# HP Sure Admin Benutzerhandbuch

**ZUSAMMENFASSUNG**

HP Sure Admin ermöglicht IT-Administratoren die sichere Remote- und lokale Verwaltung sensibler Geräte-Firmware-Einstellungen mithilfe von Zertifikaten und auf öffentlichen Schlüsseln basierender Kryptographie anstelle eines Kennworts.

# Rechtliche Hinweise



Apple ist eine eingetragene Marke von Apple Computer, Inc. in den USA und anderen Ländern.

Google Play ist eine Marke von Google LLC.

Vertrauliche Computersoftware. Für den Besitz, die Verwendung oder die Vervielfältigung dieser Software ist eine gültige Lizenz von HP erforderlich. In Übereinstimmung mit FAR 12.211 und 12.212 sind kommerziell genutzte Computersoftware, Computersoftware-Dokumentationen und technische Dokumentationen für kommerziell genutzte Geräte gemäß den HP Standardlizenzbedingungen für die kommerzielle Nutzung an die US-Regierung lizenziert.

HP haftet – ausgenommen für die Verletzung des Lebens, des Körpers, der Gesundheit oder nach dem Produkthaftungsgesetz – nicht für Schäden, die fahrlässig von HP, einem gesetzlichen Vertreter oder einem Erfüllungsgehilfen verursacht wurden. Die Haftung für grobe Fahrlässigkeit und Vorsatz bleibt hiervon unberührt. Inhaltliche Änderungen dieses Dokuments behalten wir uns ohne Ankündigung vor. Die Informationen in dieser Veröffentlichung werden ohne Gewähr für ihre Richtigkeit zur Verfügung gestellt. Insbesondere enthalten diese Informationen keinerlei zugesicherte Eigenschaften. Alle sich aus der Verwendung dieser Informationen ergebenden Risiken trägt der Benutzer. Die Herstellergarantie für HP Produkte wird ausschließlich in der entsprechenden, zum Produkt gehörigen Garantieerklärung beschrieben. Aus dem vorliegenden Dokument sind keine weiter reichenden Garantieansprüche abzuleiten.

Zweite Ausgabe: Oktober 2021

Erste Ausgabe: Dezember 2019

Dokumentennummer: L83995-042

# Inhaltsverzeichnis

# 1 Einführung

HP Sure Admin ermöglicht IT-Administratoren die sichere Remote- und lokale Verwaltung sensibler Geräte-Firmware-Einstellungen mithilfe von Zertifikaten und auf öffentlichen Schlüsseln basierender Kryptographie anstelle eines Kennworts.

HP Sure Admin besteht aus den folgenden Elementen:

- **Ziel-PC:** Die Plattformen für die Verwaltung, die den Enhanced BIOS Authentication Mode (erweiterter BIOS-Authentifizierungsmodus) unterstützen.
- **HP Manageability Integration Kit (MIK):** Das Plug-In für System Center Configuration Manager (SCCM) oder HP BIOS Configuration Utility (BCU) zur Remote-Verwaltung der BIOS-Einstellungen.
- **HP Sure Admin Local Access Authenticator:** Eine Telefon-App, die das Kennwort ersetzt, um den lokalen Zugriff auf das BIOS-Setup zu aktivieren, indem ein QR-Code gescannt wird, um eine einmalige PIN zu erhalten.

## Verwenden von HP Sure Admin

In diesem Abschnitt wird die Verwendung von HP Sure Admin beschrieben.

1. Öffnen Sie das HP Sure Admin Plug-In innerhalb des HP Manageability Integration Kit (MIK) Plug-Ins für System Configuration Manager (SCCM) oder Enhanced BIOS Configuration Utility (BCU).
2. Laden Sie die HP Sure Admin Telefon-App im Google Play™ Store oder Apple App Store herunter®.
3. Erstellen Sie ein Schlüsselpaar, das vom Zielgerät und der HP Sure Admin Telefon-App verwendet wird, um eine einmalige PIN zum Entsperren des BIOS zu erhalten.

## Deaktivieren von HP Sure Admin

Dieser Abschnitt beschreibt die Optionen, mit denen HP Sure Admin deaktiviert werden kann.

- Wählen Sie in der BIOS F10-Einstellung **Restore Security settings to Factory Defaults** (Sicherheitseinstellungen auf die Werkseinstellungen zurücksetzen) aus.

**HINWEIS:** Hierzu ist die physische Präsenz erforderlich, um für den Zugriff auf die F10-Einstellungen die PIN zur Authentifizierung per HP Sure Admin Telefon-App einzugeben.

- Verwenden Sie den BCU-Befehl für den Remote-Aufruf der WMI von **Restore Security settings to Factory Defaults** (Sicherheitseinstellungen auf die Werkseinstellungen zurücksetzen).

**HINWEIS:** Weitere Informationen finden Sie im Benutzerhandbuch zu HP BIOS Configuration Utility (BCU).

- Wählen Sie auf der Seite zur MIK-Sicherheitsbereitstellung die Option **Bereitstellung aufheben** aus.

# 2 Erstellen und Verwalten von Schlüsseln

Schließen Sie die Sicherheitsbereitstellung innerhalb des MIK ab, bevor Sie den Enhanced BIOS Authentication Mode (erweiterter BIOS-Authentifizierungsmodus) aktivieren. Der erweiterte BIOS-Authentifizierungsmodus muss aktiviert sein, um Schlüssel erstellen und exportieren zu können. So aktivieren Sie den BIOS-Authentifizierungsmodus:

▲ Öffnen Sie das HP Sure Admin Plug-in, und wählen Sie **Enhanced BIOS Authentication Mode** aus, um Schlüssel zu erstellen und zu exportieren.

## Erstellen und Exportieren von Schlüsseln

Es gibt drei unterschiedliche Wege, um lokale Tastenkombinationen zu erstellen, und die HP Sure Admin Telefon-App zu aktivieren, um auf den Schlüssel zuzugreifen:

- Schlüssel mit manueller Verteilung erstellen und exportieren auf Seite 2
- Einen Schlüssel mit Azure AD Revocation erstellen und exportieren auf Seite 3
- Erstellen Sie einen Schlüssel und senden Sie ihn an Azure AD Group OneDrive: auf Seite 3

### Schlüssel mit manueller Verteilung erstellen und exportieren

Verwenden Sie diese Option, um den lokalen Zugriffs-Berechtigungsschlüssel zu exportieren und dann manuell über E-Mail oder eine andere Methode an die HP Sure Admin Telefon-App zu verteilen.

**HINWEIS:** Bei dieser Option ist kein Netzwerkzugriff für die HP Sure Admin Telefon-App erforderlich, um eine einmalige PIN zu erhalten.

1. Benennen Sie Ihren Schlüssel im Eingabefeld **Schlüsselname**.
2. Geben Sie die Passphrase in das Eingabefeld **Passphrase** ein.

   **HINWEIS:** Die Passphrase wird zum Schutz des exportierten Schlüssels verwendet und muss bereitgestellt werden, damit der Benutzer der HP Sure Admin Telefon-App den Schlüssel importieren kann.

3. Wählen Sie **Durchsuchen**, und wählen Sie den Pfad im System für den Export aus.
4. Wählen Sie **Schlüssel erstellen**. Ihr Schlüssel wurde erfolgreich erstellt, wenn neben der Schaltfläche **Schlüssel erstellen** ein Benachrichtigungssymbol mit der Meldung **Schlüssel erfolgreich erstellt** erscheint.
5. Wählen Sie **Weiter**. Auf der Übersichtsseite werden die von Ihnen eingegebenen HP Sure Admin Einstellungen angezeigt.
6. Wählen Sie **Richtlinie speichern**. Die Richtlinie wurde gespeichert, wenn die Meldung **Erfolgreich gespeichert** angezeigt wird.
7. Navigieren Sie zu dem Ordner, in dem Sie den Schlüssel gespeichert haben, und verteilen Sie ihn mithilfe einer Methode, die dem Benutzer der HP Sure Admin Telefon-App auf diesem Gerät zur Verfügung

steht, wie z. B. E-Mail. Der Benutzer benötigt auch die Passphrase, um den Schlüssel zu importieren. HP empfiehlt, unterschiedliche Verteilungsmechanismen für Schlüssel und Passphrase zu verwenden.

**HINWEIS:** Senden Sie den QR-Code in Originalgröße. Die App kann das Bild nicht korrekt lesen, wenn es kleiner als 800 × 600 ist.

## Einen Schlüssel mit Azure AD Revocation erstellen und exportieren

Verwenden Sie diese Option, um den lokalen Zugriffsschlüssel mit einer bestimmten Azure Active Directory-Gruppe zu verbinden, damit die HP Sure Admin Telefon-App sowohl die Benutzerauthentifizierung für Azure Active Directory verwenden als auch bestätigen muss, dass der Benutzer Mitglied der jeweiligen Gruppe ist, bevor eine lokale Zugriffs-PIN bereitgestellt wird. Auch bei dieser Methode ist die manuelle Verteilung des lokalen Zugriffsschlüssels für die Autorisierung an die Telefon-App über E-Mail oder eine andere Methode erforderlich.

**HINWEIS:** Für diese Option muss die HP Sure Admin Telefon-App über Netzwerkzugriff verfügen, um eine einmalige PIN zu erhalten.

1. Benennen Sie Ihren Schlüssel im Eingabefeld **Schlüsselname**.
2. Geben Sie die Passphrase in das Eingabefeld **Passphrase** ein.

   **HINWEIS:** Die Passphrase wird zum Schutz des exportierten Schlüssels verwendet und muss bereitgestellt werden, damit der Benutzer der HP Sure Admin Telefon-App den Schlüssel importieren kann.

3. Klicken Sie auf **Azure AD Anmeldung**, um sich anzumelden.
4. Wählen Sie den Namen Ihrer Gruppe aus dem Dropdown-Menü **Azure AD Gruppenname** aus. Sie müssen ein Mitglied der Gruppe sein, um auf den Schlüssel zugreifen zu können.
5. Wählen Sie **Durchsuchen**, und wählen Sie den Pfad im System für den Export aus.
6. Wählen Sie **Schlüssel erstellen**. Ihr Schlüssel wurde erfolgreich erstellt, wenn neben der Schaltfläche **Schlüssel erstellen** die Meldung **Schlüssel erfolgreich erstellt** erscheint.
7. Wählen Sie **Weiter**. Auf der Übersichtsseite werden die von Ihnen eingegebenen HP Sure Admin Einstellungen angezeigt.
8. Wählen Sie **Richtlinie speichern**. Die Richtlinie wurde gespeichert, wenn die Meldung **Erfolgreich gespeichert** angezeigt wird.
9. Navigieren Sie zu dem Ordner, in dem Sie den Schlüssel gespeichert haben, und verteilen Sie ihn mithilfe einer Methode, die dem Benutzer der HP Sure Admin Telefon-App auf diesem Gerät zur Verfügung steht, wie z. B. E-Mail. Der Benutzer benötigt auch die Passphrase, um den Schlüssel zu importieren. HP empfiehlt, unterschiedliche Verteilungsmechanismen für Schlüssel und Passphrase zu verwenden.

**HINWEIS:** Senden Sie den QR-Code in Originalgröße. Die App kann das Bild nicht korrekt lesen, wenn es kleiner als 800 × 600 ist.

## Erstellen Sie einen Schlüssel und senden Sie ihn an Azure AD Group OneDrive:

(Empfohlen) Verwenden Sie diese Option, um zu verhindern, dass der lokale Zugriffs-Berechtigungsschlüssel auf dem Telefon gespeichert wird. Wenn Sie diese Option auswählen, speichert das MIK den lokalen Zugriffs-Berechtigungsschlüssel im angegebenen OneDrive-Ordner, der nur für die autorisierte Gruppe zugänglich ist.

Benutzer der HP Sure Admin Telefon-App müssen sich jedes Mal, wenn eine PIN erforderlich ist, bei Azure AD authentifizieren.

1. Benennen Sie Ihren Schlüssel im Eingabefeld **Schlüsselname**.
2. Geben Sie die Passphrase in das Eingabefeld **Passphrase** ein.
3. Klicken Sie auf **Azure AD Login** und melden Sie sich an.
4. Wählen Sie den Namen Ihrer Gruppe aus dem Dropdown-Menü Azure AD Gruppenname aus.

**HINWEIS:** Sie müssen ein Mitglied der Gruppe sein, um auf den Schlüssel zugreifen zu können.

5. Geben Sie den Namen des OneDrive-Ordners, in dem der Schlüssel gespeichert werden soll, im Eingabefeld **OneDrive** ein.
6. Wählen Sie **Durchsuchen**, und wählen Sie den Pfad im System für den Export aus.
7. Wählen Sie **Schlüssel erstellen**.

**HINWEIS:** Ihr Schlüssel wurde erfolgreich dem angegebenen OneDrive-Ordner hinzugefügt und in den angegebenen lokalen Ordner exportiert, wenn neben der Schaltfläche **Schlüssel erstellen** ein Benachrichtigungssymbol mit der Meldung **Schlüssel erfolgreich erstellt** angezeigt wird.

8. Wählen Sie **Weiter**. Auf der Übersichtsseite werden die von Ihnen eingegebenen HP Sure Admin Einstellungen angezeigt.
9. Wählen Sie **Richtlinie speichern**. Die Richtlinie wurde gespeichert, wenn die Meldung **Erfolgreich gespeichert** angezeigt wird.

**HINWEIS:** In diesem Szenario ist es nicht erforderlich, irgendetwas zur Vorabbereitstellung an die HP Sure Admin Telefon-App zu senden. Die Ziel-PCs verweisen auf den OneDrive-Speicherort, der im QR-Code enthalten ist. Die HP Sure Admin Telefon-App verwendet diesen Zeiger für den Zugriff auf den OneDrive-Speicherort, wenn der Benutzer Teil der autorisierten Gruppe ist und sich erfolgreich authentifiziert.

# 3 Telefoneinstellungen

Laden Sie die HP Sure Admin Telefon-App im Google Play-Store oder im Apple Store herunter.

- Laden Sie HP Sure Admin im Google Play-Store für Android-Mobiltelefone herunter.
- Laden Sie HP Sure Admin im Apple Store für iOS-Mobiltelefone herunter.

## Verwenden der HP Sure Admin Phone App zum Entsperren des BIOS

Die mobile HP Sure Admin App ersetzt die Verwendung des BIOS-Kennworts für den lokalen Zugriff auf das BIOS-Setup durch die Bereitstellung einer einmaligen PIN, die durch das Scannen des vom Zielcomputer vorgelegten QR-Codes bereitgestellt wird.

Führen Sie die folgenden Schritte aus, um den Schlüssel lokal auf dem Telefon zu speichern wenn der Schlüssel an den Benutzer der Telefon-App gesendet wird. Im folgenden Beispiel wird der Schlüssel an den Benutzer der HP Sure Admin Telefon-App weitergeleitet, und der Benutzer öffnet die E-Mail auf dem Telefon.

1. Öffnen Sie die E-Mail, die den Schlüssel enthält.
2. Wenn die Seite **Registrierung** angezeigt wird, geben Sie die Passphrase in das Eingabefeld **Passphrase eingeben** und Ihre E-Mail-Adresse in das Feld **Geben Sie Ihre E-Mail-Adresse** ein, um den Schlüssel zu entschlüsseln und HP Sure Admin hinzuzufügen. Die PIN-Nummer zum Entsperren wird auf der Seite **Your PIN** (Ihre PIN) angezeigt.

   **HINWEIS:** Mit diesem Schritt wird der Schlüssel im mobilen Gerät gespeichert und die Registrierung abgeschlossen. An dieser Stelle können Sie mit der HP Sure Admin Telefon-App auf ein beliebiges Gerät zugreifen, das für den Zugriff über diesen Schlüssel bereitgestellt wurde. Eine E-Mail-Adresse ist nur erforderlich, wenn der Administrator diese benötigt.

3. Geben Sie die PIN in das Feld **BIOS Enter Response Code** (BIOS Antwortcode eingeben) ein.

### Zugriff auf das BIOS-Setup nach der Registrierung erhalten

So erhalten Sie nach der Registrierung Zugriff auf das BIOS-Setup auf einem Zielcomputer:

1. Geben Sie das BIOS-Setup beim Systemstart auf dem Zielcomputer ein.
2. Wählen Sie **QR-Code scannen** in der Telefonanwendung, und scannen Sie den QR-Code auf dem Zielcomputer.
3. Wenn Sie zur Benutzerauthentifizierung aufgefordert werden, geben Sie Ihre Anmeldeinformationen ein.
4. Die entsperrte PIN-Nummer wird auf der Seite **Your PIN** (Ihre PIN) angezeigt.
5. Geben Sie die PIN in das BIOS-Eingabefeld **Enter Response Code** (Antwortcode eingeben) auf dem Zielcomputer ein.

### Entsperren des BIOS mit Azure AD Group OneDrive

So verwenden Sie HP Sure Admin, um das BIOS mit Azure AD Group OneDrive zu entsperren:

1. Wählen Sie **QR-Code scannen**, und scannen Sie dann den QR-Code des BIOS.

**HINWEIS:** Die HP Sure Admin Telefon-App zeigt die Azure AD-Anmeldeseite an.

2. Melden Sie sich bei Ihrem Azure-Konto an.

3. Geben Sie die PIN in das Feld **BIOS Enter Response Code** (BIOS Antwortcode eingeben) ein.

**HINWEIS:** Die HP Sure Admin Telefon-App speichert den Schlüssel in diesem Szenario nicht lokal. Die HP Sure Telefon-App muss über Netzwerkzugriff verfügen, und der Benutzer muss sich jedes Mal authentifizieren, wenn eine einmalige PIN erforderlich ist.

# 4 HP Sure Admin-Fehlercodes

Verwenden Sie die Tabelle in diesem Abschnitt, um die Fehlercodes, Typen und Beschreibungen der HP Sure Admin- und KMS Admin-Konsole aufzurufen.

**Tabelle 4-1 Fehlercodes, Typen und Beschreibungen der HP Sure Admin-App**

| Fehlercode | Fehlertyp | Beschreibung |
|---|---|---|
| 100 | QRCodeUnknownError | Allgemeiner Fehler. |
| 101 | QRCodeDeserialization | QR-Code JSON kann nicht gelesen werden. Entweder ist die Zeichenfolge in keiner gültigen JSON-Datei oder die Daten sind ungültig. |
| 102 | QRCodeInvalidImage | Das gescannte QR-Code-Bild ist ungültig. QR-Code-Bilddatei kann nicht gelesen werden. |
| 103 | QRCodeNoPayload | Das gescannte QR-Code-Bild ist ungültig. Die Bilddatei hat keine JSON-Nutzlast. |
| 104 | QRCodeInvalid | Die JSON-Daten des QR-Codes können nicht gelesen werden. Entweder ist die Zeichenfolge kein gültiges JSON oder die Daten im QR-Bild sind ungültig. |
| 105 | QRCodeInvalidKeyIdHash | Der Hash des öffentlichen Schlüssels in der JSON des QR-Codes stimmt nicht mit dem Hash des öffentlichen Schlüssels (KeyID-Daten) des Registrierungspakets überein. |
| 106 | QRCodeTampered | Das gescannte QR-Code-Bild wurde manipuliert und ist ungültig. |
| 107 | QRCodeTamperedOrInvalidPassPhrase | Das gescannte QR-Code-Bild wurde manipuliert und ist ungültig, oder das eingegebene Passwort ist falsch. |

**Tabelle 4-2 OneTime-Zugriffsschlüssel über OneDrive Fehler, Typen und deren Beschreibungen**

| Fehlercode | Fehlertyp | Beschreibung |
|---|---|---|
| 200 | OneTimeKeyError | Allgemeiner Fehler. |
| 201 | OneTimeKeyNoUserGroups | Der angemeldete Benutzer gehört keiner AD-Gruppe in Ihrem Unternehmen an. |
| 203 | OneTimeKeyInvalidUserGroup | Der angemeldete Benutzer gehört nicht zu der zugewiesenen AD Gruppe für diesen Schlüssel. |
| 204 | OneTimeKeyQRFileDoesNotExist | Die OneTime-Schlüsseldatei ist im OneDrive-Ordner der AD-Gruppe nicht vorhanden. |
| 205 | OneTimeKeyInvalidQRFile | Die OneTime-Schlüsseldatei im OneDrive-Ordner der AD-Gruppe ist ungültig. |

**Tabelle 4-2 OneTime-Zugriffsschlüssel über OneDrive Fehler, Typen und deren Beschreibungen (Fortsetzung)**

| Fehlercode | Fehlertyp | Beschreibung |
|---|---|---|
| 206 | OneTimeKeyInvalidQRpayload | Die OneTime-Schlüsseldatei ist vorhanden, kann aber keine Datei-Inhalte lesen. |

**Tabelle 4-3 Azure AD Autorisierungsfehler**

| Fehlercode | Fehlertyp | Beschreibung |
|---|---|---|
| 300 | AzureADUnknownError | Allgemeiner Fehler. |
| 301 | AzureADInvalidDomain | Die eingegebene E-Mail-Adresse stimmt nicht mit dem Domänennamen im QR-Code-Bild überein. |
| 302 | AzureADAccessToken | Fehler beim Abrufen von Zugriffstoken aus Azure AD. Entweder kann sich der Benutzer nicht beim Azure AD Ihres Unternehmens anmelden oder die App verfügt nicht über die erforderlichen Berechtigungen, um eine Verbindung mit dem Azure AD Ihres Unternehmens herzustellen. Möglicherweise wurde die Authentifizierung durch den Benutzer abgebrochen. |
| 303 | AzureADUserProfile | Die HP Sure Admin-App kann jetzt Benutzerprofilinformationen aus dem Azure AD Ihres Unternehmens abrufen. |
| 304 | AzureADUserPrincipalMismatch | Die eingegebene E-Mail-Adresse stimmt nicht mit dem Hauptnamen des angemeldeten Benutzers überein. |
| 305 | AzureADUserInvalidUserGroup | Der angemeldete Benutzer gehört nicht zu der zugewiesenen Azure AD Gruppe dieses Schlüssels. |

**Tabelle 4-4 Kms Admin Console-Fehler, Typen und deren Beschreibungen**

| Fehlercode | Fehlertyp | Beschreibung |
|---|---|---|
| 401 | KmsUnauthorized | Der Nutzer ist nicht berechtigt, den KMS Service zu nutzen. |
| 402 | KmsKeyDoesNotExist | Ein passender privater Schlüssel existiert nicht im KMS-Schlüsselspeicher. Der Schlüssel ist derzeit gelöscht, kann aber wiederhergestellt werden. Die Bezeichnung des Schlüssels kann in diesem Zustand nicht wiederverwendet werden. Der Schlüssel kann nur wiederhergestellt oder gelöscht werden. |
| 403 | KmsKeyDoesNotExistInTableStorage | Schlüssel ist im Tabellenspeicher nicht vorhanden. |
| 404 | KmsUploadKeyErrorInKeyVault | Fehler beim Hinzufügen eines Schlüssels zum Schlüsselspeicher. |
| 405 | KmsUploadKeyUnauthorized | Der Benutzer ist nicht berechtigt, Schlüssel hochzuladen. Der Nutzer gehört nicht zur |

**Tabelle 4-4 Kms Admin Console-Fehler, Typen und deren Beschreibungen (Fortsetzung)**

| Fehlercode | Fehlertyp | Beschreibung |
|---|---|---|
| | | autorisierten AD Group, die diese API aufrufen darf. |
| 406 | KmsInvalidAzureADLogin | Benutzer ist nicht in Azure Tenant AAD angemeldet. |
| 407 | KmsNoUserGroups | Der angemeldete Benutzer gehört keiner AD-Gruppe in Ihrem Unternehmen an. |
| 408 | KmsInvalidUserGroup | Der angemeldete Benutzer gehört nicht zu der zugewiesenen AD Gruppe für diesen Schlüssel. |
| 409 | KmsInvalidAccessToken | Das in der Anforderung bereitgestellte Zugriffstoken ist ungültig. |
| 410 | KmsAccessTokenExpired | Die bereitgestellte AccessToken-Liste ist abgelaufen. |
| 411 | KmsAccessTokenInvalidTenantId | Der bereitgestellte accessToken weist einen ungültigen TenantId-Wert auf. |
| 412 | KmsAccessTokenTenantIdMismatch | Die TenantId im bereitgestellten AccessToken entspricht nicht der Funktions-App TenantId. |
| 413 | KmsInvalidKeyId | Die keyId ist null oder leer. |
| 414 | KmsDeleteKeyUnauthorized | Der Benutzer ist nicht zum Löschen von Schlüsseln berechtigt. Der Nutzer gehört nicht zur autorisierten AD Group, die diese API aufrufen darf. |
| 415 | KmsKeyVaultSoftDeleteUnrecoverableState | Der geheime Schlüssel konnte nicht wiederhergestellt werden. Der Benutzer sollte es erneut versuchen. |
| 416 | KmsInvalidGetKeysRequest | Die Get Keys-Anforderung ist ungültig. |
| 417 | KmsGetKeysUnauthorized | Der Benutzer ist nicht zum Abrufen von Schlüsseln berechtigt. Der Nutzer gehört nicht zur autorisierten AD Group, die diese API aufrufen darf. |
| 418 | KmsInvalidRequestPayload | Die von der API empfangene Anforderung ist ungültig. |
| 419 | KmsRequestRequired | Die erhaltene Anforderung darf nicht leer sein. |
| 420 | KmsKeyNotConcurrent | Der Schlüssel im Tabellenspeicher wurde aktualisiert oder geändert, seit der Benutzer zuletzt eine Kopie abgerufen hat. |