحة. |

**جدول ٤-٢ مفتاح الوصول إلى OneTime من أخطاء OneDrive، وأنواعه، وأوصافه**

| رمز الخطأ | نوع الخطأ | الوصف |
|---|---|---|
| 200 | OneTimeKeyError | خطأ عام. |
| 201 | OneTimeKeyNoUserGroups | لا ينتمي المستخدم الذي تَم تسجيل دخوله إلى أي مجموعة AD في مؤسستك. |
| 203 | OneTimeKeyInvalidUserGroup | لا ينتمي المستخدم الذي تم تسجيل دخوله إلى المجموعة AD المعينة إلى هذا المفتاح. |

جدول ٤-٢ مفتاح الوصول إلى OneTime من أخطاء OneDrive، وأنواعه، وأوصافه (يُتبع)

| رمز الخطأ | نوع الخطأ | الوصف |
|---|---|---|
| 204 | OneTimeKeyQRFileFileDoesExist | ملف المفتاح OneTime غير موجود في مجلد OneDrive لمجموعة AD. |
| 205 | OneTimeKeyInvalidQRFile | ملف المفتاح OneTime في مجلد OneDrive لمجموعة AD غير صالح. |
| 206 | OneTimeKeyInvalidQRload | ملف المفتاح OneTime موجود ولكن لا يمكنه قراءة حمولة الملف. |

جدول ٤-٣ أخطاء في تفويض Azure AD

| رمز الخطأ | نوع الخطأ | الوصف |
|---|---|---|
| 300 | AzureADUnknownError | خطأ عام. |
| 301 | AzureADInvalidDomain | عنوان البريد الإلكتروني الذي تم إدخاله لا يتطابق مع اسم المجال المحدد في صورة رمز الاستجابة السريعة. |
| 302 | AzureADAccessToken | خطأ في الحصول على الرمز المميز من Azure AD. إما أن المستخدم لا يمكنه تسجيل الدخول إلى Azure AD لمؤسستك أو أن التطبيق لا يمتلك الأذونات المطلوبة للاتصال بـ Azure AD لمؤسستك. وقد يكون السبب أيضا هو إلغاء المستخدم للمصادقة. |
| 303 | AzureADUserProfile | تم تمكين تطبيق HP Sure Admin للحصول على معلومات ملف تعريف المستخدم من Azure AD لمؤسستك. |
| 304 | AzureADUserCipnalMismatsch | عنوان البريد الإلكتروني الذي تم إدخاله لا يتطابق مع الاسم الرئيسي للمستخدم الذي قام بتسجيل الدخول. |
| 305 | AzureADUserInvalidUserGroup | لا ينتمي المستخدم الذي قام بتسجيل الدخول إلى مجموعة Azure AD المعينة التي تم تعيين هذا المفتاح لها. |

جدول ٤-٤ أخطاء KMS Admin Console وأنواعها، وأوصافها

| رمز الخطأ | نوع الخطأ | الوصف |
|---|---|---|
| 401 | KmsUnauthorized | المستخدم غير مفوض لاستخدام خدمة KMS. |
| 402 | KmsKeyDoesNotExist | لا يوجد مفتاح خاص مطابق في خزنة مفاتيح KMS. يوجد المفتاح في حالة حذف ولكن يمكن استرداده حاليًا، ولا يمكن إعادة استخدام اسمه في هذه الحالة. يمكن استرداد المفتاح أو حذفه فقط. |
| 403 | KmsKeyDoesNotExistInTableStorage | المفتاح غير موجود في مخزون الجدول. |

جدول ٤-٤ أخطاء KMS Admin Console وأنواعها، وأوصافها (يُتبع)

| رمز الخطأ | نوع الخطأ | الوصف |
|---|---|---|
| 404 | KmsUploadKeyErrorInKeyVault | لقد حدث خطأ أثناء إضافة مفتاح إلى قبو المفاتيح. |
| 405 | KmsUploadKeyUnauthorized | لا يُصرح للمستخدم بتحميل المفاتيح. لا ينتمي المستخدم إلى مجموعة AD المعتمدة المسموح لها بالاتصال بـ API هذا. |
| 406 | KmsInvalidAzureADLogin | لم يقم المستخدم بتسجيل الدخول إلى Azure Tenant AAD. |
| 407 | KmsNoUserGroups | لا ينتمي المستخدم الذي سجل دخوله إلى أي مجموعة AD في مؤسستك. |
| 408 | KmsInvalidUserGroup | لا ينتمي المستخدم الذي تم تسجيل دخوله إلى مجموعة AD المعينة إلى هذا المفتاح. |
| 409 | KmsInvalidAccessToken | رمز الوصول المميز الذي تم توفيره في الطلب غير صالح. |
| 410 | KmsAccessTokenExpired | انتهت صلاحية الوصول إلى Token الموفر. |
| 411 | KmsAccessTokenInvalidTenantId | إن accessToken الذي يتم توفيره لديه قيمة TenantId غير صالحة. |
| 412 | KmsAccessTokenTenantIdMismatch | لا يتطابق TenantId الموجود في accessToken المقدم مع TenantId لتطبيق الوظيفة. |
| 413 | KmsInvalidKeyId | إن KeyId فارغ أو غير موجود. |
| 414 | KmsDeleteKeyUnauthorized | لا يُصرح للمستخدم بحذف المفاتيح. لا ينتمي المستخدم إلى مجموعة AD المعتمدة المسموح لها بالاتصال بـ API هذا. |
| 415 | KmsKeyVaultSoftDeleteUnrecoverableState | فشلت محاولة استرداد السر، ولم يمكن استرداده. يجب أن يقوم المستخدم بالمحاولة مرة أخرى. |
| 416 | KmsInvalidGetKeysRequest | طلب الحصول على المفاتيح غير صالح. |
| 417 | KmsGetKeysUnauthorized | لا يصرح للمستخدم الحصول على المفاتيح. لا ينتمي المستخدم إلى مجموعة AD المعتمدة المسموح لها بالاتصال بـ API هذا. |
| 418 | KmsInvalidRequestPayload | البيانات المتلقاة من API غير صحيحة. |
| 419 | KmsRequestRequired | يجب أن يكون الطلب الذي تم استقباله غير فارغ. |
| 420 | KmsKeyNotConcurrent | تم تحديث المفتاح الخاص بمخزون الجدول أو تعديله منذ أن قام المستخدم باسترجاع نسخة منه آخر مرة. |