



Οδηγός χρήσης για το HP Sure Admin

ΣΥΝΟΨΗ

Το HP Sure Admin δίνει τη δυνατότητα στους διαχειριστές IT να διαχειρίζονται με ασφάλεια τις ευαίσθητες ρυθμίσεις υλικολογισμικού των συσκευών χρησιμοποιώντας πιστοποιητικά και κρυπτογραφία δημόσιου κλειδιού για την απομακρυσμένη και την τοπική διαχείριση των ρυθμίσεων αντί για κωδικό πρόσβασης.

Νομικές πληροφορίες

© Copyright 2019, 2021 HP Development Company, L.P.

Η ονομασία Apple είναι εμπορικό σήμα της Apple Computer, Inc., κατατεθέν στις ΗΠΑ και σε άλλες χώρες/περιοχές.

Η ονομασία Google Play είναι εμπορικό σήμα της Google LLC.

Εμπιστευτικό λογισμικό υπολογιστή.
Απαιτείται έγκυρη άδεια από την HP για την κατοχή, χρήση ή αντιγραφή. Σύμφωνα με τους αμερικανικούς ομοσπονδιακούς κανονισμούς FAR 12.211 και 12.212, η άδεια για το λογισμικό εμπορικών υπολογιστών, την τεκμηρίωση λογισμικού υπολογιστών και τα τεχνικά δεδομένα εμπορικών ειδών εκχωρείται στην κυβέρνηση των ΗΠΑ στα πλαίσια της τυπικής εμπορικής άδειας χρήσης της HP.

Οι πληροφορίες που περιέχονται στο παρόν υπόκεινται σε αλλαγές χωρίς προειδοποίηση. Οι μοναδικές εγγυήσεις για τα προϊόντα και τις υπηρεσίες της HP είναι αυτές που ορίζονται στις ρητές δηλώσεις εγγύησης που συνοδεύουν αυτά τα προϊόντα και τις υπηρεσίες. Τίποτα από όσα αναφέρονται στο παρόν δεν πρέπει να ερμηνευτεί ως πρόσθετη εγγύηση. Η HP δεν φέρει ευθύνη για τεχνικά ή συντακτικά σφάλματα ή παραλείψεις του παρόντος.

Δεύτερη έκδοση: Οκτώβριος 2021

Πρώτη έκδοση: Δεκέμβριος 2019

Αριθμός εγγράφου: L83995-152

Πίνακας περιεχομένων

1 Έναρξη χρήσης.....	1
Χρήση του HP Sure Admin	1
Απενεργοποίηση του HP Sure Admin	1
2 Δημιουργία και διαχείριση κλειδιών	2
Δημιουργία και εξαγωγή κλειδιών.....	2
Δημιουργία και εξαγωγή κλειδιού με μη αυτόματη διανομή	2
Δημιουργία και εξαγωγή κλειδιού με ανάκληση Azure AD	3
Δημιουργήστε και να στείλετε ένα κλειδί στο OneDrive της ομάδας του Azure AD:.....	3
3 Ρύθμιση τηλεφώνου.....	5
Χρήση της εφαρμογής τηλεφώνου HP Sure Admin για ξεκλείδωμα του BIOS	5
Απόκτηση πρόσβασης στο πρόγραμμα ρύθμισης του BIOS μετά την εγγραφή	5
Ξεκλείδωμα του BIOS με Το OneDrive της ομάδας AD	6
4 Κωδικοί ασφαλισμάτων HP Sure Admin.....	7

1 Έναρξη χρήσης

Το HP Sure Admin δίνει τη δυνατότητα στους διαχειριστές IT να διαχειρίζονται με ασφάλεια τις ευαίσθητες ρυθμίσεις υλικολογισμικού των συσκευών χρησιμοποιώντας πιστοποιητικά και κρυπτογραφία δημόσιου κλειδιού για την απομακρυσμένη και την τοπική διαχείριση των ρυθμίσεων αντί για κωδικό πρόσβασης.

Το HP Sure Admin αποτελείται από τα παρακάτω μέρη:

- **Υπολογιστής προορισμού:** Οι πλατφόρμες προς διαχείριση που υποστηρίζουν τη λειτουργία ελέγχου ταυτότητας Enhanced BIOS.
- **HP Manageability Integration Kit (MIK):** Η προσθήκη για το System Center Configuration Manager (SCCM) ή το HP BIOS Configuration Utility (BCU) για απομακρυσμένη διαχείριση των ρυθμίσεων του BIOS.
- **HP Sure Admin Local Access Authenticator:** Μια εφαρμογή τηλεφώνου που αντικαθιστά τον κωδικό πρόσβασης για να επιτρέψει την τοπική πρόσβαση στο πρόγραμμα ρύθμισης του BIOS με σάρωση ενός κωδικού QR για λήψη ενός PIN μίας χρήσης.

Χρήση του HP Sure Admin


Η παρούσα ενότητα περιγράφει τη διαδικασία χρήσης του HP Sure Admin.

1. Ανοίξτε την προσθήκη HP Sure Admin από την προσθήκη HP Manageability Integration Kit (MIK) για το System Center Configuration Manager (SCCM) ή το Enhanced BIOS Configuration Utility (BCU).
2. Κάντε λήψη της εφαρμογής τηλεφώνου HP Sure Admin είτε από το Google Play™ Store είτε από το Apple App Store®.
3. Δημιουργήστε ένα ζεύγος κλειδιών που θα χρησιμοποιείται από τη συσκευή προορισμού και την εφαρμογή τηλεφώνου HP Sure Admin για τη λήψη του PIN μίας χρήσης για το ξεκλείδωμα του BIOS.


Απενεργοποίηση του HP Sure Admin

Η παρούσα ενότητα περιγράφει τις επιλογές για την απενεργοποίηση του HP Sure Admin.

- Στη ρύθμιση F10 του BIOS, επιλέξτε **Restore Security settings to Factory Defaults** (Επαναφορά ρυθμίσεων ασφαλείας στις εργοστασιακές προεπιλογές).

 **ΣΗΜΕΙΩΣΗ:** Αυτό απαιτεί φυσική παρουσία με την παροχή ενός PIN ελέγχου ταυτότητας μέσω της εφαρμογής τηλεφώνου HP Sure Admin για πρόσβαση στις ρυθμίσεις F10.

- Χρησιμοποιήστε την εντολή του BCU για την απομακρυσμένη κλήση του WMI της επιλογής **Restore Security settings to Factory Defaults** (Επαναφορά ρυθμίσεων ασφαλείας στις εργοστασιακές προεπιλογές).

 **ΣΗΜΕΙΩΣΗ:** Για περισσότερες πληροφορίες, ανατρέξτε στον Οδηγό χρήσης του HP BIOS Configuration Utility (BCU).

- Στη σελίδα Security Provisioning (Παροχή ασφαλείας) του MIK, επιλέξτε **Deprovision** (Κατάργηση παροχής).

2 Δημιουργία και διαχείριση κλειδιών

Ολοκληρώστε την παροχή ασφάλειας από το MIK πριν ενεργοποιήσετε τη λειτουργία ελέγχου ταυτότητας Enhanced BIOS. Η λειτουργία ελέγχου ταυτότητας Enhanced BIOS πρέπει να είναι ενεργοποιημένη για τη δημιουργία και την εξαγωγή κλειδιών. Για να ενεργοποιήσετε τη λειτουργία ελέγχου ταυτότητας BIOS:

- ▲ Ανοίξτε την προσθήκη HP Sure Admin και επιλέξτε **Enhanced BIOS Authentication Mode** (Λειτουργία ελέγχου ταυτότητας Enhanced BIOS) για να δημιουργήσετε και να εξαγάγετε κλειδιά.


Δημιουργία και εξαγωγή κλειδιών

Υπάρχουν 3 διαφορετικοί τρόποι να δημιουργήσετε ζεύγη κλειδιών τοπικής πρόσβασης και να δώσετε στην εφαρμογή τηλεφώνου HP Sure Admin τη δυνατότητα πρόσβασης στο κλειδί.


- [Δημιουργία και εξαγωγή κλειδιού με μη αυτόματη διανομή στη σελίδα 2](#)
- [Δημιουργία και εξαγωγή κλειδιού με ανάκληση Azure AD στη σελίδα 3](#)
- [Δημιουργήστε και να στείλετε ένα κλειδί στο OneDrive της ομάδας του Azure AD: στη σελίδα 3](#)

Δημιουργία και εξαγωγή κλειδιού με μη αυτόματη διανομή

Χρησιμοποιήστε αυτή την επιλογή για να εξαγάγετε το κλειδί εξουσιοδότησης τοπικής πρόσβασης και, στη συνέχεια, να το διανείμετε με μη αυτόματο τρόπο στην εφαρμογή τηλεφώνου HP Sure Admin μέσω email ή άλλης μεθόδου.


 **ΣΗΜΕΙΩΣΗ:** Με την επιλογή αυτή δεν απαιτείται η πρόσβαση στο δίκτυο της εφαρμογής τηλεφώνου HP Sure Admin για τη λήψη ενός PIN μίας χρήσης.

1. Ονομάστε το κλειδί σας στο πλαίσιο **Key Name** (Όνομα κλειδιού).
2. Εισαγάγετε τη φράση πρόσβασης στο πλαίσιο **Passphrase** (Φράση πρόσβασης).

 **ΣΗΜΕΙΩΣΗ:** Η φράση πρόσβασης χρησιμοποιείται για την προστασία του εξαγόμενου κλειδιού και πρέπει να παρέχεται έτσι ώστε ο χρήστης της εφαρμογής τηλεφώνου HP Sure Admin να μπορεί να εισαγάγει το κλειδί.


3. Επιλέξτε **Browse** (Αναζήτηση) και επιλέξτε πού θα γίνει εξαγωγή στο σύστημα.
4. Επιλέξτε **Create Key** (Δημιουργία κλειδιού). Το κλειδί σας έχει δημιουργηθεί επιτυχώς όταν εμφανιστεί ένα εικονίδιο ειδοποίησης δίπλα στο κουμπί **Create Key** (Δημιουργία κλειδιού) με το μήνυμα **Key successfully created** (Το κλειδί δημιουργήθηκε επιτυχώς).
5. Επιλέξτε **Next** (Επόμενο). Η σελίδα σύνοψης εμφανίζει τις ρυθμίσεις του HP Sure Admin που εισαγάγατε.
6. Επιλέξτε **Save Policy** (Αποθήκευση πολιτικής). Η πολιτική έχει αποθηκευτεί όταν εμφανιστεί το μήνυμα **Saved successfully** (Αποθηκεύτηκε επιτυχώς).
7. Μεταβείτε στον φάκελο όπου αποθηκεύσατε το κλειδί και διανείμετέ το στον χρήστη της εφαρμογής τηλεφώνου HP Sure Admin χρησιμοποιώντας μια μέθοδο που είναι διαθέσιμη σε αυτόν τον χρήστη στη συγκεκριμένη συσκευή, όπως email. Ο χρήστης αυτός θα χρειαστεί επίσης τη φράση πρόσβασης για την

εισαγωγή του κλειδιού. Η HP συνιστά να χρησιμοποιείτε διαφορετικούς μηχανισμούς διανομής για το κλειδί και τη φράση πρόσβασης.


 **ΣΗΜΕΙΩΣΗ:** Κατά την αποστολή του κωδικού QR, στείλτε τον στο αρχικό του μέγεθος. Η εφαρμογή δεν μπορεί να διαβάσει σωστά την εικόνα αν έχει μέγεθος μικρότερο από 800 × 600.

Δημιουργία και εξαγωγή κλειδιού με ανάκληση Azure AD


Χρησιμοποιήστε αυτή την επιλογή για να συνδέσετε το κλειδί τοπικής πρόσβασης σε μια καθορισμένη ομάδα του Azure Active Directory και να ρυθμίσετε την εφαρμογή τηλεφώνου HP Sure Admin να απαιτεί έλεγχο ταυτότητας χρήστη στο Azure Active Directory και να επιβεβαιώνει ότι ο χρήστης είναι μέλος της καθορισμένης ομάδας πριν από την παροχή ενός PIN τοπικής πρόσβασης. Αυτή η μέθοδος απαιτεί επίσης τη μη αυτόματη διανομή του κλειδιού εξουσιοδότησης τοπικής πρόσβασης στην εφαρμογή τηλεφώνου μέσω email ή άλλης μεθόδου.

 **ΣΗΜΕΙΩΣΗ:** Με την επιλογή αυτή απαιτείται από την εφαρμογή τηλεφώνου HP Sure Admin να έχει πρόσβαση στο δίκτυο για τη λήψη ενός PIN μίας χρήσης.

1. Ονομάστε το κλειδί σας στο πλαίσιο **Key Name** (Όνομα κλειδιού).
2. Εισαγάγετε τη φράση πρόσβασης στο πλαίσιο **Passphrase** (Φράση πρόσβασης).

 **ΣΗΜΕΙΩΣΗ:** Η φράση πρόσβασης χρησιμοποιείται για την προστασία του εξαγόμενου κλειδιού και πρέπει να παρέχεται έτσι ώστε ο χρήστης της εφαρμογής τηλεφώνου HP Sure Admin να μπορεί να εισαγάγει το κλειδί.

3. Επιλέξτε **Azure AD Login** (Σύνδεση στο Azure AD) και συνδεθείτε.
4. Επιλέξτε το όνομα της ομάδας σας από το αναπτυσσόμενο πλαίσιο **Azure AD Group Name** (Όνομα ομάδας Azure AD). Πρέπει να είστε μέλος της ομάδας για να έχετε πρόσβαση στο κλειδί.
5. Επιλέξτε **Browse** (Αναζήτηση) και επιλέξτε πού θα γίνει εξαγωγή στο σύστημα.
6. Επιλέξτε **Create Key** (Δημιουργία κλειδιού). Το κλειδί σας δημιουργείται επιτυχώς όταν εμφανιστεί ένα εικονίδιο ειδοποίησης δίπλα στο κουμπί **Create Key** (Δημιουργία κλειδιού) με το μήνυμα **Key successfully created** (Το κλειδί δημιουργήθηκε επιτυχώς).
7. Επιλέξτε **Next** (Επόμενο). Η σελίδα σύνοψης εμφανίζει τις ρυθμίσεις του HP Sure Admin που εισαγάγατε.
8. Επιλέξτε **Save Policy** (Αποθήκευση πολιτικής). Η πολιτική έχει αποθηκευτεί όταν εμφανιστεί το μήνυμα **Saved successfully** (Αποθηκεύτηκε επιτυχώς).
9. Μεταβείτε στον φάκελο όπου αποθηκεύσατε το κλειδί και διανείμετέ το στον χρήστη της εφαρμογής τηλεφώνου HP Sure Admin χρησιμοποιώντας μια μέθοδο που είναι διαθέσιμη σε αυτόν τον χρήστη στη συγκεκριμένη συσκευή, όπως email. Ο χρήστης αυτός θα χρειαστεί επίσης τη φράση πρόσβασης για την εισαγωγή του κλειδιού. Η HP συνιστά να χρησιμοποιείτε διαφορετικούς μηχανισμούς διανομής για το κλειδί και τη φράση πρόσβασης.

 **ΣΗΜΕΙΩΣΗ:** Κατά την αποστολή του κωδικού QR, στείλτε τον στο αρχικό του μέγεθος. Η εφαρμογή δεν μπορεί να διαβάσει σωστά την εικόνα αν έχει μέγεθος μικρότερο από 800 × 600.

Δημιουργήστε και να στείλετε ένα κλειδί στο OneDrive της ομάδας του Azure AD:

(συνιστάται) Χρησιμοποιήστε αυτή την επιλογή για να αποφύγετε την αποθήκευση του κλειδιού εξουσιοδότησης τοπικής πρόσβασης στο τηλέφωνο. Όταν χρησιμοποιείτε αυτή την επιλογή, το MIM αποθηκεύει το κλειδί εξουσιοδότησης τοπικής πρόσβασης στον καθορισμένο φάκελο OneDrive που είναι

προσβάσιμος μόνο από την εξουσιοδοτημένη ομάδα. Ο χρήστης της εφαρμογής τηλεφώνου HP Sure Admin θα πρέπει να υποβάλλεται σε έλεγχο ταυτότητας στο Azure AD κάθε φορά που απαιτείται PIN.

1. Ονομάστε το κλειδί σας στο πλαίσιο **Key Name** (Όνομα κλειδιού).
2. Εισαγάγετε τη φράση πρόσβασης στο πλαίσιο **Passphrase** (Φράση πρόσβασης).
3. Επιλέξτε **Azure AD Login** (Σύνδεση στο Azure AD) και συνδεθείτε.
4. Επιλέξτε το όνομα της ομάδας σας από το αναπτυσσόμενο πλαίσιο **Azure AD Group Name** (Όνομα ομάδας Azure AD).



ΣΗΜΕΙΩΣΗ: Πρέπει να είστε μέλος της ομάδας για να έχετε πρόσβαση στο κλειδί.

5. Εισαγάγετε το όνομα του φακέλου OneDrive όπου θέλετε να αποθηκευτεί το κλειδί στο πλαίσιο **OneDrive**.
6. Επιλέξτε **Browse** (Αναζήτηση) και επιλέξτε πού θα γίνει εξαγωγή στο σύστημα.
7. Επιλέξτε **Create Key** (Δημιουργία κλειδιού).



ΣΗΜΕΙΩΣΗ: Το κλειδί σας έχει προστεθεί επιτυχώς στον καθορισμένο φάκελο OneDrive και έχει εξαχθεί στον καθορισμένο τοπικό φάκελο όταν εμφανιστεί ένα εικονίδιο ειδοποίησης δίπλα στο κουμπί **Create Key** (Δημιουργία κλειδιού) με το μήνυμα **Key successfully created** (Το κλειδί δημιουργήθηκε επιτυχώς).

8. Επιλέξτε **Next** (Επόμενο). Η σελίδα σύνοψης εμφανίζει τις ρυθμίσεις του HP Sure Admin που εισαγάγατε.
9. Επιλέξτε **Save Policy** (Αποθήκευση πολιτικής). Η πολιτική έχει αποθηκευτεί όταν εμφανιστεί το μήνυμα **Saved successfully** (Αποθηκεύτηκε επιτυχώς).



ΣΗΜΕΙΩΣΗ: Σε αυτό το σενάριο, δεν χρειάζεται να σταλεί κάτι στην εφαρμογή τηλεφώνου HP Sure Admin για να προετοιμαστεί από πριν. Οι υπολογιστές προορισμού προετοιμάζονται ώστε να παραπέμπουν στη θέση του OneDrive που περιλαμβάνεται στον κωδικό QR. Η εφαρμογή τηλεφώνου HP Sure Admin χρησιμοποιεί αυτόν τον δείκτη για να αποκτήσει πρόσβαση στη θέση του OneDrive, εάν ο χρήστης ανήκει στην εξουσιοδοτημένη ομάδα και πραγματοποιήσει επιτυχή έλεγχο ταυτότητας.

3 Ρύθμιση τηλεφώνου

Κάντε λήψη της εφαρμογής τηλεφώνου HP Sure Admin είτε από το Google Play είτε από το Apple Store.

- Κάντε λήψη του HP Sure Admin από το Google Store για τηλέφωνα Android.
- Κάντε λήψη του HP Sure Admin από το Apple Store για τηλέφωνα iOS.

Χρήση της εφαρμογής τηλεφώνου HP Sure Admin για ξεκλείδωμα του BIOS

Η εφαρμογή κινητού τηλεφώνου HP Sure Admin αντικαθιστά τη χρήση του κωδικού πρόσβασης BIOS για τοπική πρόσβαση στο πρόγραμμα ρύθμισης του BIOS παρέχοντας ένα PIN μίας χρήσης που λαμβάνεται με τη σάρωση του κωδικού QR που εμφανίζει ο υπολογιστής προορισμού.

Χρησιμοποιήστε τα παρακάτω βήματα για να αποθηκεύσετε το κλειδί τοπικά στο τηλέφωνο σε ένα σενάριο όπου το κλειδί αποστέλλεται στο χρήστη της εφαρμογής τηλεφώνου. Στο παράδειγμα που ακολουθεί, το κλειδί αποστέλλεται μέσω email στον χρήστη της εφαρμογής τηλεφώνου HP Sure Admin και ο χρήστης ανοίγει το email στο τηλέφωνο.

1. Ανοίξτε το email που περιέχει το κλειδί.
2. Όταν εμφανιστεί η σελίδα **Enrollment** (Εγγραφή), εισαγάγετε τη φράση πρόσβασης στο πλαίσιο **Enter passphrase** (Εισαγάγετε τη φράση πρόσβασης) και τη διεύθυνση email σας στο πλαίσιο **Enter your email address** (Εισαγάγετε τη διεύθυνση email σας) για να αποκρυπτογραφήσετε το κλειδί και να το προσθέσετε στην εφαρμογή HP Sure Admin. Ο αριθμός PIN ξεκλειδώματος εμφανίζεται στη σελίδα **Your PIN** (Το PIN σας).



ΣΗΜΕΙΩΣΗ: Σε αυτό το βήμα αποθηκεύεται το κλειδί στη φορητή συσκευή και ολοκληρώνεται η εγγραφή. Σε αυτό το στάδιο, μπορείτε να χρησιμοποιήσετε την εφαρμογή τηλεφώνου HP Sure Admin για να αποκτήσετε πρόσβαση σε οποιαδήποτε συσκευή που έχει προετοιμαστεί ώστε να είναι προσβάσιμη μέσω αυτού του κλειδιού. Η διεύθυνση email απαιτείται μόνο εάν το απαιτεί ο διαχειριστής.

3. Εισαγάγετε το PIN στο πλαίσιο **BIOS Enter Response Code** (Εισαγάγετε κωδικό απόκρισης του BIOS).

Απόκτηση πρόσβασης στο πρόγραμμα ρύθμισης του BIOS μετά την εγγραφή

Για να αποκτήσετε πρόσβαση στο πρόγραμμα ρύθμισης του BIOS σε έναν υπολογιστή προορισμού μετά την εγγραφή:

1. Εισέλθετε στο πρόγραμμα ρύθμισης του BIOS κατά την εκκίνηση του υπολογιστή προορισμού.
2. Επιλέξτε **Scan QR Code** (Σάρωση κωδικού QR) στην εφαρμογή τηλεφώνου και σαρώστε τον κωδικό QR στον υπολογιστή προορισμού.
3. Εάν σας ζητηθεί έλεγχος ταυτότητας χρήστη, δώστε τα διαπιστευτήριά σας.
4. Ο αριθμός PIN ξεκλειδώματος εμφανίζεται στη σελίδα **Your PIN** (Το PIN σας).
5. Εισαγάγετε το PIN στο πλαίσιο **Enter Response Code** (Εισαγάγετε κωδικό απόκρισης) του BIOS στον υπολογιστή προορισμού.

Ξεκλείδωμα του BIOS με Το OneDrive της ομάδας AD

Για να χρησιμοποιήσετε το HP Sure Admin για να ξεκλειδώσετε το BIOS με το OneDrive της ομάδας του Azure AD:

1. Επιλέξτε **Scan QR Code** (Σάρωση κωδικού QR) και στη συνέχεια σαρώστε τον κωδικό QR του BIOS.



ΣΗΜΕΙΩΣΗ: Η εφαρμογή HP Sure Admin εμφανίζει τη σελίδα σύνδεσης στο Azure AD.

2. Συνδεθείτε στον λογαριασμό Azure σας.
3. Εισαγάγετε το PIN στο πλαίσιο **BIOS Enter Response Code** (Εισαγάγετε κωδικό απόκρισης του BIOS).



ΣΗΜΕΙΩΣΗ: Η εφαρμογή HP Sure Admin δεν αποθηκεύει το κλειδί τοπικά σε αυτό το σενάριο. Η εφαρμογή τηλεφώνου HP Sure Admin πρέπει να έχει πρόσβαση στο δίκτυο και ο χρήστης πρέπει να υποβάλλεται σε έλεγχο ταυτότητας κάθε φορά που απαιτείται PIN μίας χρήσης.

4 Κωδικοί σφαλμάτων HP Sure Admin

Χρησιμοποιήστε τον πίνακα σε αυτή την ενότητα για να δείτε τους κωδικούς σφαλμάτων τους τύπους και τις περιγραφές του HP Sure Admin και του KMS Admin Console.

Πίνακας 4-1 Κωδικοί σφαλμάτων, τύποι και οι περιγραφές των εφαρμογών HP Sure Admin

Κωδικός σφάλματος	Τύπος σφάλματος	Περιγραφή
100	QRCodeUnknownError	Γενικό σφάλμα.
101	QRCodeDeserialization	Δεν είναι δυνατή η ανάγνωση του QR Code JSON. Είτε η συμβολοσειρά δεν βρίσκεται σε έγκυρο αρχείο JSON είτε τα δεδομένα δεν είναι έγκυρα.
102	QRCodeInvalidImage	Η εικόνα του κωδικού QR που σαρώθηκε δεν είναι έγκυρη. Δεν είναι δυνατή η ανάγνωση του αρχείου εικόνας του κωδικού QR.
103	QRCodeNoPayload	Η εικόνα του κωδικού QR που σαρώθηκε δεν είναι έγκυρη. Το αρχείο εικόνας δεν έχει ωφέλιμο φορτίο JSON.
104	QRCodeInvalid	Δεν είναι δυνατή η ανάγνωση του JSON του κωδικού QR. Είτε η συμβολοσειρά δεν είναι έγκυρο JSON είτε τα δεδομένα στην εικόνα QR δεν είναι έγκυρα.
105	QRCodeInvalidKeyldHash	Ο κατακερματισμός δημόσιου κλειδιού στο JSON του κωδικού QR δεν συμφωνεί με τον κατακερματισμό δημόσιου κλειδιού του πακέτου εγγραφής (δεδομένα KeyID).
106	QRCodeTampered	Η εικόνα του κωδικού QR που σαρώθηκε είναι αλλοιωμένη και μη έγκυρη.
107	QRCodeTamperedOrInvalidPassPhrase	Η εικόνα QR Code που σαρώθηκε είναι αλλοιωμένη και μη έγκυρη ή η φράση πρόσβασης που έχει εισαχθεί είναι λανθασμένη.

Πίνακας 4-2 Κλειδί πρόσβασης μίας χρήσης από σφάλματα, τύπους και περιγραφές OneDrive

Κωδικός σφάλματος	Τύπος σφάλματος	Περιγραφή
200	OneTimeKeyError	Γενικό σφάλμα.
201	OneTimeKeyNoUserGroups	Ο συνδεδεμένος χρήστης δεν ανήκει σε καμία ομάδα του AD του οργανισμού σας.
203	OneTimeKeyInvalidUserGroup	Ο συνδεδεμένος χρήστης δεν ανήκει στην εκχωρημένη ομάδα AD στην οποία έχει εκχωρηθεί αυτό το κλειδί.
204	OneTimeKeyQRFileDoesNotExist	Το αρχείο κλειδιού μίας χρήσης δεν υπάρχει στον φάκελο OneDrive της ομάδας του AD.

Πίνακας 4-2 Κλειδί πρόσβασης μίας χρήσης από σφάλματα, τύπους και περιγραφές OneDrive (συνέχεια)

Κωδικός σφάλματος	Τύπος σφάλματος	Περιγραφή
205	OneTimeKeyInvalidQRFile	Το αρχείο κλειδιού μίας χρήσης στον φάκελο OneDrive της ομάδας του AD δεν είναι έγκυρο.
206	OneTimeKeyInvalidQRpayload	Το αρχείο κλειδιού μίας χρήσης υπάρχει, αλλά δεν μπορεί να διαβάσει το ωφέλιμο φορτίο του αρχείου.

Πίνακας 4-3 Σφάλματα εξουσιοδότησης Azure AD

Κωδικός σφάλματος	Τύπος σφάλματος	Περιγραφή
300	AzureADUnknownError	Γενικό σφάλμα.
301	AzureADInvalidDomain	Η διεύθυνση email που έχει εισαχθεί δεν συμφωνεί με το όνομα τομέα που καθορίζεται στην εικόνα του κωδικού QR.
302	AzureADAccessToken	Σφάλμα κατά τη λήψη διακριτικού πρόσβασης από το Azure AD. Είτε ο χρήστης δεν μπορεί να συνδεθεί στο Azure AD του οργανισμού σας είτε η εφαρμογή δεν διαθέτει τα απαιτούμενα δικαιώματα για να συνδεθεί με το Azure AD του οργανισμού σας. Θα μπορούσε επίσης να οφείλεται στο γεγονός ότι ο χρήστης ακύρωσε τον έλεγχο ταυτότητας.
303	AzureADUserProfile	Η εφαρμογή HP Sure Admin ενεργοποιήθηκε για τη λήψη πληροφοριών προφίλ χρήστη από το Azure AD του οργανισμού σας.
304	AzureADUserPrincipalMismatch	Η διεύθυνση email που έχει εισαχθεί δεν συμφωνεί με το κύριο όνομα του συνδεδεμένου χρήστη.
305	AzureADUserInvalidUserGroup	Ο συνδεδεμένος χρήστης δεν ανήκει στην εκχωρημένη ομάδα Azure AD στην οποία έχει εκχωρηθεί αυτό το κλειδί.

Πίνακας 4-4 Σφάλματα, τύποι και οι περιγραφές του KMS Admin Console

Κωδικός σφάλματος	Τύπος σφάλματος	Περιγραφή
401	KmsUnauthorized	Ο χρήστης δεν είναι εξουσιοδοτημένος να χρησιμοποιεί την υπηρεσία KMS.
402	KmsKeyDoesNotExist	Δεν υπάρχει αντίστοιχο ιδιωτικό κλειδί στον αποθηκευτικό χώρο κλειδιών KMS. Το κλειδί βρίσκεται επί του παρόντος σε μια διαγραμμένη αλλά ανακτήσιμη κατάσταση και το όνομά του δεν μπορεί να χρησιμοποιηθεί ξανά σε αυτήν την κατάσταση. Το κλειδί μπορεί να ανακτηθεί ή να καθαριστεί μόνο.
403	KmsKeyDoesNotExistInTableStorage	Το κλειδί δεν υπάρχει στον χώρο αποθήκευσης του πίνακα.

Πίνακας 4-4 Σφάλματα, τύποι και οι περιγραφές του KMS Admin Console (συνέχεια)

Κωδικός σφάλματος	Τύπος σφάλματος	Περιγραφή
404	KmsUploadKeyErrorInKeyVault	Παρουσιάστηκε σφάλμα κατά την προσθήκη κλειδιού στον αποθηκευτικό χώρο κλειδιών.
405	KmsUploadKeyUnauthorized	Ο χρήστης δεν έχει εξουσιοδότηση για αποστολή κλειδιών. Ο Χρήστης δεν ανήκει στον εξουσιοδοτημένη ομάδα AD στην οποία επιτρέπεται να καλεί το συγκεκριμένο API
406	KmsInvalidAzureADLogin	Ο χρήστης δεν έχει συνδεθεί στο Azure Tenant AAD.
407	KmsNoUserGroups	Ο συνδεδεμένος χρήστης δεν ανήκει σε καμία ομάδα του AD του οργανισμού σας.
408	KmsInvalidUserGroup	Ο συνδεδεμένος χρήστης δεν ανήκει στην εκχωρημένη ομάδα AD στην οποία έχει εκχωρηθεί αυτό το κλειδί.
409	KmsInvalidAccessToken	Το διακριτικό πρόσβασης που παρέχεται στο αίτημα δεν είναι έγκυρο.
410	KmsAccessTokenExpired	Το παρεχόμενο διακριτικό πρόσβασης έχει λήξει.
411	KmsAccessTokenInvalidTenantId	Το διακριτικό πρόσβασης που παρέχεται έχει μη έγκυρη τιμή TenantId.
412	KmsAccessTokenTenantIdMismatch	Το TenantId στο παρεχόμενο διακριτικό πρόσβασης δεν ταιριάζει με την εφαρμογή λειτουργιών TenantId
413	KmsInvalidKeyId	Το αναγνωριστικό κλειδιού είναι μηδενικό ή κενό.
414	KmsDeleteKeyUnauthorized	Ο χρήστης δεν έχει εξουσιοδότηση για διαγραφή κλειδιών. Ο χρήστης δεν ανήκει στον εξουσιοδοτημένη ομάδα AD στην οποία επιτρέπεται να καλεί το συγκεκριμένο API
415	KmsKeyVaultSoftDeleteUnrecoverableState	Η προσπάθεια ανάκτησης του μυστικού απέτυχε και δεν ήταν δυνατή η ανάκτησή του. Ο χρήστης πρέπει να δοκιμάσει ξανά.
416	KmsInvalidGetKeysRequest	Το αίτημα "Λήψη κλειδιών" δεν είναι έγκυρο.
417	KmsGetKeysUnauthorized	Ο χρήστης δεν έχει εξουσιοδότηση για λήψη κλειδιών. Ο χρήστης δεν ανήκει στον εξουσιοδοτημένη ομάδα AD στην οποία επιτρέπεται να καλεί το συγκεκριμένο API
418	KmsInvalidRequestPayload	Το αίτημα που λάβατε από το API δεν είναι έγκυρο.
419	KmsRequestRequired	Το αίτημα που λάβατε δεν πρέπει να είναι κενό.
420	KmsKeyNotConcurrent	Το κλειδί στον πίνακα αποθήκευσης ενημερώθηκε ή τροποποιήθηκε από την τελευταία φορά που ο χρήστης ανέκτησε ένα αντίγραφο.

