HP Client Security

Έναρξη χρήσης

Πρώτη έκδοση: Αύγουστος 2013

Αριθμός εγγράφου: 735339-151

Πίνακας περιεχομένων

1 Εισαγωγή στο HP Client Security Manager

Το HP Client Security σάς δίνει τη δυνατότητα να προστατεύετε τα δεδομένα, τη συσκευή και την ταυτότητά σας, αυξάνοντας έτσι την ασφάλεια του υπολογιστή σας.

Οι μονάδες λογισμικού που είναι διαθέσιμες για τον υπολογιστή σας ενδέχεται να διαφέρουν ανάλογα με το μοντέλο του υπολογιστή σας.

Το λογισμικό HP Client Security μπορεί να είναι προεγκατεστημένο, προφορτωμένο ή διαθέσιμο για λήψη από την τοποθεσία της HP στο web. Για περισσότερες πληροφορίες, επισκεφτείτε τη διεύθυνση http://www.hp.com.

ΣΗΜΕΙΩΣΗ Οι οδηγίες σε αυτό τον οδηγό γράφονται με την υπόθεση ότι έχετε ήδη εγκαταστήσει τις ισχύουσες μονάδες λογισμικού HP Client Security.

Λειτουργίες του HP Client Security

Ο ακόλουθος πίνακας παρουσιάζει τα κύρια χαρακτηριστικά των μονάδων του HP Client Security.

Μονάδα	Βασικά χαρακτηριστικά
HP Client Security Manager	Οι διαχειριστές μπορούν να εκτελούν τις ακόλουθες λειτουργίες: • Προστασία του υπολογιστή σας πριν από την εκκίνηση των Windows® • Προστασία του λογαριασμού σας στα Windows με ισχυρό έλεγχο ταυτότητας • Διαχείριση της σύνδεσης και των κωδικών πρόσβασης για ιστότοπους και εφαρμογές • Εύκολη αλλαγή του κωδικού πρόσβασης του λειτουργικού σας συστήματος Windows • Χρήση δακτυλικών αποτυπωμάτων για πρόσθετη ασφάλεια και ευκολία • Εγκατάσταση μιας έξυπνης κάρτας, κάρτας χωρίς επαφή ή κάρτας προσέγγισης για έλεγχο ταυτότητας • Χρήση του τηλεφώνου Bluetooth ως μέθοδο ταυτοποίησης • Ρύθμιση κωδικού PIN για επέκταση των επιλογών ελέγχου ταυτότητας • Διαμόρφωση πολιτικών σύνδεσης και περιόδων λειτουργίας • Δημιουργία αντιγράφων ασφαλείας και επαναφορά των δεδομένων προγράμματος • Προσθήκη περισσότερων εφαρμογών όπως HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager και HP Computrace Οι γενικοί χρήστες μπορούν να εκτελέσουν τις ακόλουθες λειτουργίες: • Προβολή ρυθμίσεων για κατάσταση κρυπτογράφησης και Device Access Manager. • Ενεργοποίηση Computrace. • Διαμόρφωση προτιμήσεων και επιλογές δημιουργίας αντιγράφων ασφαλείας και επαναφοράς.
Password Manager	Οι γενικοί χρήστες μπορούν να εκτελέσουν τις ακόλουθες λειτουργίες: • Οργάνωση και ρύθμιση ονομάτων χρήστη και κωδικών πρόσβασης. • Δημιουργία ισχυρών κωδικών πρόσβασης για βελτιωμένη ασφάλεια για λογαριασμούς email και Web λογαριασμούς. Το Password Manager συμπληρώνει και υποβάλλει τις πληροφορίες αυτόματα. • Απλοποίηση της διαδικασίας σύνδεσης με το χαρακτηριστικό μοναδικής εισόδου που αυτόματα θυμάται και εφαρμόζει τις πιστοποιήσεις χρήστη. • Επισημάνετε ένα λογαριασμό σας ως συμβιβαστικό, έτσι ώστε να μπορείτε να λάβετε ειδοποίηση για άλλο(ους) λογαριασμό(ούς) με παρόμοιες πιστοποιήσεις. • Εισαγωγή δεδομένων σύνδεσης από ένα υποστηριζόμενο πρόγραμμα περιήγησης.

Μονάδα	Βασικά χαρακτηριστικά
HP Drive Encryption (μόνο σε επιλεγμένα μοντέλα)	• Παρέχει ολοκληρωμένη, πλήρη κρυπτογράφηση όγκου σκληρού δίσκου. • Αναγκάζει την επαλήθευση πριν την εκκίνηση προκειμένου να αποκρυπτογραφήσετε και να αποκτήσετε πρόσβαση στα δεδομένα. • Προσφέρει την επιλογή για να ενεργοποιήσετε αυτοκρυπτογραφούμενους δίσκους (μόνο σε επιλεγμένα μοντέλα).
HP Device Access Manager	• Επιτρέπει στους διαχειριστές IT να ελέγχουν την πρόσβαση στις συσκευές βάσει προφίλ χρηστών. • Εμποδίζει τους μη εξουσιοδοτημένους χρήστες να αφαιρέσουν δεδομένα με εξωτερικά μέσα αποθήκευσης και να εισχωρήσουν ιοί στο σύστημα από εξωτερικά μέσα. • Επιτρέπει στους διαχειριστές να απενεργοποιήσουν την πρόσβαση σε συσκευές επικοινωνίας για συγκεκριμένα άτομα ή ομάδες χρηστών.
HP Trust Circles	• Παρέχει ασφάλεια αρχείων και εγγράφων. • Κρυπτογραφεί τα αρχεία που τοποθετούνται σε φακέλους που καθορίζονται από το χρήστη και τους προστατεύει μέσα σε ένα αξιόπιστο κύκλο. • Επιτρέπει σε αρχεία να χρησιμοποιηθούν και να μοιραστούν μεταξύ μελών του αξιόπιστου κύκλου.
Theft Recovery (Computrace, πωλείται ξεχωριστά)	• Απαιτείται ξεχωριστή αγορά συνδρομών παρακολούθησης και εντοπισμού για ενεργοποίηση. • Παρέχει ασφαλή παρακολούθηση πόρων. • Παρακολουθεί τη δραστηριότητα χρήστη, καθώς και τις αλλαγές στο υλικό και το λογισμικό. • Παραμένει ενεργό ακόμα και αν ο σκληρός δίσκος έχει ανακατασκευαστεί ή αντικατασταθεί.

Περιγραφή προϊόντος για το HP Client Security και παραδείγματα κοινής χρήσης

Τα περισσότερα από τα προϊόντα HP Client Security διαθέτουν έλεγχο ταυτότητας χρήστη (συνήθως έναν κωδικό πρόσβασης διαχειριστή) και δημιουργία αντιγράφων ασφαλείας για να αποκτήσετε πρόσβαση εάν οι κωδικοί δεν είναι διαθέσιμοι, έχουν ξεχαστεί ή οποτεδήποτε η εταιρική ασφάλεια απαιτεί πρόσβαση στο Internet.

ΣΗΜΕΙΩΣΗ Ορισμένα από τα προϊόντα HP Client Security έχουν σχεδιαστεί για να περιορίσετε την πρόσβαση στα δεδομένα. Τα δεδομένα θα πρέπει να είναι κρυπτογραφημένα όταν είναι τόσο σημαντικό ο χρήστης να χάσει τις πληροφορίες αντί αυτές να παραβιαστούν. Συνιστάται για όλα τα δεδομένα να υπάρχουν αντίγραφα ασφαλείας σε μια ασφαλή τοποθεσία.

Password Manager

Το Password Manager αποθηκεύει τα ονόματα χρήστη και τους κωδικούς πρόσβασης και μπορεί να χρησιμοποιηθεί για:

- Αποθήκευση ονομάτων εισόδου και κωδικών πρόσβασης για πρόσβαση στο Internet ή σε email.
- Αυτόματη σύνδεση χρήστη σε μια τοποθεσία Web ή email.
- Διαχείριση και οργάνωση ελέγχων ταυτότητας.
- Επιλογή τοποθεσίας Web ή παγίων δικτύου και απευθείας πρόσβαση στο σύνδεσμο.
- Προβολή ονομάτων και κωδικών πρόσβασης όταν είναι απαραίτητο.
- Επισημάνετε ένα λογαριασμό σας ως συμβιβαστικό, έτσι ώστε να μπορείτε να λάβετε ειδοποίηση για άλλο(ους) λογαριασμό(ούς) με παρόμοιες πιστοποιήσεις.
- Εισαγωγή δεδομένων σύνδεσης από ένα υποστηριζόμενο πρόγραμμα περιήγησης.

Παράδειγμα 1: Ένας αντιπρόσωπος αγορών ενός μεγάλου κατασκευαστή πραγματοποιεί το μεγαλύτερο μέρος των εταιρικών της συναλλαγών μέσω Internet. Επίσης συχνά επισκέπτεται διάφορες δημοφιλείς τοποθεσίες Web που απαιτούν πληροφορίες σύνδεσης. Γνωρίζει αρκετά καλά τα θέματα ασφαλείας έτσι ώστε δεν χρησιμοποιεί τον ίδιο κωδικό πρόσβασης σε κάθε λογαριασμό. Η αντιπρόσωπος αγορών να χρησιμοποιείτε το Password Manager ώστε να ταιριάζει συνδέσεις στο web με διαφορετικά ονόματα χρήστη και κωδικούς πρόσβασης. Όταν μεταβαίνει σε μια τοποθεσία Web για να συνδεθεί, το Password Manager παρουσιάζει τα διαπιστευτήρια αυτόματα. Εάν θέλει να δει τα ονόματα χρήστη και τους κωδικούς πρόσβασης, το Password Manager μπορεί να διαμορφωθεί ώστε να τα εμφανίζει.

Το Password Manager μπορεί επίσης να χρησιμοποιηθεί για τη διαχείριση και οργάνωση των ελέγχων ταυτότητας. Αυτό το εργαλείο θα επιτρέψει σε έναν χρήστη να επιλέξει μια τοποθεσία Web ή πάγια δικτύου και να προσπελάσει απευθείας τον σύνδεσμο. Επίσης ο χρήστης μπορεί να δει τα ονόματα χρήστη και τους κωδικούς πρόσβασης όταν είναι απαραίτητο.

Παράδειγμα 2: Ένας υπάλληλος που εργάζεται σκληρά έχει πάρει προαγωγή και πλέον θα διαχειρίζεται ολόκληρο το τμήμα λογιστικής. Η ομάδα πρέπει να συνδέεται σε μεγάλο αριθμό λογαριασμών στο web πελατών για τον καθένα από τους οποίους χρησιμοποιούνται διαφορετικές πληροφορίες σύνδεσης. Αυτές οι πληροφορίες σύνδεσης πρέπει να είναι κοινόχρηστες με άλλους συναδέλφους, έτσι η εμπιστευτικότητα αποτελεί πρόβλημα. Ο υπάλληλος αποφασίζει να οργανώσει όλες τις συνδέσεις web, τα εταιρικά ονόματα χρήστη και τους κωδικούς πρόσβασης με το Password Manager. Όταν ολοκληρωθεί η διαδικασία, ο υπάλληλος παρουσιάζει το Password Manager στους υπαλλήλους, ώστε να μπορούν να εργάζονται με λογαριασμούς στο Web λογαριασμών και να μην γνωρίζουν ποτέ τα διαπιστευτήρια σύνδεσης που χρησιμοποιούν.

HP Drive Encryption (μόνο σε επιλεγμένα μοντέλα)

Το HP Drive Encryption χρησιμοποιείται για να περιορίσει την πρόσβαση σε δεδομένα που περιέχονται σε ολόκληρο το σκληρό δίσκο του υπολογιστή ή μια δευτερεύουσα μονάδα. Το Drive Encryption μπορεί επίσης να διαχειριστεί αυτοκρυπτογραφούμενους δίσκους.

Παράδειγμα 1: Ένας γιατρός θέλει να βεβαιωθεί ότι μόνο ο ίδιος μπορεί να έχει πρόσβαση σε δεδομένα στο σκληρό δίσκο του υπολογιστή του. Ένας γιατρός ενεργοποιεί το Drive Encryption, το οποίο απαιτεί έλεγχο ταυτότητας πριν την εκκίνηση προτού συνδεθεί κάποιος στα Windows. Μόλις ρυθμιστούν οι παράμετροι, η μονάδα σκληρού δίσκου δεν μπορεί να προσπελαστεί χωρίς κωδικό πρόσβασης πριν την εκκίνηση του λειτουργικού συστήματος. Ο γιατρός θα μπορούσε να βελτιώσει περαιτέρω την ασφάλεια της μονάδας επιλέγοντας την κρυπτογράφηση των δεδομένων με αυτοκρυπτογραφούμενη μονάδα.

Παράδειγμα 2: Ένας διαχειριστής νοσοκομείου θέλει να διασφαλίσει ότι μόνο οι γιατροί και το εξουσιοδοτημένο προσωπικό μπορούν να έχουν πρόσβαση σε οποιαδήποτε δεδομένα από τον τοπικό τους υπολογιστή χωρίς κοινή χρήση των προσωπικών τους κωδικών πρόσβασης. Το τμήμα πληροφορικής προσθέτει τον διαχειριστή, τους γιατρούς και όλο το εξουσιοδοτημένο προσωπικό ως χρήστες του Drive Encryption. Τώρα μόνο εξουσιοδοτημένο προσωπικό μπορεί να εκκινήσει τον υπολογιστή ή τον τομέα χρησιμοποιώντας τα προσωπικά τους ονόματα χρήστη και τους κωδικούς πρόσβασης.

HP Device Access Manager (επιλεγμένα μοντέλα μόνο)

Το HP Device Access Manager επιτρέπει σε έναν διαχειριστή να περιορίζει και να διαχειρίζεται την πρόσβαση σε υλικό. Το Device Access Manager μπορεί να χρησιμοποιηθεί για την αποτροπή μη εξουσιοδοτημένης πρόσβασης σε μονάδες USB flash όπου τα δεδομένα μπορούν να αντιγραφούν. Μπορεί επίσης να περιορίσει την πρόσβαση σε μονάδες CD/DVD, τον έλεγχο των συσκευών USB, τις συνδέσεις δικτύου, και ούτω καθεξής. Ένα παράδειγμα είναι μια κατάσταση όπου εκτός εταιρείας προμηθευτές πρέπει να έχουν πρόσβαση σε υπολογιστές, αλλά δεν θα πρέπει να είναι σε θέση να αντιγράψουν τα δεδομένα σε μια μονάδα USB.

Παράδειγμα 1: Ο διευθυντής μιας εταιρείας ιατρικών ειδών συχνά επεξεργάζεται προσωπικά ιατρικά αρχεία μαζί με πληροφορίες της εταιρείας. Οι υπάλληλοι πρέπει να έχουν πρόσβαση σε αυτά τα δεδομένα, ωστόσο, είναι πολύ σημαντικό τα δεδομένα να μην αφαιρεθούν από τον υπολογιστή μέσω μονάδας USB ή οποιουδήποτε άλλου εξωτερικού μέσου αποθήκευσης. Το δίκτυο είναι ασφαλές αλλά οι υπολογιστές έχουν συσκευές εγγραφής CD και θύρες USB που μπορεί να επιτρέψουν στα δεδομένα να αντιγραφούν ή να κλαπούν. Ο διευθυντής χρησιμοποιεί το Device Access Manager για να απενεργοποιήσει τις θύρες USB και τις συσκευές εγγραφής CD ώστε να μην μπορούν να χρησιμοποιηθούν. Παρόλο που οι θύρες USB είναι αποκλεισμένες, το ποντίκι και τα πληκτρολόγια θα εξακολουθήσουν να λειτουργούν.

Παράδειγμα 2: Μια ασφαλιστική εταιρεία δεν θέλει οι εργαζόμενοί της να εγκαθιστούν ή να τοποθετούν προσωπικό λογισμικό ή δεδομένα από το σπίτι. Ορισμένοι εργαζόμενοι πρέπει να έχουν πρόσβαση σε θύρες USB σε όλους τους υπολογιστές. Ο υπεύθυνος πληροφορικής χρησιμοποιεί το Device Access Manager για να επιτρέψει την πρόσβαση για ορισμένους υπαλλήλους ενώ παράλληλα εμποδίζει την εξωτερική πρόσβαση για άλλους.

Computrace (πωλείται ξεχωριστά)

Το Computrace (πωλείται ξεχωριστά) είναι μια υπηρεσία που μπορεί να παρακολουθεί τη θέση ενός κλεμμένου υπολογιστή κάθε φορά που ο χρήστης αποκτά πρόσβαση στο Internet. Το Computrace μπορεί επίσης να διαχειρίζεται εξ αποστάσεως και να εντοπίζει υπολογιστές καθώς και να παρακολουθεί τη χρήση του υπολογιστή και τις εφαρμογές.

Παράδειγμα 1: Ο διευθυντής ενός σχολείου έδωσε εντολή στο τμήμα πληροφορικής να καταγράψει όλους τους υπολογιστές στο σχολείο του. Μετά την απογραφή των υπολογιστών, ο διαχειριστής IT καταχώρισε όλους τους υπολογιστές στο Computrace έτσι ώστε να μπορεί να είναι δυνατός ο εντοπισμός τους σε περίπτωση που είχαν ποτέ κλαπεί. Πρόσφατα, το σχολείο διαπίστωσε ότι πολλοί υπολογιστές λείπουν κι έτσι ο διαχειριστής του τμήματος πληροφορικής ενημέρωσε τις αρχές και τους υπαλλήλους του Computrace. Οι υπολογιστές εντοπίστηκαν και επεστράφησαν στο σχολείο από τις αρχές.

Παράδειγμα 2: Μια εταιρεία ακινήτων πρέπει να διαχειρίζεται και να ενημερώνει υπολογιστές σε όλο τον κόσμο. Χρησιμοποιεί το Computrace για την παρακολούθηση και την ενημέρωση υπολογιστών χωρίς να χρειάζεται να στείλουν έναν τεχνικό IT σε κάθε υπολογιστή.

Επίτευξη βασικών στόχων ασφαλείας

Οι μονάδες του HP Client Security μπορούν να συνεργάζονται για την παροχή λύσεων σε διάφορα θέματα ασφάλειας, συμπεριλαμβανομένων των ακόλουθων βασικών στόχων ασφάλειας:

- Προστασία από στοχευμένη κλοπή
- Περιορισμός πρόσβασης σε ευαίσθητα δεδομένα
- Αποτροπή μη εξουσιοδοτημένης πρόσβασης από εσωτερικές ή εξωτερικές θέσεις
- Δημιουργία πολιτικών ισχυρών κωδικών πρόσβασης

Προστασία από στοχευμένη κλοπή

Ένα παράδειγμα στοχευμένης κλοπής είναι η κλοπή ενός υπολογιστή που περιέχει εμπιστευτικά δεδομένα και πληροφορίες πελατών από ένα σημείο ελέγχου ασφάλειας σε κάποιο αεροδρόμιο. Τα ακόλουθα χαρακτηριστικά βοηθούν στην προστασία από στοχευμένη κλοπή:

- Ο έλεγχος ταυτότητας πριν την εκκίνηση, εάν είναι ενεργοποιημένος, βοηθά στην αποτροπή της πρόσβασης στο λειτουργικό σύστημα.
  - HP Client Security - Δείτε HP Client Security στη σελίδα 14.
  - HP Drive Encryption - Δείτε HP Drive Encryption (μόνο σε επιλεγμένα μοντέλα) στη σελίδα 33.
- Η κρυπτογράφηση δεδομένων σας βοηθάει να εξασφαλίσετε ότι δεν είναι δυνατή η πρόσβαση ακόμα και αν η μονάδα σκληρού δίσκου έχει αφαιρεθεί και τοποθετηθεί σε μη ασφαλές σύστημα.
- Το Computrace μπορεί να παρακολουθεί τη θέση του υπολογιστή μετά από κλοπή.
  - Computrace - Δείτε Theft recovery (μόνο σε επιλεγμένα μοντέλα) στη σελίδα 60

Περιορισμός πρόσβασης σε ευαίσθητα δεδομένα

Ας υποθέσουμε ότι ένας ελεγκτής συμβολαίων εργάζεται επί τόπου και του έχει επιτραπεί η πρόσβαση σε κάποιον υπολογιστή για να ελέγξει ευαίσθητα οικονομικά δεδομένα. Δεν θέλετε ο ελεγκτής να είναι σε θέση να εκτυπώσει αρχεία ή να τα αποθηκεύσει σε εγγράψιμη συσκευή, όπως ένα CD. Η παρακάτω λειτουργία βοηθά στον να περιορίσετε την πρόσβαση σε δεδομένα:

- Το HP Device Access Manager επιτρέπει σε διαχειριστές IT να περιορίσουν την πρόσβαση σε συσκευές επικοινωνίας ώστε οι ευαίσθητες πληροφορίες να είναι αδύνατο να αντιγραφούν από τη μονάδα σκληρού δίσκου. Ανατρέξτε στην ενότητα Προβολή συστήματος στη σελίδα 49.

Αποτροπή μη εξουσιοδοτημένης πρόσβασης από εσωτερικές ή εξωτερικές θέσεις

Η μη εξουσιοδοτημένη πρόσβαση σε μη ασφαλές εταιρικό υπολογιστή συνιστά πραγματικό κίνδυνο για εταιρικούς πόρους δικτύου όπως πληροφορίες από οικονομικές υπηρεσίες, ανώτερα στελέχη ή την ομάδα έρευνας και ανάπτυξης, καθώς και για προσωπικές πληροφορίες όπως αρχεία ασθενών ή

προσωπικά οικονομικά αρχεία. Τα ακόλουθα χαρακτηριστικά βοηθούν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης:

- Ο έλεγχος ταυτότητας πριν την εκκίνηση, εάν είναι ενεργοποιημένος, βοηθά στην αποτροπή της πρόσβασης στο λειτουργικό σύστημα. (δείτε HP Drive Encryption (μόνο σε επιλεγμένα μοντέλα) στη σελίδα 33.
- Το HP Client Security βοηθά να διασφαλιστεί ότι κάποιος μη εξουσιοδοτημένος χρήστης δεν μπορεί να λάβει κωδικούς πρόσβασης ή να έχει πρόσβαση σε εφαρμογές που προστατεύονται με κωδικούς πρόσβασης. Ανατρέξτε στην ενότητα HP Client Security στη σελίδα 14.
- Το HP Device Access Manager επιτρέπει σε διαχειριστές IT να περιορίσουν την πρόσβαση σε εγγράψιμες συσκευές έτσι ώστε οι ευαίσθητες πληροφορίες να είναι αδύνατο να αντιγραφούν από τη μονάδα σκληρού δίσκου. Ανατρέξτε στην ενότητα HP Device Access Manager (επιλεγμένα μοντέλα μόνο) στη σελίδα 48.

Δημιουργία πολιτικών ισχυρών κωδικών πρόσβασης

Εάν τεθεί σε ισχύ η πολιτική μιας εταιρείας σύμφωνα με την οποία απαιτείται η χρήση πολιτικής ισχυρών κωδικών πρόσβασης για δεκάδες εφαρμογές βασισμένες στο web και βάσεις δεδομένων, το Password Manager παρέχει έναν προστατευμένο χώρο αποθήκευσης για κωδικούς πρόσβασης και την άνεση μοναδικής εισόδου. Ανατρέξτε στην ενότητα Password Manager στη σελίδα 21.

Πρόσθετα στοιχεία ασφαλείας

Εκχώρηση ρόλων ασφάλειας

Όσον αφορά τη διαχείριση της ασφάλειας του υπολογιστή (ειδικά για μεγάλες επιχειρήσεις), μία σημαντική πρακτική είναι ο διαχωρισμός αρμοδιοτήτων και δικαιωμάτων μεταξύ διαφόρων τύπων διαχειριστών και χρηστών.

ΣΗΜΕΙΩΣΗ Σε μια μικρή επιχείρηση ή για προσωπική χρήση, αυτοί οι ρόλοι μπορεί να έχουν ανατεθεί στο ίδιο άτομο.

Για το HP Client Security, οι αρμοδιότητες και τα δικαιώματα ασφάλειας μπορούν να διαχωριστούν στους εξής ρόλους:

- Υπάλληλος ασφάλειας - Ορίζει το επίπεδο ασφάλειας για την εταιρεία ή το δίκτυο και καθορίζει τις δυνατότητες ασφάλειας που θα τεθούν σε ισχύ όπως το Drive Encryption.

  ΣΗΜΕΙΩΣΗ Πολλές από τις λειτουργίες του HP Client Security μπορούν να προσαρμοστούν από τον υπάλληλο ασφάλειας σε συνεργασία με την HP. Για περισσότερες πληροφορίες, επισκεφτείτε τη διεύθυνση http://www.hp.com.

- Διαχειριστής IT - Εφαρμόζει και διαχειρίζεται τις δυνατότητες ασφάλειας που ορίζει ο υπάλληλος ασφάλειας. Μπορεί επίσης να ενεργοποιεί και να απενεργοποιεί ορισμένες δυνατότητες. Για παράδειγμα, εάν ο υπάλληλος ασφάλειας έχει αποφασίσει να θέσει σε εφαρμογή έξυπνες κάρτες, ο διαχειριστής IT μπορεί να ενεργοποιήσει τους κωδικούς πρόσβασης και τη λειτουργία έξυπνων καρτών.
- Χρήστης - Χρησιμοποιεί τις δυνατότητες ασφαλείας. Για παράδειγμα, εάν ο υπάλληλος ασφαλείας και ο διαχειριστής IT έχει ενεργοποιήσει τις έξυπνες κάρτες για το σύστημα, ο χρήστης μπορεί να ορίσει το PIN της έξυπνης κάρτας και να χρησιμοποιήσει την κάρτα για έλεγχο ταυτότητας.

⚠ **ΠΡΟΣΟΧΗ** Οι διαχειριστές παροτρύνονται να ακολουθούν "βέλτιστες πρακτικές" όσον αφορά τον περιορισμό των δικαιωμάτων τελικού χρήστη και τον περιορισμό της πρόσβασης χρήστη.

Σε μη εξουσιοδοτημένους χρήστες δεν θα πρέπει να εκχωρούνται δικαιώματα διαχειριστή.

Διαχείριση κωδικών πρόσβασης του HP Client Security

Οι περισσότερες από τις λειτουργίες του HP Client Security είναι ασφαλισμένες με κωδικούς πρόσβασης. Ο ακόλουθος πίνακας παραθέτει τους συχνότερα χρησιμοποιούμενους κωδικούς πρόσβασης, τη μονάδα λογισμικού όπου έχει οριστεί ο κωδικός πρόσβασης και τη λειτουργία κωδικού πρόσβασης.

Οι κωδικοί πρόσβασης που έχουν οριστεί και χρησιμοποιούνται από διαχειριστές IT αναφέρονται μόνο σε αυτόν τον πίνακα. Όλοι οι άλλοι κωδικοί πρόσβασης ενδέχεται να έχουν ρυθμιστεί από κανονικούς χρήστες ή διαχειριστές.

Κωδικός πρόσβασης του HP Client Security	Ορίστηκε στην παρακάτω μονάδα	Λειτουργία
Κωδικός σύνδεσης στα Windows	Πίνακας ελέγχου των Windows ή HP Client Security	Μπορεί να χρησιμοποιηθεί για μη αυτόματη σύνδεση και για έλεγχο ταυτότητας κατά την πρόσβαση σε διάφορες λειτουργίες του HP Client Security.
Κωδικός πρόσβασης για δημιουργία εφεδρικών αντιγράφων και επαναφορά του HP Client Security	HP Client Security, από μεμονωμένο χρήστη	Προστατεύει την πρόσβαση στο αρχείο εφεδρικών αντιγράφων και επαναφοράς του HP Client Security.
PIN έξυπνων καρτών	Credential Manager	Μπορεί να χρησιμοποιηθεί ως πολλαπλός έλεγχος ταυτότητας. Μπορεί να χρησιμοποιηθεί ως έλεγχος ταυτότητας των Windows. Ελέγχει την ταυτότητα των χρηστών του Drive Encryption αν έχει επιλεγεί η έξυπνη κάρτα.

Δημιουργία ασφαλούς κωδικού πρόσβασης

Κατά τη δημιουργία κωδικών πρόσβασης, πρέπει πρώτα να ακολουθήσετε τυχόν προδιαγραφές που ορίζονται από το πρόγραμμα. Γενικά, ωστόσο, ακολουθήστε τις παρακάτω οδηγίες για να σας βοηθήσουν να δημιουργήσετε ισχυρούς κωδικούς πρόσβασης και να μειώσετε τις πιθανότητες παραβίασης του κωδικού πρόσβασής σας:

- Χρησιμοποιήστε κωδικούς πρόσβασης με περισσότερους από 6 χαρακτήρες, κατά προτίμηση περισσότερους από 8.
- Χρησιμοποιήστε κεφαλαία και πεζά στον κωδικό πρόσβασής σας ανακατεμένα.
- Όποτε είναι δυνατό, συνδυάστε αλφαριθμητικούς χαρακτήρες και συμπεριλάβετε ειδικούς χαρακτήρες και σημεία στίξης.
- Αντικαταστήσετε τα γράμματα με ειδικούς χαρακτήρες ή αριθμούς σε μια λέξη-κλειδί. Για παράδειγμα, μπορείτε να χρησιμοποιήσετε τον αριθμό 1 για τα γράμματα I ή L.
- Συνδυάστε λέξεις από 2 ή περισσότερες γλώσσες.

- Διαχωρίστε μια λέξη ή φράση με αριθμούς ή ειδικούς χαρακτήρες στη μέση, για παράδειγμα "Mary2-2cat45."
- Μην χρησιμοποιείτε έναν κωδικό πρόσβασης που μπορεί να υπάρχει στο λεξικό.
- Μην χρησιμοποιείτε το όνομά σας για τον κωδικό πρόσβασης ή άλλα προσωπικά στοιχεία, όπως την ημερομηνία γέννησης, ονόματα κατοικίδιων ή το πατρικό επώνυμο της μητέρας σας, ακόμα και αν θέλετε να το συλλαβίσετε ανάποδα.
- Αλλάζετε τακτικά κωδικούς πρόσβασης. Μπορείτε να αλλάξετε μόνο μερικούς χαρακτήρες που αυξάνονται.
- Αν σημειώσετε τον κωδικό πρόσβασής σας, δεν πρέπει να τον τοποθετήσετε σε ένα γενικά ορατό μέρος πολύ κοντά στον υπολογιστή.
- Μην αποθηκεύετε τον κωδικό πρόσβασης σε ένα αρχείο, όπως ένα μήνυμα email, στον υπολογιστή.
- Να κάνετε κοινή χρήση λογαριασμών και μην αναφέρατε σε κανέναν τον κωδικό πρόσβασής σας.

Δημιουργία αντιγράφων ασφαλείας διαπιστευτηρίων και ρυθμίσεων

Μπορείτε να χρησιμοποιήσετε το εργαλείο δημιουργίας αντιγράφων ασφαλείας και επαναφοράς στο HP Client Security ως κεντρική τοποθεσία από την οποία μπορείτε να δημιουργήσετε αντίγραφα ασφαλείας και να επαναφέρετε τις πιστοποιήσεις ασφαλείας από ορισμένες εγκατεστημένες μονάδες του HP Client Security.

2 Έναρξη χρήσης

Για να διαμορφώσετε τις ρυθμίσεις του HP Client Security για χρήση με τα διαπιστευτήριά σας, εκκινήστε το HP Client Security με έναν από τους παρακάτω τρόπους. Μόλις ο οδηγός ολοκληρωθεί από τον χρήστη δεν μπορεί να εκκινηθεί ξανά από αυτόν τον χρήστη.

1. Από την οθόνη Έναρξη ή Εφαρμογές, κάντε κλικ ή πατήστε στην εφαρμογή **HP Client Security** (Windows 8).

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε κλικ ή πατήστε στο **HP Client Security Gadget** (Windows 7).

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε διπλό κλικ ή διπλό πάτημα στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στο δεξί άκρο της γραμμής εργαλείων.

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε κλικ ή πατήστε στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων και, στη συνέχεια, επιλέξτε **Open HP Client Security** (Άνοιγμα του HP Client Security).

2. Εκκινεί ο οδηγός εγκατάστασης του HP Client Security και εμφανίζεται η σελίδα υποδοχής.

3. Διαβάστε την οθόνη υποδοχής, επαληθεύστε την ταυτότητά σας πληκτρολογώντας τον κωδικό πρόσβασης των Windows και κάντε κλικ ή πατήστε στο **Next** (Επόμενο).

   Εάν δεν έχετε δημιουργήσει ακόμα κωδικό πρόσβασης των Windows, σας ζητείται να τον δημιουργήσετε. Ο κωδικός πρόσβασης των Windows είναι αναγκαίος έτσι ώστε να προστατεύετε το λογαριασμό σας των Windows από πρόσβαση από μη εξουσιοδοτημένα άτομα και για να χρησιμοποιείτε τις λειτουργίες του HP Client Security.

4. Στη σελίδα HP SpareKey, επιλέξτε τρεις ερωτήσεις ασφαλείας. Εισαγάγετε μια απάντηση για κάθε ερώτηση και, στη συνέχεια, κάντε κλικ στο **Next** (Επόμενο). Επιτρέπονται επίσης προσαρμοσμένες ερωτήσεις. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα HP SpareKey—Επαναφορά κωδικού πρόσβασης στη σελίδα 16.

5. Στη σελίδα Δακτυλικά αποτυπώματα, δηλώστε τουλάχιστον τον ελάχιστο αριθμό απαιτούμενων δακτυλικών αποτυπωμάτων και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Next** (Επόμενο). Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Δακτυλικά αποτυπώματα στη σελίδα 15.

6. Στη σελίδα Κρυπτογράφηση δίσκου, ενεργοποιήστε την κρυπτογράφηση, δημιουργήστε αντίγραφο ασφαλείας του κλειδιού κρυπτογράφησης και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Next** (Επόμενο). Για περισσότερες πληροφορίες, δείτε τη βοήθεια του λογισμικού HP Drive Encryption.

ΣΗΜΕΙΩΣΗ Αυτό ισχύει για το σενάριο όπου ο χρήστης είναι διαχειριστής και ο οδηγός εγκατάστασης του HP Client Security δεν έχει διαμορφωθεί προηγουμένως από ένα διαχειριστή.

7. Στην τελευταία σελίδα του οδηγού, κάντε κλικ ή πατήστε στο **Finish** (Τέλος).

   Η σελίδα αυτή παρέχει την κατάσταση των λειτουργιών και διαπιστευτηρίων.

8. Ο οδηγός εγκατάστασης του HP Client Security διασφαλίζει την ενεργοποίηση των λειτουργιών Just In Time Authentication και File Sanitizer. Για περισσότερες πληροφορίες, ανατρέξτε στη βοήθεια του λογισμικού HP Device Access Manager και στη βοήθεια του λογισμικού HP File Sanitizer.

ΣΗΜΕΙΩΣΗ Αυτό ισχύει για το σενάριο όπου ο χρήστης είναι διαχειριστής και ο οδηγός εγκατάστασης του HP Client Security δεν έχει διαμορφωθεί προηγουμένως από ένα διαχειριστή.

Άνοιγμα του HP Client Security

Μπορείτε να ανοίξετε την εφαρμογή HP Client Security με έναν από τους ακόλουθους τρόπους:

ΣΗΜΕΙΩΣΗ Ο οδηγός εγκατάστασης του HP Client Security πρέπει να έχει ολοκληρωθεί για να μπορέσετε να εκκινήσετε την εφαρμογή HP Client Security.

- Από την οθόνη Έναρξη ή Εφαρμογές, κάντε κλικ ή πατήστε στην εφαρμογή **HP Client Security**.

  – ή –

  Από την επιφάνεια εργασίας των Windows, κάντε κλικ ή πατήστε στο **HP Client Security** Gadget (Windows 7).

  – ή –

  Από την επιφάνεια εργασίας των Windows, κάντε διπλό κλικ ή διπλό πάτημα στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στο δεξί άκρο της γραμμής εργαλείων.

  – ή –

  Από την επιφάνεια εργασίας των Windows, κάντε κλικ ή πατήστε στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων και, στη συνέχεια, επιλέξτε **Open HP Client Security** (Άνοιγμα του HP Client Security).

3 Εύκολος Οδηγός εγκατάστασης για μικρές επιχειρήσεις

Αυτό το κεφάλαιο έχει σχεδιαστεί για να δείξει τα βασικά βήματα για να ενεργοποιήσετε τις πιο κοινές και χρήσιμες επιλογές του HP Client Security για μικρές επιχειρήσεις. Πολλά εργαλεία και επιλογές αυτού του λογισμικού σας επιτρέπουν να ρυθμίσετε τις προτιμήσεις και να ορίσετε τον έλεγχο πρόσβασης. Αυτός ο εύχρηστος οδηγός εγκατάστασης εστιάζει στο πώς κάθε μονάδα θα τεθεί σε λειτουργία με την ελάχιστη προσπάθεια και χρόνο. Για πρόσθετες πληροφορίες, επιλέξτε τη μονάδα που σας ενδιαφέρει και, στη συνέχεια, κάντε κλικ στο **;** ή κουμπί Βοήθεια στην επάνω δεξιά γωνία. Αυτό το κουμπί θα εμφανίζει αυτόματα πληροφορίες για να σας βοηθήσει με το τρέχον παράθυρο.

Έναρξη χρήσης

1. Από την επιφάνεια εργασίας των Windows, ανοίξτε το HP Client Security κάνοντας διπλό κλικ στο εικονίδιο **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στη δεξιά πλευρά της γραμμής εργασιών.
2. Εισαγάγετε τον κωδικό πρόσβασης των Windows ή δημιουργήστε έναν κωδικό πρόσβασης των Windows.
3. Ολοκληρώστε την εγκατάσταση του HP Client Security.

Για να χρησιμοποιήσετε το HP Client Security απαιτείται έλεγχος ταυτότητας μόνο μία φορά κατά τη διάρκεια της σύνδεσης στα Windows, ανατρέξτε στην ενότητα Λειτουργίες ασφαλείας στη σελίδα 30.

Password Manager

Όλοι οι χρήστες έχουν αρκετούς κωδικούς πρόσβασης - ιδιαίτερα εάν επισκέπτεστε τακτικά τοποθεσίες web ή χρησιμοποιείτε εφαρμογές που απαιτούν να συνδεθείτε. Ο κανονικός χρήστης είτε χρησιμοποιεί τον ίδιο κωδικό πρόσβασης χρήστη για κάθε εφαρμογή και τοποθεσία web ή γίνεται δημιουργικός και αμέσως ξεχνά ποιος κωδικό πρόσβασης ταιριάζει με ποια εφαρμογή.

Το Password Manager μπορεί αυτόματα να θυμάται τους κωδικούς πρόσβασης ή σάς δίνει τη δυνατότητα να διακρίνετε ποιες τοποθεσίες να θυμάστε και ποιες πρέπει να αγνοήσετε. Μετά την είσοδό σας στον υπολογιστή, το Password Manager θα παρέχει τους κωδικούς πρόσβασης ή τις πιστοποιήσεις για τις εφαρμογές ή τις τοποθεσίες web που συμμετέχουν στο πρόγραμμα.

Όταν αποκτήσετε πρόσβαση σε οποιαδήποτε εφαρμογή ή τοποθεσία Web που απαιτεί πιστοποιήσεις, το Password Manager θα αναγνωρίζει αυτόματα την τοποθεσία, και θα σας ρωτάει εάν θέλετε το λογισμικό να θυμάται τις πληροφορίες. Εάν θέλετε να εξαιρέσετε συγκεκριμένες τοποθεσίες, μπορείτε να αρνηθείτε την αίτηση.

Για να εκκινήσετε την αποθήκευση τοποθεσιών web, ονομάτων χρηστών και κωδικών πρόσβασης:

1. Για παράδειγμα, πλοηγηθείτε σε μία τοποθεσία web ή εφαρμογή που συμμετέχει στο πρόγραμμα και, στη συνέχεια, κάντε κλικ στο εικονίδιο Password Manager στην επάνω αριστερή γωνία της σελίδας web για να προσθέσετε τον έλεγχο ταυτότητας web.
2. Δώστε όνομα στη σύνδεση (προαιρετικό) και πληκτρολογήστε το όνομα χρήστη και τον κωδικό πρόσβασης στο Password Manager.

3. Όταν ολοκληρώσετε, κάντε κλικ στο κουμπί **OK**.

4. Το Password Manager μπορεί επίσης να αποθηκεύσει το όνομα χρήστη και τους κωδικούς πρόσβασης για κοινή χρήση δικτύου ή αντιστοίχιση μονάδων δικτύου.

Προβολή και διαχείριση αποθηκευμένων ελέγχων ταυτότητας στο Password Manager

Το Password Manager σας δίνει τη δυνατότητα να δείτε, να διαχειριστείτε, να δημιουργήσετε αντίγραφα ασφαλείας και να πραγματοποιήσετε εκκίνηση ελέγχων ταυτότητας από μια κεντρική θέση. Το Password Manager υποστηρίζει επίσης την εκκίνηση των αποθηκευμένων τοποθεσιών από τα Windows.

Για να ανοίξετε το Password Manager, χρησιμοποιήστε τον συνδυασμό πλήκτρων Ctrl+Πλήκτρο Windows+h για να ανοίξετε το Password Manager και, στη συνέχεια, κάντε κλικ στο κουμπί **Σύνδεση** για να εκκινήσετε και να ελέγξετε την αποθηκευμένη συντόμευση.

Η επιλογή **Επεξεργασία** του Password Manager σάς επιτρέπει να προβάλλετε και να τροποποιήσετε το όνομα, το όνομα σύνδεσης, ακόμη και να αποκαλύψετε τους κωδικούς πρόσβασης.

Το HP Client Security για μικρές επιχειρήσεις επιτρέπει τη δημιουργία αντιγράφων ασφαλείας όλων των πιστοποιήσεων και των ρυθμίσεων ή/και την αντιγραφή τους σε άλλον υπολογιστή.

HP Device Access Manager

Το Device Access Manager μπορεί να χρησιμοποιηθεί για να περιορίσετε τη χρήση διάφορων εσωτερικών και εξωτερικών συσκευών αποθήκευσης ώστε τα δεδομένα σας να παραμείνουν ασφαλή στο σκληρό δίσκο και όχι να διαρρεύσουν από την επιχείρησή σας. Ένα παράδειγμα είναι να επιτρέπεται η πρόσβαση των χρηστών στα δεδομένα σας αλλά να μην είναι σε θέση να τα αντιγράψουν σε CD, προσωπικές συσκευές αναπαραγωγής μουσικής ή συσκευές μνήμης USB.

1. Ανοίξτε το **Device Access Manager** (δείτε). Άνοιγμα του Device Access Manager στη σελίδα 49

   Εμφανίζεται η πρόσβαση για τον τρέχοντα χρήστη.

2. Για να αλλάξετε πρόσβαση για χρήστες, ομάδες ή συσκευές, κάντε κλικ ή πατήστε **Αλλαγή**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Προβολή συστήματος στη σελίδα 49.

HP Drive Encryption

Το HP Drive Encryption χρησιμοποιείται για την προστασία των δεδομένων σας, κρυπτογραφώντας ολόκληρο τον σκληρό δίσκο. Τα δεδομένα στο σκληρό δίσκο θα παραμένουν προστατευμένα εάν ο υπολογιστής σας κλαπεί ή/και η μονάδα σκληρού δίσκου αφαιρεθεί από τον αρχικό υπολογιστή και τοποθετηθεί σε άλλο υπολογιστή.

Ένα πρόσθετο πλεονέκτημα ασφαλείας είναι ότι το Drive Encryption απαιτεί τον σωστό έλεγχο ταυτότητας του χρήστη χρησιμοποιώντας το όνομα χρήστη και τον κωδικό πρόσβασης πριν την εκκίνηση του λειτουργικού συστήματος. Αυτή η διαδικασία ονομάζεται έλεγχος ταυτότητας πριν την εκκίνηση.

Για να σας διευκολύνουν, πολλές μονάδες λογισμικού συγχρονίζουν τους κωδικούς πρόσβασης αυτόματα, συμπεριλαμβανομένων των λογαριασμών χρηστών των Windows, των τομέων ελέγχων ταυτότητας, του HP Drive Encryption, του Password Manager και του HP Client Security.

Για να ρυθμίσετε το HP Drive Encryption κατά την αρχική εγκατάσταση με τον οδηγό εγκατάστασης του HP Client Security, ανατρέξτε στην ενότητα Έναρξη χρήσης στη σελίδα 10.

4 HP Client Security

Η αρχική σελίδα του HP Client Security είναι η κεντρική τοποθεσία για εύκολη πρόσβαση στις λειτουργίες, τις εφαρμογές και τις ρυθμίσεις του HP Client Security. Η αρχική σελίδα διαιρείται σε τρεις ενότητες:

- **DATA** (ΔΕΔΟΜΕΝΑ)—Παρέχει πρόσβαση σε εφαρμογές που χρησιμοποιούνται για τη διαχείριση της ασφαλείας δεδομένων.
- **DEVICE** (ΣΥΣΚΕΥΗ)—Παρέχει πρόσβαση σε εφαρμογές που χρησιμοποιούνται για τη διαχείριση της ασφάλειας της συσκευής.
- **IDENTITY** (ΤΑΥΤΟΤΗΤΑ)—Παρέχει τη δυνατότητα δήλωσης και διαχείρισης των διαπιστευτηρίων ελέγχου ταυτότητας.

Μετακινήστε τον κέρσορα πάνω από ένα τετράγωνο εφαρμογής για να εμφανιστεί η περιγραφή της εφαρμογής.

Το HP Client Security ενδέχεται να παρέχει συνδέσμους σε ρυθμίσεις χρηστών και διαχειριστικές ρυθμίσεις στο κάτω μέρος της σελίδας. Το HP Client Security παρέχει πρόσβαση σε ρυθμίσεις για προχωρημένους και λειτουργίες πατώντας ή κάνοντας κλικ στο εικονίδιο **Gear** (ρυθμίσεις).

Λειτουργίες, εφαρμογές και ρυθμίσεις ταυτότητας

Οι λειτουργίες, εφαρμογές και ρυθμίσεις ταυτότητας που παρέχονται από το HP Client Security σάς βοηθούν να διαχειρίζεστε διάφορες πλευρές της ψηφιακής σας ταυτότητας. Κάντε κλικ ή πατήστε σε ένα από τα παρακάτω τετράγωνα στην αρχική σελίδα του HP Client Security και στη συνέχεια πληκτρολογήστε τον κωδικό πρόσβασης των Windows:

- **Fingerprints** (Δαχτυλικά αποτυπώματα)—Δήλωση και διαχείριση των διαπιστευτηρίων δαχτυλικών αποτυπωμάτων.
- **SpareKey** (Ανταλλακτικό κλειδί)—Εγκαθιστά και διαχειρίζεται το διαπιστευτήριο HP SpareKey που μπορεί να χρησιμοποιηθεί για σύνδεση στον υπολογιστή σας αν έχουν χαθεί ή δεν μπορούν να εντοπιστούν τα άλλα διαπιστευτήρια. Σας επιτρέπει επίσης να επαναφέρετε τον ξεχασμένο κωδικό πρόσβασης.
- **Windows Password** (Κωδικός πρόσβασης των Windows)—Παρέχει εύκολη πρόσβαση για αλλαγή του κωδικού πρόσβασης των Windows.
- **Bluetooth Devices** (Συσκευές Bluetooth)—Επιτρέπει τη δήλωση και διαχείριση συσκευών Bluetooth.
- **Cards** (Κάρτες)—Επιτρέπει τη δήλωση και διαχείριση έξυπνων καρτών, καρτών χωρίς επαφή και καρτών προσέγγισης.
- **PIN** (Κωδικός PIN)—Επιτρέπει τη δήλωση και διαχείριση του διαπιστευτηρίου κωδικός PIN.
- **RSA SecurID**—Επιτρέπει να εγγραφείτε και να διαχειριστείτε τα διαπιστευτήρια του RSA SecurID (εάν έχει γίνει σωστή εγκατάσταση).
- **Password Manager** (Διαχείριση κωδικού πρόσβασης)—Επιτρέπει τη διαχείριση κωδικών πρόσβασης για τους online λογαριασμούς και εφαρμογές.

Δακτυλικά αποτυπώματα

Ο οδηγός εγκατάστασης του HP Client Security σας καθοδηγεί στη διαδικασία εγκατάστασης ή “δήλωσης” των δακτυλικών σας αποτυπωμάτων.

Μπορείτε επίσης να δηλώσετε ή να διαγράψετε τα δακτυλικά σας αποτυπώματα στη σελίδα Δακτυλικά αποτυπώματα, στην οποία μπορείτε να αποκτήσετε πρόσβαση κάνοντας κλικ ή πατώντας στο εικονίδιο **Fingerprints** (Δακτυλικά αποτυπώματα) στην αρχική σελίδα του HP Client Security.

1. Στη σελίδα Δακτυλικά αποτυπώματα, σαρώστε ένα δάκτυλο μέχρι να δηλωθεί με επιτυχία.

   Ο αριθμός δακτύλων που απαιτείται να δηλώσετε υποδεικνύεται στη σελίδα. Προτιμούνται οι δείκτες ή τα μεσαία δάκτυλα.

2. Για να διαγράψετε δάκτυλα που έχετε δηλώσει προηγουμένως, κάντε κλικ ή πατήστε στο **Delete** (Διαγραφή).

3. Για να δηλώσετε πρόσθετα δάκτυλα, κάντε κλικ ή πατήστε στο **Enroll an additional fingerprint** (Δήλωση πρόσθετου δάκτυλου).

4. Κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση) πριν αφήσετε τη σελίδα.

⚠ **ΠΡΟΣΟΧΗ** Όταν δηλώνετε δάκτυλα μέσω του οδηγού, οι πληροφορίες για τα δακτυλικά αποτυπώματα δεν αποθηκεύονται μέχρι να κάνετε κλικ στο **Next** (Επόμενο). Αν αφήσετε τον υπολογιστή ανενεργό για λίγο ή κλείσετε το πρόγραμμα, οι αλλαγές που κάνατε **δεν** αποθηκεύτηκαν.

- ▲ Για να αποκτήσετε πρόσβαση στις ρυθμίσεις διαχείρισης δακτυλικών αποτυπωμάτων, όπου οι διαχειριστές μπορούν να ορίσουν τη δήλωση, την ακρίβεια και άλλες ρυθμίσεις, κάντε κλικ ή πατήστε στο **Administrative Settings** (Ρυθμίσεις διαχείρισης) (απαιτούνται δικαιώματα διαχείρισης).

- ▲ Για να αποκτήσετε πρόσβαση στις ρυθμίσεις χρηστών δακτυλικών αποτυπωμάτων, όπου μπορείτε να ορίσετε ρυθμίσεις που διέπουν την εμφάνιση και συμπεριφορά της αναγνώρισης δακτυλικών δικαιωμάτων, κάντε κλικ ή πατήστε στο **User Settings** (Ρυθμίσεις χρήστη).

Ρυθμίσεις διαχείρισης δακτυλικών αποτυπωμάτων

Οι διαχειριστές μπορούν να ορίσουν τη δήλωση, ακρίβεια και άλλες ρυθμίσεις για έναν αναγνώστη δακτυλικών αποτυπωμάτων. Απαιτούνται δικαιώματα διαχειριστή.

- ▲ Για να αποκτήσετε πρόσβαση στις ρυθμίσεις διαχείρισης για τα διαπιστευτήρια δακτυλικών αποτυπωμάτων, κάντε κλικ ή πατήστε στο **Administrative Settings** (Ρυθμίσεις διαχείρισης) στη σελίδα Δακτυλικά αποτυπώματα.

- **User enrollment** (Δήλωση χρήστη)—Επιλέξτε τον ελάχιστο και το μέγιστο αριθμό δακτυλικών αποτυπωμάτων που ο χρήστης επιτρέπεται να δηλώσει.

- **Recognition** (Αναγνώριση)—Μετακινήστε το ρυθμιστικό για να προσαρμόσετε την ευαισθησία που χρησιμοποιείται από τον αναγνώστη δακτυλικών αποτυπωμάτων όταν σαρώνετε το δάκτυλό σας.

  Αν το δακτυλικό σας αποτύπωμα δεν αναγνωρίζεται με συνέπεια, ενδέχεται να χρειαστεί να επιλέξετε μια χαμηλότερη ρύθμιση αναγνώρισης. Η υψηλότερη ρύθμιση αυξάνει την ευαισθησία σε παραλλαγές των σαρώσεων δακτυλικών αποτυπωμάτων επομένως μειώνει την πιθανότητα εσφαλμένης αποδοχής. Η ρύθμιση **Medium-High** (Μεσαία-Υψηλή) παρέχει ένα καλό μίγμα ασφάλειας και άνεσης.

Ρυθμίσεις χρηστών δακτυλικών αποτυπωμάτων

Στη σελίδα Ρυθμίσεις χρηστών δακτυλικών αποτυπωμάτων, μπορείτε να ορίσετε ρυθμίσεις που διέπουν την εμφάνιση και συμπεριφορά της αναγνώρισης δακτυλικών αποτυπωμάτων.

▲ Για να αποκτήσετε πρόσβαση στις ρυθμίσεις χρηστών για τα διαπιστευτήρια δακτυλικών αποτυπωμάτων, κάντε κλικ ή πατήστε στο **User Settings** (Ρυθμίσεις χρηστών) στη σελίδα Δακτυλικά αποτυπώματα.

- **Enable sound feedback** (Ενεργοποίηση ανάδρασης ήχου)—Από προεπιλογή, το HP Client Security σάς δίνει ηχητική ανάδραση όταν έχει σαρωθεί ένα δακτυλικό αποτύπωμα, αναπαράγοντας διαφορετικούς ήχους για συγκεκριμένα συμβάντα του προγράμματος. Μπορείτε να εκχωρήσετε νέους ήχους σε αυτά τα συμβάντα μέσω της καρτέλας Ήχοι στη ρύθμιση ήχου στον πίνακα ελέγχου των Windows ή να απενεργοποιήσετε την ανάδραση ήχου καταργώντας την επιλογή του πλαισίου ελέγχου.
- **Show scan quality feedback** (Εμφάνιση σχολίου ποιότητας σάρωσης)—Για εμφάνιση όλων των σαρώσεων, ανεξάρτητα από ποιότητα, επιλέξτε το πλαίσιο ελέγχου. Για εμφάνιση μόνο ποιοτικών σαρώσεων, καταργήστε την επιλογή του πλαισίου ελέγχου.

HP SpareKey—Επαναφορά κωδικού πρόσβασης

Το HP SpareKey σάς επιτρέπει να ανακτήσετε πρόσβαση στον υπολογιστή σας (σε υποστηριζόμενες πλατφόρμες) απαντώντας σε τρεις ερωτήσεις ασφαλείας.

Το HP Client Security σάς ζητάει να εγκαταστήσετε το προσωπικό σας HP SpareKey κατά τη διάρκεια της αρχικής εγκατάστασης στον οδηγό εγκατάστασης του HP Client Security.

Για να εγκαταστήσετε το HP SpareKey:

1. Στη σελίδα HP SpareKey του οδηγού, επιλέξτε τρεις ερωτήσεις ασφάλειας και στη συνέχεια πληκτρολογήστε μια απάντηση για κάθε ερώτηση.

   Μπορείτε να επιλέξετε μια ερώτηση από μια προκαθορισμένη λίστα ή να γράψετε τη δική σας ερώτηση.

2. Κάντε κλικ ή πατήστε στο **Enroll** (Δήλωση).

Για να διαγράψετε το HP SpareKey:

▲ Κάντε κλικ ή πατήστε στο **Delete your SpareKey** (Διαγραφή του SpareKey).

Αφού εγκαταστήσετε το SpareKey, μπορείτε να αποκτήσετε πρόσβαση στον υπολογιστή χρησιμοποιώντας το SpareKey από μια οθόνη σύνδεσης με έλεγχο ταυτότητας κατά την εκκίνηση στην οθόνη υποδοχής των Windows.

Μπορείτε να επιλέξετε διαφορετικές ερωτήσεις ή να αλλάξετε τις απαντήσεις στη σελίδα του SpareKey, στην οποία μπορείτε να αποκτήσετε πρόσβαση από το τετράγωνο Επαναφορά κωδικού πρόσβασης στην αρχική σελίδα του HP Client Security.

Για πρόσβαση στις ρυθμίσεις του HP SpareKey, όπου ο διαχειριστής μπορεί να καθορίσει ρυθμίσεις σχετικές με τα διαπιστευτήρια HP SpareKey, κάντε κλικ στο **Settings** (Ρυθμίσεις) (απαιτούνται δικαιώματα διαχειριστή).

HP SpareKey Settings

Στη σελίδα ρυθμίσεων του HP SpareKey, μπορείτε να ορίσετε ρυθμίσεις που διέπουν τη συμπεριφορά και χρήση του διαπιστευτηρίου HP SpareKey.

▲ Για εκκίνηση της σελίδας ρυθμίσεων του HP SpareKey, κάντε κλικ ή πατήστε στο **Settings** (Ρυθμίσεις) στη σελίδα HP SpareKey (απαιτούνται δικαιώματα διαχειριστή).

Οι διαχειριστές μπορούν να επιλέξουν από τις ακόλουθες ρυθμίσεις:

- Καθορισμός των ερωτήσεων που θα παρουσιάζονται σε κάθε χρήστη κατά τη διάρκεια της εγκατάστασης του HP SpareKey.
- Προσθήκη έως τριών προσαρμοσμένων ερωτήσεων ασφαλείας στη λίστα που εμφανίζεται στους χρήστες.
- Επιλογή αν θα επιτρέπεται στους χρήστες να γράφουν τις δικές τους ερωτήσεις ασφαλείας.
- Καθορισμός ποια περιβάλλοντα ελέγχου ταυτότητας (Windows ή έλεγχος ταυτότητας κατά την εκκίνηση) επιτρέπουν τη χρήση του HP SpareKey για επαναφορά του κωδικού πρόσβασης.

Κωδικός πρόσβασης των Windows

Το HP Client Security κάνει ευκολότερη και γρηγορότερη την αλλαγή του κωδικού πρόσβασης των Windows σε σχέση με τον πίνακα ελέγχου των Windows.

Για να αλλάξετε τον κωδικό πρόσβασης των Windows:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο **Windows Password** (Κωδικός πρόσβασης των Windows).
2. Πληκτρολογήστε τον τρέχοντα κωδικό πρόσβασης στο πλαίσιο κειμένου **Current Windows password** (Τρέχων κωδικός πρόσβασης).
3. Πληκτρολογήστε ένα νέο κωδικό πρόσβασης στο πλαίσιο κειμένου **New Windows password** (Νέος κωδικός πρόσβασης των Windows) και στη συνέχεια πληκτρολογήστε το ξανά στο πλαίσιο κειμένου **Confirm new password** (Επιβεβαίωση κωδικού πρόσβασης).
4. Κάντε κλικ ή πατήστε στο **Change** (Αλλαγή) για να αλλάξετε αμέσως τον τρέχοντα κωδικό πρόσβασης στον νέο που πληκτρολογήσατε.

Συσκευές Bluetooth

Αν ο διαχειριστής έχει ενεργοποιήσει την επιλογή Bluetooth ως διαπιστευτήριο ελέγχου ταυτότητας, μπορείτε να εγκαταστήσετε ένα τηλέφωνο Bluetooth σε συνδυασμό με άλλα διαπιστευτήρια για πρόσθετη ασφάλεια.

ΣΗΜΕΙΩΣΗ Υποστηρίζονται μόνο συσκευές τηλεφώνου Bluetooth.

1. Βεβαιωθείτε ότι η λειτουργικότητα Bluetooth είναι ενεργοποιημένη στον υπολογιστή και ότι το τηλέφωνο Bluetooth έχει ρυθμιστεί στη λειτουργία εντοπισμού. Για να συνδέσετε το τηλέφωνο, μπορεί να απαιτηθεί να πληκτρολογήσετε έναν κωδικό που δημιουργείται αυτόματα στη συσκευή Bluetooth. Ανάλογα με τη διαμόρφωση ρυθμίσεων της συσκευής Bluetooth, ενδέχεται να απαιτηθεί μια σύγκριση των κωδικών ζεύξης μεταξύ του υπολογιστή και του τηλεφώνου.
2. Για να δηλώσετε το τηλέφωνο, επιλέξτε το και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Enroll** (Δήλωση).

Για πρόσβαση στη σελίδα Ρυθμίσεις συσκευής Bluetooth στη σελίδα 17 όπου ο διαχειριστής μπορεί να ορίσει ρυθμίσεις για συσκευές Bluetooth, κάντε κλικ στο **Settings** (Ρυθμίσεις) (απαιτούνται δικαιώματα διαχειριστή).

Ρυθμίσεις συσκευής Bluetooth

Οι διαχειριστές μπορούν να ορίσουν τις ακόλουθες ρυθμίσεις που διέπουν τη συμπεριφορά και χρήση των διαπιστευτηρίων της συσκευής Bluetooth:

Σιωπηρός έλεγχος ταυτότητας

- **Automatically use your connected enrolled Bluetooth Device during verification of your identity** (Αυτόματη χρήση της δηλωμένης συνδεδεμένης συσκευής Bluetooth κατά τη διάρκεια επαλήθευσης της ταυτότητας)—Επιλέξτε το πλαίσιο ελέγχου για να επιτρέπετε στους χρήστες να χρησιμοποιούν για έλεγχο ταυτότητας τα διαπιστευτήρια Bluetooth χωρίς να απαιτείται ενέργεια από το χρήστη ή καταργήστε την επιλογή αν θέλετε να απενεργοποιήσετε αυτή την επιλογή.

Εγγύτητα Bluetooth

- **Κλειδώστε τον υπολογιστή όταν η εγγεγραμμένη συσκευή σας Bluetooth τίθεται εκτός της εμβέλειας του υπολογιστή σας**—Επιλέξτε αυτό το πλαίσιο ελέγχου για να κλειδώσετε τον υπολογιστή όταν μια συσκευή Bluetooth που ήταν συνδεδεμένη κατά τη σύνδεση τίθεται εκτός εμβέλειας ή καταργήστε την επιλογή του πλαισίου ελέγχου για να απενεργοποιήσετε αυτήν την επιλογή.

ΣΗΜΕΙΩΣΗ Το στοιχείο Bluetooth στον υπολογιστή πρέπει να υποστηρίζει αυτή τη δυνατότητα για να μπορεί να εκμεταλλευτεί αυτή τη λειτουργία.

Κάρτες

Το HP Client Security μπορεί να υποστηρίξει ένα αριθμό διαφορετικών τύπων καρτών ταυτοποίησης, οι οποίες είναι μικρές πλαστικές κάρτες που περιέχουν ένα υπολογιστικό τσιπ. Οι τύποι αυτοί περιλαμβάνουν έξυπνες κάρτες, κάρτες χωρίς επαφή και κάρτες εγγύτητας. Μπορείτε να χρησιμοποιήσετε την κάρτα ως διαπιστευτήριο ελέγχου ταυτότητας, αν μια από αυτές τις κάρτες και ο κατάλληλος αναγνώστης καρτών είναι συνδεδεμένα στον υπολογιστή, αν ο διαχειριστής έχει εγκαταστήσει το σχετικό πρόγραμμα οδήγησης του κατασκευαστή και αν ο διαχειριστής έχει ενεργοποιήσει την κάρτα ως διαπιστευτήριο ελέγχου ταυτότητας.

Για τις έξυπνες κάρτες, ο κατασκευαστής πρέπει να παρέχει εργαλεία για την εγκατάσταση του πιστοποιητικού ασφάλειας και τη διαχείριση κωδικού PIN που χρησιμοποιεί το HP Client Security στον αλγόριθμο ασφαλείας. Ο αριθμός και ο τύπος των χαρακτήρων που χρησιμοποιούνται ως κωδικός PIN ενδέχεται να διαφέρει. Ο διαχειριστής πρέπει να προετοιμάσει την έξυπνη κάρτα πριν τη χρήση της.

Οι ακόλουθες μορφές έξυπνων καρτών υποστηρίζονται από το HP Client Security:

- CSP
- PKCS11

Οι ακόλουθοι τύποι καρτών χωρίς επαφή υποστηρίζονται από το HP Client Security:

- Κάρτες μνήμης χωρίς επαφή HID iCLASS
- Κάρτες μνήμης χωρίς επαφή MiFare Classic 1k, 4k και mini

Οι ακόλουθες μορφές καρτών προσέγγισης υποστηρίζονται από το HP Client Security:

- Κάρτες εγγύτητας HID

Για να δηλώσετε μια έξυπνη κάρτα:

1. Εισαγάγετε την κάρτα σε έναν προσαρτημένο αναγνώστη έξυπνων καρτών.
2. Όταν η κάρτα αναγνωριστεί, καταχωρήστε τον κωδικό PIN της κάρτας και, στη συνέχεια, κάντε κλικ ή πατήστε **Enroll** (Δήλωση).

Για να αλλάξετε τον κωδικό PIN μιας έξυπνης κάρτας:

1. Εισαγάγετε την κάρτα σε έναν προσαρτημένο αναγνώστη έξυπνων καρτών.
2. Όταν η κάρτα αναγνωριστεί, εισαγάγετε τον κωδικό PIN της κάρτας και στη συνέχεια κάντε κλικ ή πατήστε στην επιλογή **Authenticate** (Έλεγχος ταυτότητας).
3. Κάντε κλικ ή πατήστε στην επιλογή **Change PIN** (Αλλαγή κωδικού PIN) και πληκτρολογήστε το νέο κωδικό PIN.

Για να δηλώσετε μια κάρτα χωρίς επαφή ή μια κάρτα εγγύτητας:

1. Τοποθετήστε την κάρτα πάνω ή πολύ κοντά στον κατάλληλο αναγνώστη.
2. Όταν η κάρτα αναγνωριστεί κάντε κλικ ή πατήστε στην επιλογή **Enroll** (Δήλωση).

Για να διαγράψετε μια δηλωμένη κάρτα:

1. Παρουσιάστε την κάρτα στον αναγνώστη.
2. Μόνο για έξυπνες κάρτες, πληκτρολογήστε τον κωδικό PIN της κάρτας και κάντε κλικ ή πατήστε στην επιλογή **Authenticate** (Έλεγχος ταυτότητας).
3. Κάντε κλικ ή πατήστε στην επιλογή **Delete** (Διαγραφή).

Μετά τη δήλωση της κάρτας μπορείτε να δείτε λεπτομέρειες σχετικά με την κάρτα στην επιλογή **Enrolled Cards** (Δηλωμένες κάρτες). Όταν η κάρτα διαγραφεί, αφαιρείται από τη λίστα.

Για να αποκτήσετε πρόσβαση στις ρυθμίσεις μιας κάρτας εγγύτητας, χωρίς επαφή ή έξυπνης κάρτας, όπου οι διαχειριστές μπορούν να καθορίσουν ρυθμίσεις που σχετίζονται με τα διαπιστευτήρια της κάρτας, κάντε κλικ ή πατήστε στην επιλογή **Settings** (Ρυθμίσεις) (απαιτούνται δικαιώματα διαχειριστή).

Ρυθμίσεις κάρτας εγγύτητας, χωρίς επαφή ή έξυπνης κάρτας

Για πρόσβαση στις ρυθμίσεις μιας κάρτας, κάντε κλικ ή πατήστε στην κάρτα στη λίστα και, στη συνέχεια, κάντε κλικ ή πατήστε στο βέλος που εμφανίζεται.

Για να αλλάξετε τον κωδικό PIN μιας έξυπνης κάρτας:

1. Παρουσιάστε την κάρτα στον αναγνώστη
2. Πληκτρολογήστε τον κωδικό PIN της κάρτας και κάντε κλικ ή πατήστε στην επιλογή **Continue** (Συνέχεια).
3. Πληκτρολογήστε και επιβεβαιώστε το νέο κωδικό PIN και κάντε κλικ ή πατήστε στην επιλογή **Continue** (Συνέχεια).

Για να προετοιμάσετε τον κωδικό PIN μιας έξυπνης κάρτας:

1. Παρουσιάστε την κάρτα στον αναγνώστη
2. Πληκτρολογήστε τον κωδικό PIN της κάρτας και κάντε κλικ ή πατήστε στην επιλογή **Continue** (Συνέχεια).
3. Πληκτρολογήστε και επιβεβαιώστε το νέο κωδικό PIN και κάντε κλικ ή πατήστε στην επιλογή **Continue** (Συνέχεια).
4. Κάντε κλικ ή πατήστε στο **Yes** (Ναι) για να επιβεβαιώσετε την προετοιμασία.

Για να διαγράψετε τα δεδομένα της κάρτας:

1. Παρουσιάστε την κάρτα στον αναγνώστη
2. Πληκτρολογήστε τον κωδικό PIN της κάρτας (μόνο για έξυπνες κάρτες) και, στη συνέχεια, κάντε κλικ ή πατήστε στην επιλογή **Continue** (Συνέχεια).
3. Κάντε κλικ ή πατήστε **Yes** (Ναι) για να επιβεβαιώσετε τη διαγραφή.

PIN

Αν ο διαχειριστής έχει ενεργοποιήσει τον κωδικό PIN ως διαπιστευτήριο ελέγχου ταυτότητας, μπορείτε να εγκαταστήσετε ένα PIN σε συνδυασμό με άλλα διαπιστευτήρια για πρόσθετη ασφάλεια.

Για να εγκαταστήσετε ένα νέο κωδικό PIN:

▲ Πληκτρολογήστε το PIN, πληκτρολογήστε το ξανά για επιβεβαίωση και κάντε κλικ ή πατήστε στην επιλογή **Apply** (Εφαρμογή).

Για να διαγράψετε έναν κωδικό PIN:

▲ Κάντε κλικ ή πατήστε **Delete** (Διαγραφή) και, στη συνέχεια, κάντε κλικ ή πατήστε **Yes** (Ναι) για επιβεβαίωση.

Για να αποκτήσετε πρόσβαση στις ρυθμίσεις κωδικού PIN, όπου οι διαχειριστές μπορούν να καθορίσουν ρυθμίσεις που σχετίζονται με τα διαπιστευτήρια PIN, κάντε κλικ ή πατήστε στην επιλογή **Settings** (Ρυθμίσεις) (απαιτούνται δικαιώματα διαχειριστή).

Ρυθμίσεις PIN

Στη σελίδα Ρυθμίσεις κωδικού PIN, μπορείτε να καθορίσετε το ελάχιστο και το μέγιστο αποδεκτό μήκος για το διαπιστευτήριο PIN.

RSA SecurID

Μπορείτε να δηλώσετε ή να διαγράψετε ένα διαπιστευτήριο RSA SecurID, αν ο διαχειριστής έχει ενεργοποιήσει το RSA ως διαπιστευτήριο ελέγχου ταυτότητας και ισχύουν οι ακόλουθες συνθήκες,

ΣΗΜΕΙΩΣΗ Απαιτείται κατάλληλη εγκατάσταση.

- Ο χρήστης πρέπει να έχει δημιουργηθεί σε ένα διακομιστή RSA.
- Το διακριτικό RSA SecurID που έχει εκχωρηθεί στο χρήστη και ο υπολογιστής πρέπει να συμμετέχουν στον τομέα του διακομιστή RSA.
- Το λογισμικό SecurID είναι εγκατεστημένο στον υπολογιστή.
- Είναι διαθέσιμη μια σύνδεση στον κατάλληλα διαμορφωμένο διακομιστή RSA.

Για να δηλώσετε ένα διαπιστευτήριο RSA SecurID:

▲ Πληκτρολογήστε το όνομα χρήστη και τον κωδικό πρόσβασης του RSA SecurID (κωδικός διακριτικού RSA SecurID ή κωδικός PIN+διακριτικού, ανάλογα με το περιβάλλον σας) και, στη συνέχεια, κάντε κλικ ή πατήστε στην επιλογή **Apply** (Εφαρμογή).

Μετά την επιτυχή δήλωση, εμφανίζεται το μήνυμα, “Your RSA SecurID credential has been successfully enrolled” (Επιτυχής δήλωση του πιστοποιητικού RSA SecurID) και ενεργοποιείται το κουμπί Διαγραφή.

Για να διαγράψετε ένα διαπιστευτήριο RSA SecurID:

▲ Κάντε κλικ στην επιλογή **Delete** (Διαγραφή) και στη συνέχεια επιλέξτε **Yes** (Ναι) στον αναδυόμενο διάλογο που θέτει την ερώτηση “Are you sure you want to delete your RSA SecurID credential?” (Θέλετε σίγουρα να διαγράψετε το διαπιστευτήριο RSA SecurID;)

Password Manager

Η σύνδεση σε ιστότοπους και εφαρμογές είναι ευκολότερη και πιο ασφαλής όταν χρησιμοποιείτε το Password Manager. Μπορείτε να δημιουργήσετε πιο ισχυρούς κωδικούς πρόσβασης που δεν χρειάζεται να τους σημειώσετε ή να τους θυμάστε και στη συνέχεια να συνδέεστε εύκολα και γρήγορα με ένα δακτυλικό αποτύπωμα, μια έξυπνη κάρτα, μια κάρτα εγγύτητας, ένα τηλέφωνο Bluetooth, τον κωδικό PIN, το διαπιστευτήριο RSA ή τον κωδικό πρόσβασης των Windows.

ΣΗΜΕΙΩΣΗ Λόγω της διαρκούς αλλαγής της δομής των οθονών σύνδεσης Web, το Password Manager ενδέχεται να μην μπορεί να υποστηρίζει πάντα όλους τους ιστότοπους.

Το Password Manager προσφέρει τις ακόλουθες επιλογές:

Σελίδα Password Manager

- Κάντε κλικ ή πατήστε σε ένα λογαριασμό για να εκκινήσετε αυτόματα μια σελίδα web ή μια εφαρμογή και να συνδεθείτε.
- Χρήση κατηγοριών για την οργάνωση των λογαριασμών σας.

Ισχύς κωδικού πρόσβασης

- Δείτε με μια ματιά αν κάποιος από τους κωδικούς πρόσβασης εμφανίζει κίνδυνο ασφάλειας.
- Όταν προσθέτετε δεδομένα σύνδεσης, ελέγξτε την ισχύ των ανεξάρτητων κωδικών πρόσβασης που χρησιμοποιούνται για ιστότοπους και εφαρμογές.
- Η ισχύς του κωδικού πρόσβασης απεικονίζεται με ενδείξεις κατάστασης σε κόκκινο, κίτρινο ή πράσινο χρώμα.

Το εικονίδιο του **Password Manager** εμφανίζεται στην πάνω αριστερή γωνία της σελίδας Web ή της οθόνης σύνδεσης σε μια εφαρμογή. Όταν δεν έχει δημιουργηθεί ακόμη σύνδεση για αυτόν τον ιστότοπο ή την εφαρμογή, εμφανίζεται το σύμβολο πρόσθεσης στο εικονίδιο.

▲ Κάντε κλικ ή πατήστε στο εικονίδιο του **Password Manager** για να εμφανιστεί ένα μενού περιβάλλοντος όπου μπορείτε να επιλέξετε από τα ακόλουθα:

- Προσθήκη [somedomain.com] στο Password Manager
- Άνοιγμα του Password Manager
- Ρυθμίσεις εικονιδίου
- Βοήθεια

Για ιστοσελίδες ή προγράμματα όπου δεν έχει δημιουργηθεί ακόμη σύνδεση

Οι ακόλουθες επιλογές εμφανίζονται στο μενού περιβάλλοντος:

- **Add [somedomain.com] to the Password Manager** (Προσθήκη [somedomain.com] στο Password Manager)—Σας επιτρέπει να προσθέσετε μια σύνδεση στην τρέχουσα οθόνη σύνδεσης.
- **Open Password Manager** (Άνοιγμα του Password Manager)—Εκκινεί το Password Manager.

- **Icon Settings** (Ρυθμίσεις εικονιδίου)—Σας επιτρέπει να καθορίζετε τις καταστάσεις στις οποίες θα εμφανίζεται το εικονίδιο του **Password Manager**.
- **Help** (Βοήθεια)—Εμφανίζει τη Βοήθεια του HP Client Security.

Για ιστοσελίδες ή προγράμματα όπου έχει ήδη δημιουργηθεί σύνδεση

Οι ακόλουθες επιλογές εμφανίζονται στο μενού περιβάλλοντος:

- **Fill in logon data** (Συμπλήρωση δεδομένων σύνδεσης)—Εμφανίζει τη σελίδα **Verify your identity** (Επαλήθευση ταυτότητας). Μετά από τον επιτυχή έλεγχο ταυτότητας, τα δεδομένα σύνδεσης τοποθετούνται στα πεδία σύνδεσης και η σελίδα υποβάλλεται (αν η υποβολή έχει καθοριστεί όταν δημιουργήθηκε η σύνδεση ή κατά την τελευταία τροποποίηση).
- **Edit Logon** (Επεξεργασία σύνδεσης)—Σας επιτρέπει να τροποποιείτε τα δεδομένα σύνδεσης για αυτόν τον ιστότοπο.
- **Add Logon** (Προσθήκη σύνδεσης)—Σας επιτρέπει να προσθέσετε ένα λογαριασμό στο Password Manager.
- **Open Password Manager** (Άνοιγμα του Password Manager)—Εκκινεί το Password Manager.
- **Help** (Βοήθεια)—Εμφανίζει τη Βοήθεια του HP Client Security.

ΣΗΜΕΙΩΣΗ Ο διαχειριστής του υπολογιστή ενδέχεται να έχει διαμορφώσει το HP Client Security έτσι ώστε να απαιτούνται περισσότερα του ενός διαπιστευτήρια κατά την επαλήθευση της ταυτότητας.

Προσθήκη συνδέσεων

Μπορείτε να προσθέσετε εύκολα μια σύνδεση για έναν ιστότοπο ή ένα πρόγραμμα εισάγοντας μία φορά τις πληροφορίες σύνδεσης. Από εκείνη τη στιγμή, το Password Manager εισάγει για εσάς τις πληροφορίες. Μπορείτε να χρησιμοποιήσετε αυτές τις συνδέσεις μετά από περιήγηση στον ιστότοπο ή στο πρόγραμμα.

Για να προσθέσετε μια σύνδεση:

1. Ανοίξτε την οθόνη σύνδεσης για έναν ιστότοπο ή ένα πρόγραμμα.
2. Κάντε κλικ ή πατήστε στο εικονίδιο του **Password Manager** και στη συνέχεια κάντε κλικ ή πατήστε σε ένα από τα ακόλουθα, ανάλογα με το αν η οθόνη σύνδεσης είναι για ιστότοπο ή για πρόγραμμα:
   - Για ιστότοπο, κάντε κλικ ή πατήστε στην επιλογή **Add [domain name] to Password Manager** (Προσθήκη [όνομα τομέα] στο Password Manager).
   - Για πρόγραμμα, κάντε κλικ ή πατήστε στην επιλογή **Add this logon screen to Password Manager** (Προσθήκη αυτής της οθόνης σύνδεσης στο Password Manager).
3. Εισαγάγετε τα δεδομένα σύνδεσης. Τα πεδία σύνδεσης στην οθόνη και τα αντίστοιχα πεδία στο πλαίσιο διαλόγου προσδιορίζονται με ένα έντονο πορτοκαλί πλαίσιο.
   α. Για να συμπληρώσετε ένα πεδίο σύνδεσης με μια από τις προδιαμορφωμένες επιλογές, κάντε κλικ ή πατήστε στα βέλη στα δεξιά του πεδίου.
   β. Για να δείτε τον κωδικό πρόσβασης για αυτή τη σύνδεση, κάντε κλικ ή πατήστε στην επιλογή **Show password** (Εμφάνιση κωδικού πρόσβασης).
   γ. Για να συμπληρώσετε τα πεδία σύνδεσης, αλλά να μην τα υποβάλλετε, καταργήστε την επιλογή του πλαισίου ελέγχου **Automatically submit logon data** (Αυτόματη υποβολή δεδομένων σύνδεσης).

δ. Κάντε κλικ ή πατήστε στο **OK** για να επιλέξετε τη μέθοδο ελέγχου ταυτότητας που θέλετε να χρησιμοποιήσετε (δακτυλικά αποτυπώματα, έξυπνη κάρτα, κάρτα εγγύτητας, κάρτα χωρίς επαφή, τηλέφωνο Bluetooth, κωδικό PIN ή κωδικό πρόσβασης) και στη συνέχεια συνδεθείτε με την επιλεγμένη μέθοδο ελέγχου ταυτότητας.

   Το σύμβολο πρόσθεσης αφαιρείται από το εικονίδιο του **Password Manager** για να σας ενημερώσει ότι έχει δημιουργηθεί η σύνδεση.

ε. Αν το Password Manager δεν εντοπίσει τα πεδία σύνδεσης, κάντε κλικ ή πατήστε στην επιλογή **More fields** (Περισσότερα πεδία).

   - Επιλέξτε το πλαίσιο ελέγχου για κάθε πεδίο που απαιτείται για τη σύνδεση ή καταργήστε την επιλογή του πλαισίου ελέγχου για κάθε πεδίο που δεν απαιτείται για τη σύνδεση.
   - Κάντε κλικ ή πατήστε **Close** (Κλείσιμο).

Κάθε φορά που αποκτάτε πρόσβαση στον ιστότοπο ή ανοίγετε το πρόγραμμα, το εικονίδιο του **Password Manager** εμφανίζεται στην πάνω αριστερή γωνία της οθόνης σύνδεσης στον ιστότοπο ή στην εφαρμογή, υποδεικνύοντας ότι μπορείτε να χρησιμοποιήσετε τα καταχωρημένα διαπιστευτήρια για να συνδεθείτε.

Επεξεργασία συνδέσεων

Για να τροποποιήσετε μια σύνδεση:

1. Ανοίξτε την οθόνη σύνδεσης για έναν ιστότοπο ή ένα πρόγραμμα.
2. Για να εμφανιστεί το πλαίσιο διαλόγου όπου μπορείτε να επεξεργαστείτε τις πληροφορίες σύνδεσης, κάντε κλικ ή πατήστε στο εικονίδιο του **Password Manager** και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Edit Logon** (Επεξεργασία σύνδεσης).

   Τα πεδία σύνδεσης στην οθόνη και τα αντίστοιχα πεδία στο πλαίσιο διαλόγου προσδιορίζονται με ένα έντονο πορτοκαλί πλαίσιο.

   Μπορείτε επίσης να επεξεργαστείτε πληροφορίες λογαριασμού από τη σελίδα του Password Manager, κάνοντας κλικ ή πατώντας στη σύνδεση για να εμφανιστούν οι επιλογές επεξεργασίας και, στη συνέχεια, επιλέξτε **Edit** (Επεξεργασία).
3. Τροποποιήστε τις πληροφορίες σύνδεσης.
   - Για να τροποποιήσετε το **Account name** (Όνομα λογαριασμού), πληκτρολογήστε ένα νέο όνομα στο πεδίο.
   - Για να προσθέσετε ή να τροποποιήσετε το όνομα για την επιλογή **Category** (Κατηγορία), πληκτρολογήστε ή τροποποιήστε το όνομα στο πεδίο **Category** (Κατηγορία).
   - Για να επιλέξετε ένα πεδίο σύνδεσης **Username** (Όνομα χρήστη) με μια από τις προδιαμορφωμένες επιλογές, κάντε κλικ ή πατήστε στο κάτω βέλος δεξιά του πεδίου.

     Οι προδιαμορφωμένες επιλογές είναι διαθέσιμες μόνο όταν τροποποιείτε τη σύνδεση από την εντολή Επεξεργασία στο μενού περιβάλλοντος του εικονιδίου του Password Manager.
   - Για να επιλέξετε το πεδίο σύνδεσης **Password** (Κωδικός πρόσβασης) με μια από τις προδιαμορφωμένες επιλογές, κάντε κλικ ή πατήστε στο κάτω βέλος δεξιά του πεδίου.

     Οι προδιαμορφωμένες επιλογές είναι διαθέσιμες μόνο όταν τροποποιείτε τη σύνδεση από την εντολή Επεξεργασία στο μενού περιβάλλοντος του εικονιδίου του Password Manager.
   - Για να προσθέσετε πεδία από την οθόνη στη σύνδεση, κάντε κλικ ή πατήστε στο **More fields** (Περισσότερα πεδία).

- Για να δείτε τον κωδικό πρόσβασης για αυτή τη σύνδεση, κάντε κλικ ή πατήστε στο εικονίδιο **Show password** (Εμφάνιση κωδικού πρόσβασης).
- Για να συμπληρώσετε τα πεδία σύνδεσης, αλλά να μην τα υποβάλλετε, καταργήστε την επιλογή του πλαισίου ελέγχου **Automatically submit logon data** (Αυτόματη υποβολή δεδομένων σύνδεσης).
- Για να σημειώσετε αυτή τη σύνδεση ως συμβιβαστικό κωδικό πρόσβασης, επιλέξτε το πλαίσιο ελέγχου **This password is compromised** (Αυτός είναι συμβιβαστικός κωδικός πρόσβασης).

  Αφού αποθηκεύσετε τις αλλαγές, όλες οι άλλες συνδέσεις που μοιράζονται τον ίδιο κωδικό πρόσβασης θα σημειωθούν επίσης ως συμβιβαστικές. Μπορείτε στη συνέχεια να επισκεφτείτε κάθε λογαριασμό που επηρεάζεται και να αλλάξετε τους κωδικούς πρόσβασης ανάλογα με τις ανάγκες.

4. Κάντε κλικ ή πατήστε στο **OK**.

Χρήση του μενού Password Manager Quick Links

Το Password Manager παρέχει ένα γρήγορο και εύκολο τρόπο εκκίνησης των ιστότοπων και των προγραμμάτων για τα οποία έχετε δημιουργήσει συνδέσεις. Κάντε διπλό κλικ ή διπλό πάτημα σε μια σύνδεση προγράμματος ή ιστότοπου από το μενού **Password Manager Quick Links** ή από τη σελίδα του Password Manager στο HP Client Security, για να ανοίξετε την οθόνη σύνδεσης και συμπληρώστε τα δεδομένα σύνδεσης.

Όταν δημιουργείτε μια σύνδεση, προστίθεται αυτόματα στο μενού **Quick Links** του Password Manager.

Για να εμφανίσετε το μενού **Quick Links**:

▲ Πατήστε τον συνδυασμό πλήκτρων του **Password Manager** (Ctrl+πλήκτρο των Windows+h είναι η εργοστασιακή ρύθμιση). Για να αλλάξετε το συνδυασμό πλήκτρων πρόσβασης, από την αρχική σελίδα του HP Client Security, κάντε κλικ στο **Password Manager** και στη συνέχεια κάντε κλικ ή πατήστε στην επιλογή **Settings** (Ρυθμίσεις).

Οργάνωση των συνδέσεων σε κατηγορίες

Δημιουργήστε μια ή περισσότερες κατηγορίες για να διατηρείτε σε τάξη τις συνδέσεις σας.

Για να εκχωρήσετε μια σύνδεση σε μια κατηγορία:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο **Password Manager**.
2. Κάντε κλικ ή πατήστε σε μια καταχώρηση λογαριασμού και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Edit** (Επεξεργασία).
3. Στο πεδίο **Category** (Κατηγορία), πληκτρολογήστε ένα όνομα κατηγορίας.
4. Κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση).

Για να αφαιρέσετε ένα λογαριασμό από μια κατηγορία:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο **Password Manager**.
2. Κάντε κλικ ή πατήστε σε μια καταχώρηση λογαριασμού και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Edit** (Επεξεργασία).
3. Στο πεδίο **Category** (Κατηγορία), διαγράψτε το όνομα κατηγορίας.
4. Κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση).

Για να μετονομάσετε μια κατηγορία:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο **Password Manager**.
2. Κάντε κλικ ή πατήστε σε μια καταχώρηση λογαριασμού και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Edit** (Επεξεργασία).
3. Στο πεδίο **Category** (Κατηγορία), αλλάξτε το όνομα της κατηγορίας.
4. Κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση).

Διαχείριση των συνδέσεων

Το Password Manager σάς επιτρέπει να διαχειρίζεστε τις πληροφορίες σύνδεσης για ονόματα χρηστών, κωδικούς πρόσβασης και πολλαπλούς λογαριασμούς σύνδεσης από μια κεντρική τοποθεσία.

Οι συνδέσεις σας εμφανίζονται στη σελίδα του Password Manager.

Για να διαχειριστείτε τις συνδέσεις σας:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο **Password Manager**.
2. Κάντε κλικ ή πατήστε σε μια υπάρχουσα σύνδεση και, στη συνέχεια, επιλέξτε μια από τις παρακάτω επιλογές και ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη:
   - **Edit** (Επεξεργασία)—Τροποποίηση μιας σύνδεσης. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Επεξεργασία συνδέσεων στη σελίδα 23.
   - **Log in** (Σύνδεση)—Σύνδεση στον επιλεγμένο λογαριασμό.
   - **Delete** (Διαγραφή)—Διαγραφή της σύνδεσης για τον επιλεγμένο λογαριασμό.

Για να προσθέσετε μια ακόμη σύνδεση για ιστότοπο ή πρόγραμμα:

1. Ανοίξτε την οθόνη σύνδεσης για τον ιστότοπο ή το πρόγραμμα.
2. Κάντε κλικ ή πατήστε στο εικονίδιο του **Password Manager** για να εμφανίσετε το μενού περιβάλλοντος.
3. Κάντε κλικ ή πατήστε στο **Add Logon** (Προσθήκη σύνδεσης) και ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Αξιολόγηση της ισχύος του κωδικού πρόσβασης

Η χρήση ισχυρών κωδικών πρόσβασης για σύνδεση στους ιστότοπους και τα προγράμματα είναι σημαντική για την προστασία της ταυτότητάς σας.

Το Password Manager διευκολύνει την παρακολούθηση και τη βελτίωση της ασφάλειάς σας με στιγμιαία και αυτόματη ανάλυση της ισχύος καθενός από τους κωδικούς πρόσβασης που χρησιμοποιούνται για σύνδεση στους ιστότοπους και τα προγράμματα.

Καθώς πληκτρολογείτε τον κωδικό πρόσβασης κατά τη δημιουργία μιας σύνδεσης στο Password Manager, εμφανίζεται μια έγχρωμη γραμμή κάτω από τον κωδικό πρόσβασης που υποδεικνύει την ισχύ του κωδικού πρόσβασης. Τα χρώματα υποδεικνύουν τις ακόλουθες τιμές:

- **Red** (Κόκκινο)—Ασθενές
- **Yellow** (Κίτρινο)—Μέτριο
- **Green** (Πράσινο)—Ισχυρό

Ρυθμίσεις του εικονιδίου του Password Manager

Το Password Manager επιχειρεί να ταυτοποιήσει τις οθόνες σύνδεσης για ιστότοπους και προγράμματα. Όταν εντοπίζει μια οθόνη σύνδεσης για την οποία δεν έχετε δημιουργήσει μια σύνδεση, το Password Manager σάς ζητά να προσθέσετε μια σύνδεση για την οθόνη εμφανίζοντας το εικονίδιο του **Password Manager** με το σύμβολο πρόσθεσης.

1. Κάντε κλικ ή πατήστε στο εικονίδιο και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Icon Settings** (Ρυθμίσεις εικονιδίου) για να προσαρμόσετε τον τρόπο με τον οποίο το Password Manager χειρίζεται πιθανούς ιστότοπους σύνδεσης.
   - **Prompt to add logons for logon screens** (Ερώτηση για προσθήκη συνδέσεων για οθόνες συνδέσεων)—Κάντε κλικ ή πατήστε σε αυτή την επιλογή για να σας ζητήσει το Password Manager να προσθέσετε μια σύνδεση όταν εμφανίζεται μια οθόνη σύνδεσης που δεν διαθέτει ήδη εγκατεστημένη σύνδεση.
   - **Exclude this screen** (Εξαίρεση αυτής της οθόνης)—Επιλέξτε το πλαίσιο ελέγχου έτσι ώστε το Password Manager να μην σας ζητήσει ξανά να προσθέσετε σύνδεση για αυτή την οθόνη σύνδεσης.
   - **Do not prompt to add logons for logon screens** (Να μην ζητείται η προσθήκη συνδέσεων για οθόνες σύνδεσης)—Επιλέξτε το κουμπί επιλογής.
2. Για να προσθέσετε μια σύνδεση για μια οθόνη που έχει προηγουμένως εξαιρεθεί:
   α. Συνδεθείτε στον ιστότοπο που έχει προηγουμένως εξαιρεθεί.
   β. Για να θυμάται το Password Manager τον κωδικό πρόσβασης για αυτήν την τοποθεσία, κάντε κλικ ή πατήστε **Απομνημόνευση** στο αναδυόμενο παράθυρο διαλόγου για να αποθηκεύσετε τον κωδικό πρόσβασης και να δημιουργήσετε μια σύνδεση για την οθόνη.
3. Για πρόσβαση σε περισσότερες ρυθμίσεις του Password Manager, κάντε κλικ ή πατήστε στο εικονίδιο του Password Manager, κάντε κλικ ή πατήστε στο **Open Password Manager** (Άνοιγμα του Password Manager) και κάντε κλικ ή πατήστε στο **Settings** (Ρυθμίσεις) στη σελίδα του Password Manager.

Εισαγωγή και εξαγωγή συνδέσεων

Στη σελίδα Εισαγωγή και Εξαγωγή του HP Password Manager μπορείτε να εισάγετε συνδέσεις αποθηκευμένες από εφαρμογές περιήγησης στο web στον υπολογιστή σας. Μπορείτε επίσης να εισάγετε δεδομένα από ένα αντίγραφο ασφαλείας αρχείου του HP Client Security και να εξάγετε τα δεδομένα σε ένα αντίγραφο ασφαλείας αρχείου του HP Client Security.

▲ Για να εκκινήσετε τη σελίδα εισαγωγής και εξαγωγής, κάντε κλικ ή πατήστε στο **Import and export** (Εισαγωγή και εξαγωγή) στη σελίδα του Password Manager.

Για να εισάγετε κωδικούς πρόσβασης από μια εφαρμογή περιήγησης:

1. Κάντε κλικ ή πατήστε στην εφαρμογή περιήγησης από την οποία θέλετε να εισάγετε κωδικούς πρόσβασης (εμφανίζονται μόνο οι εγκατεστημένες εφαρμογές περιήγησης).
2. Καταργήστε την επιλογή από το πλαίσιο ελέγχου για λογαριασμούς για τους οποίους δεν θέλετε να εισάγετε κωδικούς πρόσβασης.
3. Κάντε κλικ ή πατήστε **Εισαγωγή**.

Η εισαγωγή δεδομένων από, ή η εξαγωγή δεδομένων σε, αντίγραφο ασφαλείας αρχείου του HP Client Security μπορεί να πραγματοποιηθεί μέσω των σχετικών συνδέσμων (στην επιλογή **Other Options)** (Άλλες επιλογές) στη σελίδα εισαγωγής και εξαγωγής.

ΣΗΜΕΙΩΣΗ Αυτή η λειτουργία εισάγει και εξάγει μόνο δεδομένα του Password Manager. Για πληροφορίες σχετικά με τη δημιουργία αντιγράφων ασφαλείας και την επαναφορά πρόσθετων δεδομένων του HP Client Security, βλ. Δημιουργία αντιγράφων ασφαλείας και επαναφορά των δεδομένων στη σελίδα 31.

Για εισαγωγή δεδομένων από ένα αντίγραφο ασφαλείας αρχείου του HP Client Security:

1. Από τη σελίδα Εισαγωγή και Εξαγωγή του HP Password Manager, κάντε κλικ ή πατήστε στο **Import data from an HP Client Security backup file** (Εισαγωγή δεδομένων από ένα αντίγραφο ασφαλείας αρχείου του HP Client Security).
2. Επιβεβαιώστε την ταυτότητά σας.
3. Επιλέξτε το αντίγραφο ασφαλείας αρχείου που έχει δημιουργηθεί προηγουμένως ή πληκτρολογήστε τη διαδρομή στο πεδίο που παρέχεται και στη συνέχεια κάντε κλικ ή πατήστε στην επιλογή **Browse** (Αναζήτηση).
4. Πληκτρολογήστε τον κωδικό πρόσβασης που χρησιμοποιείται για προστασία του αρχείου και κάντε κλικ ή πατήστε στο **Next** (Επόμενο).
5. Κάντε κλικ ή πατήστε στο **Restore** (Επαναφορά).

Για να εξάγετε δεδομένα σε ένα αντίγραφο ασφαλείας αρχείου του HP Client Security:

1. Από τη σελίδα Εισαγωγή και Εξαγωγή του HP Password Manager, κάντε κλικ ή πατήστε στο **Export data from an HP Client Security backup file** (Εξαγωγή δεδομένων από ένα αντίγραφο ασφαλείας αρχείου του HP Client Security).
2. Επιβεβαιώστε την ταυτότητά σας και κάντε κλικ ή πατήστε στο **Next** (Επόμενο).
3. Πληκτρολογήστε το όνομα του αντιγράφου ασφαλείας αρχείου. Από προεπιλογή, το αρχείο αποθηκεύεται στο φάκελο Έγγραφα. Για να καθορίσετε μια διαφορετική τοποθεσία κάντε κλικ ή πατήστε στο **Browse** (Αναζήτηση).
4. Πληκτρολογήστε και επιβεβαιώστε τον κωδικό πρόσβασης που χρησιμοποιείται για την προστασία του αρχείου και κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση).

Ρυθμίσεις

Μπορείτε να ορίσετε ρυθμίσεις για την προσαρμογή του Password Manager στις προτιμήσεις σας:

- **Prompt to add logons for logon screens** (Να ζητείται η προσθήκη συνδέσεων για οθόνες συνδέσεων)—Το εικονίδιο του **Password Manager** με το σύμβολο πρόσθεσης εμφανίζεται όποτε εντοπίζεται μια οθόνη σύνδεσης σε έναν ιστότοπο ή σε ένα πρόγραμμα, υποδεικνύοντας ότι μπορείτε να προσθέσετε μια σύνδεση για αυτή την οθόνη στο μενού **Logons** (Συνδέσεις).

  Για να απενεργοποιήσετε αυτή τη λειτουργία, καταργήστε την επιλογή από το πλαίσιο ελέγχου δίπλα στο **Prompt to add logons for logon screens** (Να ζητείται η προσθήκη συνδέσεων για οθόνες συνδέσεων).

- **Ανοίξτε το Password Manager με το Ctrl+Win+h**—Ο προεπιλεγμένος συνδυασμός πλήκτρων που ανοίγει το μενού **Γρήγορες συνδέσεις του Password Manager** είναι Ctrl+πλήκτρο των Windows+h.

  Για να αλλάξετε το συνδυασμό πλήκτρων, κάντε κλικ ή πατήστε σε αυτή την επιλογή και στη συνέχεια πληκτρολογήστε ένα νέο συνδυασμό πλήκτρων. Οι συνδυασμοί ενδέχεται να περιλαμβάνουν ένα ή περισσότερα από τα ακόλουθα: ctrl, alt ή shift και οποιοδήποτε αλφαβητικό ή αριθμητικό πλήκτρο.

  Οι συνδυασμοί που είναι δεσμευμένοι για τα Windows ή τις εφαρμογές Windows δεν μπορούν να χρησιμοποιηθούν.

- Για να επιστρέψετε τις ρυθμίσεις στις εργοστασιακά προεπιλεγμένες κάντε κλικ ή πατήστε στο **Restore defaults** (Επαναφορά προεπιλογών).

Ρυθμίσεις για προχωρημένους

Οι διαχειριστές μπορούν να αποκτήσουν πρόσβαση στις ακόλουθες εφαρμογές επιλέγοντας το εικονίδιο **Gear** (ρυθμίσεις) στην αρχική σελίδα του HP Client Security.

- **Administrator Policies** (Πολιτικές διαχειριστή)—Σας επιτρέπει να διαμορφώσετε τις ρυθμίσεις για τις πολιτικές σύνδεσης και περιόδων λειτουργίας για διαχειριστές.
- **Standard User Policies** (Πολιτικές τυπικών χρηστών)—Σας επιτρέπει να διαμορφώσετε τις ρυθμίσεις για τις πολιτικές σύνδεσης και περιόδων λειτουργίας για τυπικούς χρήστες.
- **Security Features** (Λειτουργίες ασφαλείας)—Σας επιτρέπει να αυξήσετε την ασφάλεια του υπολογιστή προστατεύοντας το λογαριασμό Windows με χρήση ισχυρού ελέγχου ταυτότητας ή/και με την ενεργοποίηση του ελέγχου ταυτότητας πριν από την εκκίνηση των Windows.
- **Χρήστες**—Επιτρέπει τη διαχείριση χρηστών και τις πιστοποιήσεις τους.
- **My Policies** (Οι πολιτικές μου)—Σας επιτρέπει να κάνετε επισκόπηση των πολιτικών ελέγχου ταυτότητας και της κατάστασης δήλωσης.
- **Backup and Restore** (Δημιουργία αντιγράφου ασφαλείας και επαναφορά)—Σας επιτρέπει να δημιουργείτε αντίγραφα ασφαλείας ή να επαναφέρετε τα δεδομένα του HP Client Security.
- **Σχετικά με το HP Client Security**—Εμφανίζει πληροφορίες έκδοσης για HP Client Security.

Πολιτικές διαχειριστή

Μπορείτε να διαμορφώσετε τις ρυθμίσεις για τις πολιτικές σύνδεσης και τις περιόδους λειτουργίας για τους διαχειριστές αυτού του υπολογιστή. Οι πολιτικές σύνδεσης που ορίζονται εδώ διέπουν τα διαπιστευτήρια που απαιτούνται για έναν τοπικό διαχειριστή για να συνδεθεί στα Windows. Οι πολιτικές περιόδων λειτουργίας που ορίζονται εδώ διέπουν τα διαπιστευτήρια που απαιτούνται για

έναν τοπικό διαχειριστή για την επιβεβαίωση ταυτότητας μέσα σε μια περίοδο λειτουργίας των Windows.

Από προεπιλογή, όλες οι νέες ή τροποποιημένες πολιτικές τίθενται σε ισχύ αμέσως μετά το πάτημα ή το κλικ στην επιλογή **Apply** (Εφαρμογή).

Για να προσθέσετε μια νέα πολιτική:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Administrator Policies** (Πολιτικές διαχειριστή).
3. Κάντε κλικ ή πατήστε στο **Add new policy** (Προσθήκη νέας πολιτικής).
4. Κάντε κλικ στα κάτω βέλη για να επιλέξετε κύρια και (προαιρετικά) δευτερεύοντα διαπιστευτήρια για τη νέα πολιτική και στη συνέχεια κάντε κλικ ή πατήστε στο **Add** (Προσθήκη).
5. Κάντε κλικ στο κουμπί **Εφαρμογή**.

Για να καθυστερήσετε την έναρξη ισχύος μιας νέας ή τροποποιημένης πολιτικής:

1. Κάντε κλικ ή πατήστε στην επιλογή **Enforce this policy immediately** (Άμεση ισχύς αυτής της πολιτικής).
2. Επιλέξτε **Enforce this policy on the specific date** (Θέση σε ισχύ αυτής της πολιτικής μια συγκεκριμένη ημερομηνία).
3. Πληκτρολογήστε μια ημερομηνία ή χρησιμοποιήστε το αναδυόμενο ημερολόγιο για να επιλέξτε την ημερομηνία που πρέπει να τεθεί σε ισχύ αυτή η πολιτική.
4. Αν θέλετε, επιλέξτε πότε θα υπενθυμίσετε στους χρήστες για τη νέα πολιτική.
5. Κάντε κλικ στο κουμπί **Εφαρμογή**.

Πολιτικές τυπικών χρηστών

Μπορείτε να διαμορφώσετε τις ρυθμίσεις για τις πολιτικές σύνδεσης και τις περιόδους λειτουργίας για τους τυπικούς χρήστες αυτού του υπολογιστή. Οι πολιτικές σύνδεσης που ορίζονται εδώ διέπουν τα διαπιστευτήρια που απαιτούνται για έναν τυπικό χρήστη για να συνδεθεί στα Windows. Οι πολιτικές περιόδων λειτουργίας που ορίζονται εδώ διέπουν τα διαπιστευτήρια που απαιτούνται για έναν τυπικό χρήστη για την επιβεβαίωση ταυτότητας μέσα σε μια περίοδο λειτουργίας των Windows.

Από προεπιλογή, όλες οι νέες ή τροποποιημένες πολιτικές τίθενται σε ισχύ αμέσως μετά το πάτημα ή το κλικ στην επιλογή **Apply** (Εφαρμογή).

Για να προσθέσετε μια νέα πολιτική:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Standard User Policies** (Πολιτικές τυπικών χρηστών).
3. Κάντε κλικ ή πατήστε στο **Add new policy** (Προσθήκη νέας πολιτικής).
4. Κάντε κλικ στα κάτω βέλη για να επιλέξετε κύρια και (προαιρετικά) δευτερεύοντα διαπιστευτήρια για τη νέα πολιτική και στη συνέχεια κάντε κλικ ή πατήστε στο **Add** (Προσθήκη).
5. Κάντε κλικ στο κουμπί **Εφαρμογή**.

Για να καθυστερήσετε την έναρξη ισχύος μιας νέας ή τροποποιημένης πολιτικής:

1. Κάντε κλικ ή πατήστε στην επιλογή **Enforce this policy immediately** (Άμεση ισχύς αυτής της πολιτικής).
2. Επιλέξτε **Enforce this policy on the specific date** (Θέση σε ισχύ αυτής της πολιτικής μια συγκεκριμένη ημερομηνία).
3. Πληκτρολογήστε μια ημερομηνία ή χρησιμοποιήστε το αναδυόμενο ημερολόγιο για να επιλέξτε την ημερομηνία που πρέπει να τεθεί σε ισχύ αυτή η πολιτική.
4. Αν θέλετε, επιλέξτε πότε θα υπενθυμίσετε στους χρήστες για τη νέα πολιτική.
5. Κάντε κλικ στο κουμπί **Εφαρμογή**.

Λειτουργίες ασφαλείας

Μπορείτε να ενεργοποιήσετε τις λειτουργίες του HP Client Security που σας βοηθούν να προστατεύσετε τον υπολογιστή από μη εξουσιοδοτημένη πρόσβαση.

Για να εγκαταστήσετε τις λειτουργίες ασφαλείας:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Security Features** (Λειτουργίες ασφαλείας).
3. Ενεργοποιήστε τις λειτουργίες ασφαλείας επιλέγοντας τα πλαίσια ελέγχου και στη συνέχεια κάντε κλικ ή πατήστε στο **Apply** (Εφαρμογή). Όσο περισσότερες λειτουργίες επιλέξετε τόσο πιο ασφαλής είναι ο υπολογιστής σας.

   Αυτές οι λειτουργίες ισχύουν για όλους τους χρήστες.

   - **Windows Logon Security** (Ασφάλεια στην σύνδεση των Windows)—Προστατεύει τους λογαριασμούς Windows απαιτώντας τη χρήση διαπιστευτηρίων του HP Client Security για πρόσβαση.
   - **Pre-Boot Security (Power-on authentication)** [Ασφάλεια πριν την εκκίνηση (έλεγχος ταυτότητας κατά την εκκίνηση)]—Προστατεύει τον υπολογιστή σας πριν από την έναρξη των Windows. Αυτή η επιλογή δεν είναι διαθέσιμη αν το BIOS δεν την υποστηρίζει.
   - **Allow One Step logon** (Να επιτρέπεται η σύνδεση σε ένα βήμα)—Αυτή η ρύθμιση επιτρέπει την παράλειψη της σύνδεσης των Windows αν έχει πραγματοποιηθεί προηγουμένως έλεγχος ταυτότητας κατά την εκκίνηση ή σε επίπεδο κρυπτογράφησης μονάδας δίσκου.
4. Κάντε κλικ ή πατήστε **Χρήστες**και στη συνέχεια κάντε κλικ ή πατήστε το τετράγωνο του χρήστη.

Χρήστες

Μπορείτε να παρακολουθείτε και να διαχειρίζεστε τους χρήστες του HP Client Security του υπολογιστή.

Για προσθέσετε έναν άλλο χρήστη Windows στο HP Client Security:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Users** (Χρήστες).
3. Κάντε κλικ ή πατήστε στο **Add another Windows user to HP Client Security** (Προσθήκη ενός άλλου χρήστη Windows στο HP Client Security).

4. Πληκτρολογήστε το όνομα του χρήστη που θέλετε να προσθέσετε και κάντε κλικ ή πατήστε στο **OK**.
5. Πληκτρολογήστε τον κωδικό πρόσβασης των Windows του χρήστη.

   Στη σελίδα Χρήστης εμφανίζεται ένα τετράγωνο για τον πρόσθετο χρήστη.

Για διαγράψετε έναν χρήστη Windows από το HP Client Security:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Users** (Χρήστες).
3. Κάντε κλικ ή πατήστε στο όνομα του χρήστη που θέλετε να διαγράψετε.
4. Κάντε κλικ ή πατήστε **Διαγραφή χρήστη** και, στη συνέχεια, κάντε κλικ ή πατήστε **Ναι** για επιβεβαίωση.

Για να εμφανιστεί μια σύνοψη των πολιτικών σύνδεσης και περιόδων λειτουργίας που έχουν επιβληθεί για ένα χρήστη:

▲ Κάντε κλικ ή πατήστε **Χρήστες**και στη συνέχεια κάντε κλικ ή πατήστε το τετράγωνο του χρήστη.

Οι πολιτικές μου

Μπορείτε να εμφανίσετε τις πολιτικές ελέγχου ταυτότητας και την κατάσταση δηλώσεων για εσάς. Η σελίδα Οι πολιτικές μου παρέχει επίσης συνδέσμους στις σελίδες με τις πολιτικές για διαχειριστές και τις πολιτικές για τυπικούς χρήστες.

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **My Policies** (Οι πολιτικές μου).

   Εμφανίζονται οι πολιτικές σύνδεσης και περιόδων λειτουργίας που έχουν επιβληθεί για τον τρέχοντα συνδεδεμένο χρήστη.

Η σελίδα Οι πολιτικές μου παρέχει επίσης συνδέσμους στο Πολιτικές διαχειριστή στη σελίδα 28 και στο Πολιτικές τυπικών χρηστών στη σελίδα 29.

Δημιουργία αντιγράφων ασφαλείας και επαναφορά των δεδομένων

Συνιστάται να δημιουργείτε αντίγραφα ασφαλείας των δεδομένων σας στο HP Client Security σε τακτική βάση. Η συχνότητα δημιουργίας των αντιγράφων ασφαλείας εξαρτάται από τη συχνότητα με την οποία αλλάζουν τα δεδομένα. Π.χ., αν δημιουργείτε νέες συνδέσεις καθημερινά πρέπει να δημιουργείτε αντίγραφα ασφαλείας των δεδομένων καθημερινά.

Τα αντίγραφα ασφαλείας μπορούν επίσης να χρησιμοποιηθούν για τη μετεγκατάσταση από έναν υπολογιστή σε άλλον, ή αλλιώς την εισαγωγή και εξαγωγή.

ΣΗΜΕΙΩΣΗ Αυτή η λειτουργία δημιουργεί αντίγραφα ασφαλείας μόνο του Password Manager. Το Drive Encryption έχει ανεξάρτητη μέθοδο δημιουργίας αντιγράφων ασφαλείας. Οι πληροφορίες του Device Access Manager και του ελέγχου ταυτότητας μέσω δακτυλικών αποτυπωμάτων δεν συμπεριλαμβάνονται στα αντίγραφα ασφαλείας.

Το HP Client Security πρέπει να είναι εγκατεστημένο στον υπολογιστή που πρόκειται να λάβει τα αντίγραφα ασφαλείας των δεδομένων πριν γίνει η επαναφορά των δεδομένων από το αρχείο αντιγράφου ασφαλείας.

Για να δημιουργήσετε αντίγραφα ασφαλείας των δεδομένων:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Administrator Policies** (Πολιτικές διαχειριστή).
3. Κάντε κλικ ή πατήστε στο **Backup and Restore** (Δημιουργία αντιγράφου ασφαλείας και επαναφορά).
4. Κάντε κλικ ή πατήστε στο **Backup** (Δημιουργία αντιγράφου ασφαλείας) και, στη συνέχεια, επιβεβαιώστε την ταυτότητά σας.
5. Επιλέξτε το στοιχείο που θέλετε να συμπεριλάβετε στο αντίγραφο ασφαλείας και κάντε κλικ ή πατήστε στο **Next** (Επόμενο).
6. Πληκτρολογήστε το όνομα του αρχείου αποθήκευσης. Από προεπιλογή, το αρχείο αποθηκεύεται στο φάκελο Έγγραφα. Για να καθορίσετε μια διαφορετική τοποθεσία κάντε κλικ ή πατήστε στο **Browse** (Αναζήτηση).
7. Πληκτρολογήστε και επιβεβαιώστε έναν κωδικό πρόσβασης για να προστατεύσετε το αρχείο.
8. Κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση).

Για να επαναφέρετε τα δεδομένα:

1. Από την αρχική σελίδα του HP Client Security κάντε κλικ ή πατήστε στο εικονίδιο **Gear**.
2. Στη σελίδα Ρυθμίσεις για προχωρημένους, κάντε κλικ ή πατήστε στο **Administrator Policies** (Πολιτικές διαχειριστή).
3. Κάντε κλικ ή πατήστε στο **Backup and Restore** (Δημιουργία αντιγράφου ασφαλείας και επαναφορά).
4. Επιλέξτε **Restore** (Επαναφορά) και επιβεβαιώστε την ταυτότητά σας.
5. Επιλέξτε το αρχείο αποθήκευσης που δημιουργήσατε προηγουμένως. Πληκτρολογήστε τη διαδρομή στο παρεχόμενο πεδίο. Για να καθορίσετε μια διαφορετική τοποθεσία κάντε κλικ ή πατήστε στο **Browse** (Αναζήτηση).
6. Πληκτρολογήστε τον κωδικό πρόσβασης που χρησιμοποιείται για προστασία του αρχείου και κάντε κλικ ή πατήστε στο **Next** (Επόμενο).
7. Επιλέξτε τα στοιχεία για τα οποία θέλετε να επαναφέρετε τα δεδομένα.
8. Κάντε κλικ ή πατήστε στο **Restore** (Επαναφορά).

5 HP Drive Encryption (μόνο σε επιλεγμένα μοντέλα)

Το HP Drive Encryption παρέχει πλήρη προστασία δεδομένων μέσω κρυπτογράφησης των δεδομένων του υπολογιστή. Όταν το Drive Encryption είναι ενεργοποιημένο, πρέπει να συνδεθείτε από την οθόνη σύνδεσης του Drive Encryption, που εμφανίζεται πριν την εκκίνηση του λειτουργικού συστήματος Windows®.

Η αρχική οθόνη του HP Client Security επιτρέπει στους διαχειριστές Windows να ενεργοποιήσουν το Drive Encryption, να δημιουργήσουν αντίγραφα ασφαλείας του κλειδιού κρυπτογράφησης και να επιλέξουν ή να καταργήσουν την επιλογή δίσκου(-ων) ή διαμερίσματος(-ων) για κρυπτογράφηση. Για περισσότερες πληροφορίες, δείτε τη βοήθεια του λογισμικού HP Client Security.

Με το Drive Encryption μπορείτε να πραγματοποιήσετε τις ακόλουθες εργασίες:

- Επιλογή ρυθμίσεων του Drive Encryption:
  - Κρυπτογράφηση ή αποκρυπτογράφηση ανεξάρτητων δίσκων ή διαμερισμάτων με χρήση κρυπτογράφησης μέσω λογισμικού
  - Κρυπτογράφηση ή αποκρυπτογράφηση ανεξάρτητων δίσκων με αυτοκρυπτογράφηση με χρήση κρυπτογράφησης μέσω υλικού
  - Προσθήκη επιπλέον ασφάλειας μέσω απενεργοποίησης της λειτουργίας Αναστολή ή Αναμονή ώστε να διασφαλίζεται ότι ζητείται πάντα ο έλεγχος ταυτότητας πριν την εκκίνηση του Drive Encryption

ΣΗΜΕΙΩΣΗ Μπορείτε να κρυπτογραφήσετε μόνο εσωτερικές μονάδες σκληρού δίσκου SATA και εξωτερικές μονάδες σκληρού δίσκου eSATA.

- Δημιουργία αντιγράφων ασφαλείας κλειδιών
- Ανάκτηση της πρόσβασης σε έναν κρυπτογραφημένο υπολογιστή με χρήση αντιγράφων ασφαλείας κλειδιών και του HP SpareKey
- Ενεργοποίηση του ελέγχου ταυτότητας πριν την εκκίνηση του Drive Encryption με χρήση κωδικού πρόσβασης, καταχωρημένου δακτυλικού αποτυπώματος ή κωδικού PIN για έξυπνες κάρτες

Άνοιγμα του Drive Encryption

Οι διαχειριστές μπορούν να αποκτήσουν πρόσβαση στο Drive Encryption ανοίγοντας το HP Client Security:

1. Από την οθόνη Έναρξη, κάντε κλικ ή πατήστε στην εφαρμογή **HP Client Security** (Windows 8).

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε διπλό κλικ ή διπλό πάτημα στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στο δεξί άκρο της γραμμής εργαλείων.

2. Κάντε κλικ ή πατήστε στο εικονίδιο του **Drive Encryption**.

Γενικές εργασίες

Ενεργοποίηση του Drive Encryption για τυπικούς σκληρούς δίσκους

Οι τυπικοί σκληροί δίσκοι κρυπτογραφούνται με χρήση κρυπτογράφησης μέσω λογισμικού. Ακολουθήστε τα παρακάτω βήματα για να κρυπτογραφήσετε ένα δίσκο ή ένα διαμέρισμα δίσκου:

1. Εκκινήστε το **Drive Encryption**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του Drive Encryption στη σελίδα 33.
2. Επιλέξτε το πλαίσιο ελέγχου για το δίσκο ή το διαμέρισμα που θέλετε να κρυπτογραφήσετε και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Backup Key** (Αντίγραφο ασφαλείας κλειδιού).

ΣΗΜΕΙΩΣΗ Για περισσότερη ασφάλεια, επιλέξτε το πλαίσιο ελέγχου **Disable sleep mode for increased security** (Απενεργοποίηση της λειτουργίας αναστολής για αυξημένη ασφάλεια). Όταν απενεργοποιείτε τη λειτουργία αναστολής, δεν υπάρχει απολύτως κανένας κίνδυνος να αποθηκευτούν στη μνήμη τα διαπιστευτήρια που χρησιμοποιούνται για το ξεκλείδωμα της μονάδας δίσκου.

3. Επιλέξτε μία ή περισσότερες από τις επιλογές αντιγράφων ασφαλείας και κάντε κλικ ή πατήστε στο **Backup** (Δημιουργία αντιγράφων ασφαλείας). Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Δημιουργία αντιγράφου ασφαλείας κλειδιού κρυπτογράφησης στη σελίδα 38.
4. Μπορείτε να συνεχίσετε την εργασία σας κατά τη διάρκεια της δημιουργίας αντιγράφου ασφαλείας του κλειδιού κρυπτογράφησης. Μην επανεκκινήσετε τον υπολογιστή.

ΣΗΜΕΙΩΣΗ Θα σας ζητηθεί να επανεκκινήσετε τον υπολογιστή. Μετά την επανεκκίνηση, εμφανίζεται η οθόνη πριν την εκκίνηση, όπου ζητείται έλεγχος ταυτότητας πριν από την έναρξη των Windows.

Το Drive Encryption έχει ενεργοποιηθεί. Η κρυπτογράφηση των επιλεγμένων διαμερισμάτων δίσκων ενδέχεται να διαρκέσει κάποιες ώρες, ανάλογα με τον αριθμό και το μέγεθος των διαμερισμάτων.

Για περισσότερες πληροφορίες, δείτε τη βοήθεια του λογισμικού HP Client Security.

Ενεργοποίηση του Drive Encryption για σκληρούς δίσκους με αυτοκρυπτογράφηση

Οι δίσκοι με αυτοκρυπτογράφηση που συμμορφώνονται με τις προδιαγραφές OPAL του Trusted Computing Group για τη διαχείριση δίσκων με αυτοκρυπτογράφηση μπορούν να κρυπτογραφηθούν με χρήση κρυπτογράφησης μέσω λογισμικού ή υλικού. Η κρυπτογράφηση μέσω υλικού είναι πολύ ταχύτερη από την κρυπτογράφηση μέσω λογισμικού. Ωστόσο, δεν μπορείτε να επιλέξετε ποια διαμερίσματα του δίσκου θα κρυπτογραφήσετε. Κρυπτογραφείται ολόκληρος ο δίσκος, μαζί με όλα τα τυχόν διαμερίσματα.

Για να κρυπτογραφήσετε συγκεκριμένα διαμερίσματα, πρέπει να χρησιμοποιήσετε κρυπτογράφηση μέσω λογισμικού. Βεβαιωθείτε ότι έχετε καταργήσει την επιλογή του πλαισίου ελέγχου **Only allow hardware encryption for Self-Encrypting Drives (SEDs)** [Να επιτρέπεται μόνο κρυπτογράφηση μέσω υλικού για τους δίσκους με αυτοκρυπτογράφηση (SED)].

Ακολουθήστε τα παρακάτω βήματα για να ενεργοποιήσετε το Drive Encryption για δίσκους με αυτοκρυπτογράφηση:

1. Εκκινήστε το **Drive Encryption**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του Drive Encryption στη σελίδα 33.
2. Επιλέξτε το πλαίσιο ελέγχου για το δίσκο που θέλετε να κρυπτογραφήσετε και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Backup Key** (Αντίγραφο ασφαλείας κλειδιού).

ΣΗΜΕΙΩΣΗ Για περισσότερη ασφάλεια, επιλέξτε το πλαίσιο ελέγχου **Disable sleep mode for increased security** (Απενεργοποίηση της λειτουργίας αναστολής για αυξημένη ασφάλεια). Όταν απενεργοποιείτε τη λειτουργία αναστολής, δεν υπάρχει απολύτως κανένας κίνδυνος να αποθηκευτούν στη μνήμη τα διαπιστευτήρια που χρησιμοποιούνται για το ξεκλείδωμα της μονάδας δίσκου.

3. Επιλέξτε μία ή περισσότερες από τις επιλογές αντιγράφων ασφαλείας και κάντε κλικ ή πατήστε στο **Backup** (Δημιουργία αντιγράφων ασφαλείας). Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Δημιουργία αντιγράφου ασφαλείας κλειδιού κρυπτογράφησης στη σελίδα 38.
4. Μπορείτε να συνεχίσετε την εργασία σας κατά τη διάρκεια της δημιουργίας αντιγράφου ασφαλείας του κλειδιού κρυπτογράφησης. Μην επανεκκινήσετε τον υπολογιστή.

ΣΗΜΕΙΩΣΗ Για μονάδες με αυτοκρυπτογράφηση, θα σας ζητηθεί να τερματίσετε τη λειτουργία του υπολογιστή.

Για περισσότερες πληροφορίες, δείτε τη βοήθεια του λογισμικού HP Client Security.

Απενεργοποίηση του Drive Encryption

1. Εκκινήστε το **Drive Encryption**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του Drive Encryption στη σελίδα 33.
2. Καταργήστε την επιλογή στο πλαίσιο ελέγχου για όλους τους κρυπτογραφημένους δίσκους και κάντε κλικ ή πατήστε στο **Apply** (Εφαρμογή).

   Ξεκινά η απενεργοποίηση του Drive Encryption.

ΣΗΜΕΙΩΣΗ Αν είχε χρησιμοποιηθεί κρυπτογράφηση μέσω λογισμικού, ξεκινά η αποκρυπτογράφηση. Ενδέχεται να διαρκέσει κάποιες ώρες ανάλογα με το μέγεθος των κρυπτογραφημένων διαμερισμάτων του σκληρού δίσκου. Όταν ολοκληρωθεί η αποκρυπτογράφηση, το Drive Encryption απενεργοποιείται.

Αν είχε χρησιμοποιηθεί κρυπτογράφηση μέσω υλικού, η μονάδα αποκρυπτογραφείται στιγμιαία και μετά από μερικά λεπτά το Drive Encryption απενεργοποιείται.

Όταν το Drive Encryption απενεργοποιηθεί, θα σας ζητηθεί να τερματίσετε τη λειτουργία του υπολογιστή αν είχε χρησιμοποιηθεί κρυπτογράφηση μέσω υλικού ή να επανεκκινήσετε τον υπολογιστή αν είχε χρησιμοποιηθεί κρυπτογράφηση μέσω λογισμικού.

Σύνδεση μετά την ενεργοποίηση του Drive Encryption

Όταν ενεργοποιήσετε τον υπολογιστή μετά την ενεργοποίηση του Drive Encryption και έχει δηλωθεί ο λογαριασμός χρήστη, πρέπει να συνδεθείτε στην οθόνη σύνδεσης του Drive Encryption:

ΣΗΜΕΙΩΣΗ Όταν γίνεται επαναφορά από την Αναστολή ή την Αναμονή, ο έλεγχος ταυτότητας πριν την εκκίνηση του Drive Encryption δεν εμφανίζεται για κρυπτογράφηση μέσω λογισμικού ή υλικού. Η κρυπτογράφηση μέσω υλικού παρέχει την επιλογή **Disable sleep mode for increased security** (Απενεργοποίηση της λειτουργίας αναστολής για αυξημένη ασφάλεια) που όταν είναι ενεργοποιημένη αποτρέπει τη λειτουργία Αναστολής ή Αναμονής.

Κατά την επαναφορά από την Αδρανοποίηση, ο έλεγχος ταυτότητας πριν την εκκίνηση του Drive Encryption εμφανίζεται για κρυπτογράφηση μέσω λογισμικού ή υλικού.

ΣΗΜΕΙΩΣΗ Αν ο διαχειριστής Windows έχει ενεργοποιήσει την ασφάλεια προεκκίνησης BIOS στο HP Client Security και αν είναι ενεργοποιημένη (από προεπιλογή) η σύνδεση σε ένα βήμα, μπορείτε να συνδεθείτε στον υπολογιστή αμέσως μετά τον έλεγχο ταυτότητας πριν την εκκίνηση του BIOS χωρίς να χρειαστεί επανέλεγχος ταυτότητας στην οθόνη σύνδεσης του Drive Encryption.

Σύνδεση ενός χρήστη:

▲ Στη σελίδα **Logon** (Σύνδεση), εισαγάγετε τον κωδικό πρόσβασης των Windows, τον κωδικό PIN της έξυπνης κάρτας, το SpareKey ή σαρώστε με ένα καταχωρημένο δάκτυλο.

Σύνδεση πολλών χρηστών:

1. Στη σελίδα **Select user to logon** (Επιλογή χρήστη για σύνδεση), επιλέξτε το χρήστη που θα συνδεθεί από την αναπτυσσόμενη λίστα και κάντε κλικ ή πατήστε στην επιλογή **Next** (Επόμενο).
2. Στη σελίδα **Logon** (Σύνδεση), εισαγάγετε τον κωδικό πρόσβασης των Windows, τον κωδικό PIN της έξυπνης κάρτας, ή σαρώστε με ένα καταχωρημένο δάκτυλο.

ΣΗΜΕΙΩΣΗ Υποστηρίζονται οι ακόλουθες έξυπνες κάρτες:

Υποστηριζόμενες έξυπνες κάρτες

- Gemalto Cyberflex Access 64k V2c

ΣΗΜΕΙΩΣΗ Αν το κλειδί επαναφοράς χρησιμοποιείται για σύνδεση στην οθόνη σύνδεσης του Drive Encryption, απαιτούνται πρόσθετα διαπιστευτήρια στην σύνδεση των Windows για πρόσβαση σε λογαριασμούς χρηστών.

Κρυπτογράφηση πρόσθετων σκληρών δίσκων

Συνιστάται ιδιαιτέρως να χρησιμοποιείτε το HP Drive Encryption για προστασία των δεδομένων μέσω κρυπτογράφησης του σκληρού δίσκου. Μετά την ενεργοποίηση μπορείτε να κρυπτογραφήσετε τυχόν πρόσθετους σκληρούς δίσκους ή διαμερίσματα ακολουθώντας τα παρακάτω βήματα:

1. Εκκινήστε το **Drive Encryption**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του Drive Encryption στη σελίδα 33.
2. Για μονάδες με κρυπτογράφηση μέσω λογισμικού, επιλέξτε τα διαμερίσματα του δίσκου που θέλετε να κρυπτογραφήσετε.

   ΣΗΜΕΙΩΣΗ Αυτό ισχύει επίσης και σε ένα μικτό σενάριο δίσκων όπου υπάρχουν μία ή περισσότερες τυπικές μονάδες σκληρού δίσκου και μία ή περισσότερες μονάδες με αυτοκρυπτογράφηση.

   – ή –

   ▲ Για μονάδες με κρυπτογράφηση μέσω υλικού, επιλέξτε τις πρόσθετες μονάδες που θέλετε να κρυπτογραφήσετε.

Προηγμένες εργασίες

Διαχείριση του Drive Encryption (εργασία διαχειριστή)

Οι διαχειριστές μπορούν να χρησιμοποιήσουν το Drive Encryption για προβολή και αλλαγή της κατάστασης κρυπτογράφησης (μη κρυπτογραφημένος ή κρυπτογραφημένος) όλων των σκληρών δίσκων στον υπολογιστή.

- Αν η κατάσταση είναι Ενεργοποιήθηκε, το Drive Encryption είναι ενεργοποιημένο και ρυθμισμένο. Η μονάδα βρίσκεται σε μία από τις ακόλουθες καταστάσεις:

Κρυπτογράφηση μέσω λογισμικού

- Χωρίς κρυπτογράφηση
- Κρυπτογραφήθηκε
- Κρυπτογράφηση σε εξέλιξη
- Αποκρυπτογράφηση σε εξέλιξη

Κρυπτογράφηση μέσω υλικού

- Κρυπτογραφήθηκε
- Χωρίς κρυπτογράφηση (για πρόσθετες μονάδες)

Κρυπτογράφηση ή αποκρυπτογράφηση ανεξάρτητων διαμερισμάτων δίσκων (μόνο κρυπτογράφηση μέσω λογισμικού)

Οι διαχειριστές μπορούν να χρησιμοποιήσουν το Drive Encryption για να κρυπτογραφήσουν ένα ή περισσότερα διαμερίσματα στον υπολογιστή ή να αποκρυπτογραφήσουν τυχόν διαμερίσματα που έχουν ήδη κρυπτογραφηθεί.

1. Εκκινήστε το **Drive Encryption**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του Drive Encryption στη σελίδα 33.
2. Στην επιλογή **Drive Status** (Κατάσταση δίσκου), επιλέξτε ή καταργήστε την επιλογή από το πλαίσιο ελέγχου που βρίσκεται δίπλα σε καθένα από τα διαμερίσματα που θέλετε να κρυπτογραφήσετε ή να αποκρυπτογραφήσετε και στη συνέχεια κάντε κλικ ή πατήστε στο **Apply** (Εφαρμογή).

ΣΗΜΕΙΩΣΗ Όταν ένα διαμέρισμα είναι σε διαδικασία κρυπτογράφησης ή αποκρυπτογράφησης, εμφανίζεται μια γραμμή προόδου που δείχνει το ποσοστό κρυπτογράφησης.

ΣΗΜΕΙΩΣΗ Τα δυναμικά διαμερίσματα δεν υποστηρίζονται. Αν ένα διαμέρισμα εμφανίζεται ως διαθέσιμο αλλά δεν μπορεί να κρυπτογραφηθεί το διαμέρισμα είναι δυναμικό. Ένα δυναμικό διαμέρισμα προέρχεται από τη συρρίκνωση ενός διαμερίσματος για τη δημιουργία ενός νέου διαμερίσματος μέσα στη Διαχείριση δίσκου.

Εμφανίζεται μια προειδοποίηση αν ένα διαμέρισμα πρόκειται να μετατραπεί σε δυναμικό διαμέρισμα.

Διαχείριση δίσκου

- **Nickname** (Ψευδώνυμο)—Μπορείτε να αποδώσετε στους σκληρούς δίσκους και στα διαμερίσματα ονόματα για ευκολότερη ταυτοποίηση.
- **Disconnected drives** (Αποσυνδεδεμένοι δίσκοι)—Το Drive Encryption μπορεί να ανιχνεύσει δίσκους που έχουν απομακρυνθεί από τον υπολογιστή. Ένας δίσκος που έχει αφαιρεθεί από τον υπολογιστή μετακινείται αυτόματα στη λίστα Αποσυνδεδεμένα. Αν ο δίσκος επιστρέψει στο σύστημα θα εμφανιστεί ξανά στη λίστα Συνδεδεμένα.
- Αν δεν χρειάζεται πια να ανιχνεύετε ή να διαχειρίζεστε τον αποσυνδεδεμένο δίσκο, μπορείτε να τον διαγράψετε από τη λίστα Αποσυνδεδεμένα.
- Το Drive Encryption παραμένει ενεργοποιημένο μέχρι να καταργηθούν οι επιλογές για όλους τους συνδεδεμένους δίσκους και η λίστα Αποσυνδεδεμένα να είναι κενή.

Δημιουργία αντιγράφων ασφαλείας και επαναφορά (εργασία διαχειριστή)

Όταν είναι ενεργοποιημένο το Drive Encryption, οι διαχειριστές μπορούν να χρησιμοποιήσουν τη σελίδα δημιουργίας αντιγράφου ασφαλείας κλειδιού κρυπτογράφησης για να δημιουργήσουν αντίγραφα ασφαλείας των κλειδιών κρυπτογράφησης σε αφαιρούμενα μέσα και να εκτελέσουν επαναφορά.

Δημιουργία αντιγράφου ασφαλείας κλειδιού κρυπτογράφησης

Οι διαχειριστές μπορούν να δημιουργούν αντίγραφα ασφαλείας του κλειδιού κρυπτογράφησης για ένα κρυπτογραφημένο δίσκο σε μια αφαιρούμενη συσκευή αποθήκευσης.

⚠ **ΠΡΟΣΟΧΗ** Βεβαιωθείτε ότι έχετε φυλάξει τη συσκευή αποθήκευσης που περιέχει το αντίγραφο ασφαλείας του κλειδιού σε ασφαλή τοποθεσία, γιατί αν ξεχάσετε τον κωδικό πρόσβασης, απωλέσετε την έξυπνη κάρτα ή δεν έχετε καταχωρήσει δακτυλικό αποτύπωμα, αυτή η συσκευή είναι η μόνη που σας παρέχει πρόσβαση στον υπολογιστή. Η τοποθεσία φύλαξης πρέπει επίσης να είναι ασφαλής γιατί η συσκευή αποθήκευσης επιτρέπει πρόσβαση στα Windows.

1. Εκκινήστε το **Drive Encryption**. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του Drive Encryption στη σελίδα 33.
2. Επιλέξτε το πλαίσιο ελέγχου για ένα δίσκο και στη συνέχεια κάντε κλικ ή πατήστε στο **Backup Key** (Δημιουργία αντιγράφου ασφαλείας κλειδιού).
3. Στην επιλογή **Create HP Drive Encryption recovery key** (Δημιουργία κλειδιού επαναφοράς HP Drive Encryption), επιλέξτε μία ή περισσότερες από τις ακόλουθες επιλογές:
   - **Removable Storage** (Αφαιρούμενο μέσο αποθήκευσης)—Επιλέξτε το πλαίσιο ελέγχου και στη συνέχεια επιλέξτε τη συσκευή αποθήκευσης στην οποία θα αποθηκευτεί το κλειδί κρυπτογράφησης.
   - **SkyDrive**—Επιλέξτε το πλαίσιο ελέγχου. Πρέπει να έχετε συνδεθεί στο Internet. Συνδεθείτε στο Microsoft SkyDrive και κάντε κλικ ή πατήστε στο **Ναι**.

     ΣΗΜΕΙΩΣΗ Για να χρησιμοποιήσετε το αντίγραφο ασφαλείας κλειδιού του HP Drive Encryption που είναι αποθηκευμένο στο SkyDrive, πρέπει να πραγματοποιήσετε λήψη από το SkyDrive σε μια αφαιρούμενη συσκευή αποθήκευσης και στη συνέχεια να συνδέσετε τη συσκευή αποθήκευσης στον υπολογιστή.
   - **TPM** (μόνο σε επιλεγμένα μοντέλα)—Σας επιτρέπει να επαναφέρετε τα δεδομένα χρησιμοποιώντας τον κωδικό πρόσβασης TPM.

ΠΡΟΣΟΧΗ Αν ο κωδικός TPM έχει διαγραφεί ή ο υπολογιστής έχει πάθει βλάβη θα χάσετε την πρόσβαση στο αντίγραφο ασφαλείας. Εάν αυτή η μέθοδος είναι ενεργοποιημένη, κάποια άλλη μέθοδος αντιγράφων ασφαλείας θα πρέπει επίσης να είναι επιλεγμένη.

4. Κάντε κλικ ή πατήστε στο **Backup** (Δημιουργία αντιγράφου ασφαλείας).

   Το κλειδί κρυπτογράφησης αποθηκεύεται στη συσκευή αποθήκευσης που επιλέξατε.

Επανάκτηση πρόσβασης σε ενεργοποιημένο υπολογιστή με χρήση αντιγράφου ασφαλείας κλειδιού

Οι διαχειριστές μπορούν να πραγματοποιήσουν επαναφορά χρησιμοποιώντας το αντίγραφο ασφαλείας κλειδιού του Drive Encryption που βρίσκεται σε μια αφαιρούμενη συσκευή αποθήκευσης ενεργοποιώντας ή επιλέγοντας **Backup Key** (Δημιουργία αντιγράφου ασφαλείας κλειδιού κρυπτογράφησης) στο Drive Encryption.

1. Εισαγάγετε την αφαιρούμενη συσκευή αποθήκευσης που περιέχει το αντίγραφο ασφαλείας του κλειδιού κρυπτογράφησης.
2. Ενεργοποιήστε τον υπολογιστή.
3. Όταν ανοίξει το πλαίσιο διαλόγου σύνδεσης του HP Drive Encryption, κάντε κλικ ή πατήστε στο **Recovery** (Επαναφορά).
4. Εισαγάγετε τη διαδρομή του αρχείου ή το όνομα που περιέχει το αντίγραφο ασφαλείας κλειδιού και κάντε κλικ ή πατήστε στο **Recovery** (Επαναφορά).
5. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ ή πατήστε στο **OK**.

   Εμφανίζεται η οθόνη σύνδεσης των Windows.

ΣΗΜΕΙΩΣΗ Αν το κλειδί επαναφοράς χρησιμοποιείται για σύνδεση στην οθόνη σύνδεσης του Drive Encryption, απαιτούνται πρόσθετα διαπιστευτήρια στην σύνδεση των Windows για πρόσβαση σε λογαριασμούς χρηστών. Συνιστάται ιδιαιτέρως να ορίσετε ξανά τον κωδικό πρόσβασης μετά από την επαναφορά.

Εκτέλεση επαναφοράς μέσω του HP SpareKey

Η επαναφορά SpareKey μέσα από την κρυπτογράφηση δίσκου πριν την εκκίνηση απαιτεί από εσάς να απαντήσετε σωστά σε ερωτήσεις ασφαλείας για να μπορέσετε να αποκτήσετε πρόσβαση στον υπολογιστή. Για περισσότερες πληροφορίες σχετικά με την εγκατάσταση της επαναφοράς μέσω SpareKey, δείτε τη βοήθεια του λογισμικού HP Client Security.

Για να πραγματοποιήσετε μια επαναφορά μέσω του HP SpareKey αν ξεχάσετε τον κωδικό πρόσβασης:

1. Ενεργοποιήστε τον υπολογιστή.
2. Όταν εμφανίζεται η σελίδα του HP Drive Encryption, πλοηγηθείτε στη σελίδα σύνδεσης χρήστη.
3. Κάντε κλικ στο κουμπί **SpareKey**.

ΣΗΜΕΙΩΣΗ Αν το SpareKey δεν έχει προετοιμαστεί στο HP Client Security, το κουμπί **SpareKey** δεν είναι διαθέσιμο.

4. Πληκτρολογήστε σωστές απαντήσεις στις εμφανιζόμενες ερωτήσεις και, στη συνέχεια, κάντε κλικ στην επιλογή **Σύνδεση**.

   Εμφανίζεται η οθόνη σύνδεσης των Windows.

ΣΗΜΕΙΩΣΗ Αν το SpareKey χρησιμοποιείται για σύνδεση στην οθόνη σύνδεσης του Drive Encryption, απαιτούνται πρόσθετα διαπιστευτήρια στην σύνδεση των Windows για πρόσβαση σε λογαριασμούς χρηστών. Συνιστάται ιδιαιτέρως να ορίσετε ξανά τον κωδικό πρόσβασης μετά από την επαναφορά.

6 HP File Sanitizer (μόνο σε επιλεγμένα μοντέλα)

Το File Sanitizer σας δίνει τη δυνατότητα να καταστρέφετε με ασφάλεια πόρους (π.χ.: προσωπικές πληροφορίες ή αρχεία, ιστορικά δεδομένα ή δεδομένα που σχετίζονται με το Web, ή άλλα στοιχεία δεδομένων) στην εσωτερική μονάδα σκληρού δίσκου του υπολογιστή και περιοδικά να απαλοίφετε πλήρως τα διαγραμμένα δεδομένα από την εσωτερική μονάδα σκληρού δίσκου του υπολογιστή.

Το File Sanitizer δεν μπορεί να χρησιμοποιηθεί για την καταστροφή ή την απαλοιφή διαγραμμένων αρχείων στους ακόλουθους τύπους μονάδων σκληρού δίσκου:

- Μονάδες δίσκων στερεάς κατάστασης (SSD), συμπεριλαμβανομένων τόμων RAID που επεκτείνουν μια συσκευή SSD
- Εξωτερικές μονάδες δίσκων που συνδέονται μέσω διασύνδεσης USB, Firewire ή eSATA

Αν επιχειρήσετε μια λειτουργία καταστροφής ή απαλοιφής σε SSD, θα εμφανιστεί ένα προειδοποιητικό μήνυμα και η λειτουργία δεν θα πραγματοποιηθεί.

Μόνιμη διαγραφή

Η μόνιμη διαγραφή διαφέρει από την τυπική λειτουργία διαγραφής των Windows®. Όταν διαγράφετε μόνιμα έναν πόρο χρησιμοποιώντας το File Sanitizer, τα αρχεία αντικαθίστανται από ανούσια δεδομένα, γεγονός που καθιστά πρακτικά αδύνατη την ανάκτηση του αρχικού πόρου. Η απλή λειτουργία διαγραφής των Windows ενδέχεται να αφήσει το αρχείο (ή τον πόρο) άθικτο στη μονάδα σκληρού δίσκου ή σε μια κατάσταση από την οποία μπορεί να ανακτηθεί με μεθόδους εγκληματολογικής έρευνας.

Μπορείτε να προγραμματίσετε μια μελλοντική ώρα μόνιμης διαγραφής ή να την ενεργοποιήσετε μη αυτόματα επιλέγοντας το εικονίδιο **File Sanitizer** στην αρχική οθόνη του HP Client Security ή χρησιμοποιώντας το εικονίδιο του **File Sanitizer** στην επιφάνεια εργασίας των Windows. Για περισσότερες πληροφορίες ανατρέξτε στο Ρύθμιση προγραμματισμού μόνιμης διαγραφής στη σελίδα 43, Καταστροφή με δεξί κλικ στη σελίδα 45 ή στο Μη αυτόματη εκκίνηση της λειτουργίας καταστροφής στη σελίδα 46.

ΣΗΜΕΙΩΣΗ Ένα αρχείο .dll μπορεί να καταστραφεί και να διαγραφεί από το σύστημα μόνο αν έχει μετακινηθεί στον κάδο ανακύκλωσης.

Εκκαθάριση ελεύθερου χώρου

Η διαγραφή ενός πόρου στα Windows δεν αφαιρεί πλήρως τα περιεχόμενα του πόρου από το σκληρό δίσκο. Τα Windows διαγράφουν μόνο την αναφορά στον πόρο ή τη θέση του στο σκληρό δίσκο. Τα περιεχόμενα του πόρου παραμένουν στη μονάδα σκληρού δίσκου μέχρι να αντικατασταθούν με νέες πληροφορίες από έναν άλλο πόρο στην ίδια περιοχή του σκληρού δίσκου.

Η απαλοιφή ελεύθερου χώρου σάς δίνει τη δυνατότητα να γράφετε με ασφάλεια τυχαία δεδομένα πάνω σε διαγραμμένους πόρους, αποτρέποντας έτσι άλλους χρήστες από το να δουν το αρχικό περιεχόμενο του διαγραμμένου πόρου.

ΣΗΜΕΙΩΣΗ Η απαλοιφή ελεύθερου χώρου δεν παρέχει πρόσθετη ασφάλεια σε κατεστραμμένους πόρους.

Μπορείτε να ορίσετε μια μελλοντική ώρα απαλοιφής ελεύθερου χώρου ή να ενεργοποιήσετε μη αυτόματα την απαλοιφή ελεύθερου χώρου πόρων που έχουν ήδη καταστραφεί επιλέγοντας το εικονίδιο του **File Sanitizer** στην αρχική σελίδα του HP Client Security ή χρησιμοποιώντας το εικονίδιο του **File Sanitizer** στην επιφάνεια εργασίας των Windows. Για περισσότερες πληροφορίες ανατρέξτε στο Ρύθμιση προγραμματισμού απαλοιφής ελεύθερου χώρου στη σελίδα 44, Μη αυτόματη εκκίνηση απαλοιφής ελεύθερου χώρου στη σελίδα 46 ή στο Χρήση του εικονιδίου του File Sanitizer στη σελίδα 45.

Άνοιγμα του File Sanitizer

1. Από την οθόνη Έναρξη, κάντε κλικ ή πατήστε στην εφαρμογή **HP Client Security** (Windows 8).

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε διπλό κλικ ή διπλό πάτημα στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στο δεξί άκρο της γραμμής εργαλείων.

2. Στην επιλογή **Data** (Δεδομένα), κάντε κλικ ή πατήστε στο **File Sanitizer**.

– ή –

▲ Κάντε διπλό κλικ ή διπλό πάτημα στο εικονίδιο του **File Sanitizer** στην επιφάνεια εργασίας των Windows.

– ή –

▲ Κάντε διπλό κλικ ή πατήστε και κρατήστε πατημένο το εικονίδιο του **File Sanitizer** στην επιφάνεια εργασίας των Windows και στη συνέχεια επιλέξτε **Open File Sanitizer** (Άνοιγμα του File Sanitizer).

Διαδικασίες ρύθμισης

Shredding (Μόνιμη διαγραφή)—Το File Sanitizer διαγράφει ή καταστρέφει με ασφάλεια επιλεγμένες κατηγορίες πόρων.

1. Στην επιλογή **Shredding** (Μόνιμη διαγραφή), επιλέξτε το πλαίσιο ελέγχου για κάθε τύπο αρχείου που θέλετε να καταστρέψετε ή καταργήστε την επιλογή του πλαισίου αν δεν θέλετε να καταστρέψετε αυτά τα είδη αρχείων.

   - **Recycle Bin** (Κάδος ανακύκλωσης)—Καταστρέφει όλα τα στοιχεία που βρίσκονται στον κάδο ανακύκλωσης.
   - **Temporary system files** (Προσωρινά αρχεία συστήματος)—Καταστρέφει όλα τα αρχεία που βρίσκονται στο φάκελο προσωρινών αρχείων συστήματος. Εκτελείται αναζήτηση στις ακόλουθες μεταβλητές περιβάλλοντος με την ακόλουθη σειρά και η πρώτη διαδρομή που βρίσκεται θεωρείται ως ο φάκελος συστήματος:
     - TMP
     - TEMP
   - **Temporary Internet files** (Προσωρινά αρχεία Internet)—Καταστρέφει αντίγραφα σελίδων Web, εικόνες και πολυμέσα που έχουν αποθηκευτεί από προγράμματα περιήγησης στο Web για ταχύτερη προβολή.
   - **Cookies**—Καταστρέφει όλα τα αρχεία που είναι αποθηκευμένα σε έναν υπολογιστή από ιστότοπους στο Web για αποθήκευση προτιμήσεων όπως πληροφορίες σύνδεσης.

2. Για να εκκινήσετε τη μόνιμη διαγραφή, κάντε κλικ ή πατήστε στο **Shred** (Μόνιμη διαγραφή).

Bleaching (Απαλοιφή)—Εγγράφει τυχαία δεδομένα στον ελεύθερο χώρο και αποτρέπει την επαναφορά διαγραμμένων στοιχείων.

▲ Για να εκκινήσετε την απαλοιφή, κάντε κλικ ή πατήστε στο **Bleach** (Απαλοιφή).

File Sanitizer Options (Επιλογές του File Sanitizer)—Επιλέξτε το πλαίσιο ελέγχου για να ενεργοποιήσετε καθεμία από τις ακόλουθες επιλογές ή καταργήστε την επιλογή για να απενεργοποιήσετε μια επιλογή:

- **Enable Desktop icon** (Ενεργοποίηση εικονιδίου επιφάνειας εργασίας)—Εμφανίζει το εικονίδιο του File Sanitizer στην επιφάνεια εργασίας των Windows.
- **Enable right-click** (Ενεργοποίηση δεξί κλικ)—Σας επιτρέπει να κάνετε δεξί κλικ ή να πατήσετε και να κρατήσετε πατημένο έναν πόρο και στη συνέχεια να επιλέξετε **HP File Sanitizer – Shred** (HP File Sanitizer – Μόνιμη διαγραφή).
- **Ask for Windows password before manual shredding** (Να ζητείται κωδικός πρόσβασης των Windows πριν από τη μη αυτόματη μόνιμη διαγραφή)—Απαιτεί έλεγχο ταυτότητας με τον κωδικό πρόσβασης των Windows πριν από τη μη αυτόματη μόνιμη διαγραφή ενός στοιχείου.
- **Shred Cookies and Temporary Internet Files on browser close** (Μόνιμη διαγραφή Cookies και προσωρινών αρχείων Internet κατά το κλείσιμο του προγράμματος περιήγησης)—Διαγράφει μόνιμα όλους τους επιλεγμένους πόρους που σχετίζονται με το Web, όπως το ιστορικό περιήγησης URL όταν κλείσετε το πρόγραμμα περιήγησης στο Web.

Ρύθμιση προγραμματισμού μόνιμης διαγραφής

Μπορείτε να προγραμματίσετε την αυτόματη καταστροφή ή μπορείτε επίσης να εκτελέσετε με μη αυτόματο τρόπο καταστροφή πόρων οποιαδήποτε χρονική στιγμή. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Διαδικασίες ρύθμισης στη σελίδα 42.

1. Ανοίξτε το File Sanitizer και κάντε κλικ ή πατήστε στο **Settings** (Ρυθμίσεις).
2. Για να προγραμματίσετε μια μελλοντική ώρα για την καταστροφή επιλεγμένων πόρων, στην επιλογή **Shred Schedule** (Προγραμματισμός καταστροφής), επιλέξτε **Never** (Ποτέ), **Once** (Μία φορά), **Daily** (Καθημερινά), **Weekly** (Εβδομαδιαία), ή **Monthly** (Μηνιαία) και στη συνέχεια επιλέξτε την ημέρα και ώρα:

   α. Κάντε κλικ ή πατήστε στην ώρα, τα λεπτά ή στο πεδίο ΠΜ/ΜΜ.

   β. Κάντε κύλιση μέχρι η επιθυμητή τιμή να εμφανίζεται στο ίδιο επίπεδο με τα άλλα πεδία.

   γ. Κάντε κλικ ή πατήστε στη λευκή περιοχή που περιβάλλει τα πεδία ρύθμισης χρόνου.

   δ. Επαναλάβετε για κάθε πεδίο μέχρι να επιλέξετε το σωστό προγραμματισμό χρόνου.
3. Εμφανίζονται οι ακόλουθοι τέσσερις τύποι πόρων:

   - **Recycle Bin** (Κάδος ανακύκλωσης)—Καταστρέφει όλα τα στοιχεία που βρίσκονται στον κάδο ανακύκλωσης.
   - **Temporary system files** (Προσωρινά αρχεία συστήματος)—Καταστρέφει όλα τα αρχεία που βρίσκονται στο φάκελο προσωρινών αρχείων συστήματος. Εκτελείται αναζήτηση στις ακόλουθες μεταβλητές περιβάλλοντος με την ακόλουθη σειρά και η πρώτη διαδρομή που βρίσκεται θεωρείται ως ο φάκελος συστήματος:
     - TMP
     - TEMP

- **Temporary Internet files** (Προσωρινά αρχεία Internet)—Καταστρέφει αντίγραφα σελίδων Web, εικόνες και πολυμέσα που έχουν αποθηκευτεί από προγράμματα περιήγησης στο Web για ταχύτερη προβολή.
- **Cookies**—Καταστρέφει όλα τα αρχεία που είναι αποθηκευμένα σε έναν υπολογιστή από ιστότοπους στο Web για αποθήκευση προτιμήσεων όπως πληροφορίες σύνδεσης.

Αν επιλεγούν, αυτοί οι πόροι καταστρέφονται τη χρονική στιγμή που έχει προγραμματιστεί.

4. Για να επιλέξετε πρόσθετους πόρους για καταστροφή:

   α. Στην επιλογή **Scheduled Shred List** (Λίστα προγραμματισμένης καταστροφής), κάντε κλικ ή πατήστε στο **Add folder** (Προσθήκη φακέλου) και αναζητήστε το αρχείο ή το φάκελο.

   β. Κάντε κλικ ή πατήστε στο **Open** (Άνοιγμα) και στη συνέχεια κάντε κλικ ή πατήστε στο **OK**.

   Για να αφαιρέσετε έναν πόρο από τη λίστα προγραμματισμένης καταστροφής, καταργήστε το πλαίσιο ελέγχου για τον πόρο.

Ρύθμιση προγραμματισμού απαλοιφής ελεύθερου χώρου

Η απαλοιφή ελεύθερου χώρου δεν παρέχει πρόσθετη ασφάλεια σε κατεστραμμένους πόρους.

1. Ανοίξτε το File Sanitizer και κάντε κλικ ή πατήστε στο **Settings** (Ρυθμίσεις).
2. Για να προγραμματίσετε ένα μελλοντικό χρόνο για απαλοιφή της μονάδας σκληρού δίσκου, κάτω από το **Προγραμματισμός απαλοιφής**, επιλέξτε **Ποτέ**, **Μία φορά**, **Ημερησίως**, **Εβδομαδιαίως**, **Μηνιαίως**και, στη συνέχεια, επιλέξτε μια ημέρα και ώρα.

   α. Κάντε κλικ ή πατήστε στην ώρα, τα λεπτά ή στο πεδίο ΠΜ/ΜΜ.

   β. Κάντε κύλιση μέχρι η επιθυμητή ώρα να εμφανίζεται στο ίδιο επίπεδο με τα άλλα πεδία.

   γ. Κάντε κλικ ή πατήστε στη λευκή περιοχή που περιβάλλει τα πεδία ρύθμισης χρόνου.

   δ. Επαναλάβετε μέχρι να προγραμματίσετε τη σωστή ώρα.

ΣΗΜΕΙΩΣΗ Η λειτουργία απαλοιφής ελεύθερου χώρου μπορεί να διαρκέσει αρκετά. Βεβαιωθείτε ότι ο υπολογιστής είναι συνδεδεμένος στην τροφοδοσία AC. Παρόλο που η απαλοιφή ελεύθερου χώρου εκτελείται στο παρασκήνιο, η αυξημένη χρήση του επεξεργαστή ενδέχεται να επηρεάσει την απόδοση του υπολογιστή. Η απαλοιφή ελεύθερου χώρου μπορεί να εκτελεστεί αργά το βράδυ ή όταν ο υπολογιστής δεν χρησιμοποιείται.

Προστασία αρχείων από τη λειτουργία καταστροφής

Για να προστατεύσετε αρχεία ή φακέλους από τη λειτουργία καταστροφής:

1. Ανοίξτε το File Sanitizer και κάντε κλικ ή πατήστε στο **Settings** (Ρυθμίσεις).
2. Στην επιλογή **Never Shred List** (Ποτέ στη λίστα καταστροφής) κάντε κλικ ή πατήστε στο **Add folder** (Προσθήκη φακέλου) και αναζητήστε το αρχείο ή το φάκελο.
3. Κάντε κλικ ή πατήστε στο **Open** (Άνοιγμα) και στη συνέχεια κάντε κλικ ή πατήστε στο **OK**.

ΣΗΜΕΙΩΣΗ Τα αρχεία που βρίσκονται σε αυτή τη λίστα παραμένουν προστατευμένα όσο βρίσκονται στη λίστα.

Για να αφαιρέσετε έναν πόρο από τη λίστα εξαιρέσεων, καταργήστε το πλαίσιο ελέγχου για τον πόρο.

Γενικές εργασίες

Χρήση του File Sanitizer για την εκτέλεση των ακόλουθων εργασιών:

- **Χρήση του εικονιδίου του File Sanitizer για εκκίνηση της καταστροφής**—Μεταφορά αρχείων στο εικονίδιο του **File Sanitizer** στην επιφάνεια εργασίας των Windows. Για περισσότερες λεπτομέρειες ανατρέξτε στο Χρήση του εικονιδίου του File Sanitizer στη σελίδα 45.
- **Μη αυτόματη καταστροφή συγκεκριμένου πόρου ή όλων των επιλεγμένων πόρων**—Καταστροφή στοιχείων οποιαδήποτε χρονική στιγμή χωρίς να περιμένετε μια προγραμματισμένη ώρα καταστροφής. Για περισσότερες λεπτομέρειες ανατρέξτε στο Καταστροφή με δεξί κλικ στη σελίδα 45 ή στο Μη αυτόματη εκκίνηση της λειτουργίας καταστροφής στη σελίδα 46.
- **Μη αυτόματη ενεργοποίηση της απαλοιφής ελεύθερου χώρου**—Ενεργοποίηση της απαλοιφής ελεύθερου χώρου οποιαδήποτε στιγμή. Για περισσότερες λεπτομέρειες ανατρέξτε στο Μη αυτόματη εκκίνηση απαλοιφής ελεύθερου χώρου στη σελίδα 46.
- **Προβολή των αρχείων καταγραφής**—Προβολή των αρχείων καταγραφής των λειτουργιών καταστροφής και απαλοιφής ελεύθερου χώρου, τα οποία περιέχουν τυχόν σφάλματα ή αποτυχίες από την τελευταία λειτουργία καταστροφής και απαλοιφής ελεύθερου χώρου. Για περισσότερες λεπτομέρειες ανατρέξτε στο Προβολή των αρχείων καταγραφής στη σελίδα 46.

ΣΗΜΕΙΩΣΗ Η λειτουργία καταστροφής ή απαλοιφής ελεύθερου χώρου μπορεί να διαρκέσει αρκετά. Παρόλο που η λειτουργία καταστροφής ή απαλοιφής ελεύθερου χώρου εκτελείται στο παρασκήνιο, η αυξημένη χρήση του επεξεργαστή ενδέχεται να επηρεάσει την απόδοση του υπολογιστή.

Χρήση του εικονιδίου του File Sanitizer

ΠΡΟΣΟΧΗ Δεν είναι δυνατή η επαναφορά των μόνιμα διαγραμμένων στοιχείων. Σκεφτείτε προσεκτικά ποια στοιχεία επιλέγετε για μη αυτόματη καταστροφή.

Όταν εκκινείτε μια λειτουργία μη αυτόματης καταστροφής, καταστρέφονται τα αρχεία που εμφανίζονται στην τυπική λίστα καταστροφής του File Sanitizer (βλ. Διαδικασίες ρύθμισης στη σελίδα 42).

Μπορείτε να εκκινήσετε μια μη αυτόματη λειτουργία καταστροφής με έναν από τους παρακάτω τρόπους:

1. Ανοίξτε το File Sanitizer (δείτε Άνοιγμα του File Sanitizer στη σελίδα 42) και κάντε κλικ ή πατήστε στο **Shred** (Καταστροφή).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, βεβαιωθείτε ότι έχετε επιλέξει τους πόρους που θέλετε να καταστρέψετε και στη συνέχεια κάντε κλικ ή πατήστε στο **OK**.

– ή –

1. Κάντε διπλό κλικ ή πατήστε και κρατήστε πατημένο το εικονίδιο **File Sanitizer** στην επιφάνεια εργασίας των Windows και στη συνέχεια επιλέξτε **Shred Now** (Καταστροφή τώρα).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, βεβαιωθείτε ότι έχετε επιλέξει τους πόρους που θέλετε να καταστρέψετε και στη συνέχεια κάντε κλικ ή πατήστε στο **Shred** (Καταστροφή).

Καταστροφή με δεξί κλικ

ΠΡΟΣΟΧΗ Δεν είναι δυνατή η επαναφορά των μόνιμα διαγραμμένων στοιχείων. Σκεφτείτε προσεκτικά ποια στοιχεία επιλέγετε για μη αυτόματη καταστροφή.

Αν έχετε επιλέξει **Enable right-click shredding** (Ενεργοποίηση καταστροφής με δεξί κλικ) στην προβολή του File Sanitizer, μπορείτε να καταστρέψετε έναν πόρο ως εξής:

1. Κάντε αναζήτηση του εγγράφου ή του φακέλου που θέλετε να καταστρέψετε.
2. Κάντε δεξί κλικ ή πατήστε και κρατήστε πατημένο το αρχείο ή το φάκελο και επιλέξτε **HP File Sanitizer – Shred** (HP File Sanitizer – Καταστροφή).

Μη αυτόματη εκκίνηση της λειτουργίας καταστροφής

⚠ **ΠΡΟΣΟΧΗ** Δεν είναι δυνατή η επαναφορά των μόνιμα διαγραμμένων στοιχείων. Σκεφτείτε προσεκτικά ποια στοιχεία επιλέγετε για μη αυτόματη καταστροφή.

Όταν εκκινείτε μια λειτουργία μη αυτόματης καταστροφής, καταστρέφονται τα αρχεία που εμφανίζονται στην τυπική λίστα καταστροφής του File Sanitizer (βλ. Διαδικασίες ρύθμισης στη σελίδα 42).

Μπορείτε να εκκινήσετε μια μη αυτόματη λειτουργία καταστροφής με έναν από τους παρακάτω τρόπους:

1. Ανοίξτε το File Sanitizer (δείτε Άνοιγμα του File Sanitizer στη σελίδα 42) και κάντε κλικ ή πατήστε στο **Shred** (Καταστροφή).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, βεβαιωθείτε ότι έχετε επιλέξει τους πόρους που θέλετε να καταστρέψετε και στη συνέχεια κάντε κλικ ή πατήστε στο **OK**.

– ή –

1. Κάντε διπλό κλικ ή πατήστε και κρατήστε πατημένο το εικονίδιο **File Sanitizer** στην επιφάνεια εργασίας των Windows και στη συνέχεια επιλέξτε **Shred Now** (Καταστροφή τώρα).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, βεβαιωθείτε ότι έχετε επιλέξει τους πόρους που θέλετε να καταστρέψετε και στη συνέχεια κάντε κλικ ή πατήστε στο **Shred** (Καταστροφή).

Μη αυτόματη εκκίνηση απαλοιφής ελεύθερου χώρου

Όταν εκκινείτε μια λειτουργία μη αυτόματης απαλοιφής, απαλείφεται η τυπική λίστα στην προβολή του File Sanitizer (δείτε Διαδικασίες ρύθμισης στη σελίδα 42).

Μπορείτε να εκκινήσετε μια μη αυτόματη λειτουργία απαλοιφής με έναν από τους παρακάτω τρόπους:

1. Ανοίξτε το File Sanitizer (δείτε Άνοιγμα του File Sanitizer στη σελίδα 42) και κάντε κλικ ή πατήστε στο **Bleach** (Απαλοιφή).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ ή πατήστε στο **OK**.

– ή –

1. Κάντε διπλό κλικ ή πατήστε και κρατήστε πατημένο το εικονίδιο **File Sanitizer** στην επιφάνεια εργασίας των Windows και στη συνέχεια επιλέξτε **Bleach Now** (Απαλοιφή τώρα).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ ή πατήστε στο **Bleach** (Απαλοιφή).

Προβολή των αρχείων καταγραφής

Κάθε φορά που εκτελείται μια λειτουργία καταστροφής ή απαλοιφής ελεύθερου χώρου, δημιουργούνται αρχεία καταγραφής τυχόν σφαλμάτων ή αποτυχιών. Τα αρχεία καταγραφής ενημερώνονται πάντα σύμφωνα με τις τελευταίες λειτουργίες καταστροφής ή απαλοιφής ελεύθερου χώρου.

ΣΗΜΕΙΩΣΗ Τα αρχεία για τα οποία η λειτουργία καταστροφής ή απαλοιφής ήταν επιτυχής δεν εμφανίζονται στα αρχεία καταγραφής.

Ένα αρχείο καταγραφής δημιουργείται για τις λειτουργίες καταστροφής και ένα άλλο για τις λειτουργίες απαλοιφής ελεύθερου χώρου. Και τα δύο αρχεία καταγραφής βρίσκονται στη μονάδα σκληρού δίσκου στους εξής φακέλους:

- C:\Program Files\Hewlett-Packard\File Sanitizer*[όνομαχρήστη]*_ShredderLog.txt
- C:\Program Files\Hewlett-Packard\File Sanitizer*[όνομαχρήστη]*_DiskBleachLog.txt

Για συστήματα 64-bit τα αρχεία καταγραφής βρίσκονται στη μονάδα σκληρού δίσκου στους εξής φακέλους:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[όνομαχρήστη]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[όνομαχρήστη]*_DiskBleachLog.txt

7 HP Device Access Manager (επιλεγμένα μοντέλα μόνο)

Το HP Device Access Manager ελέγχει την πρόσβαση σε δεδομένα απενεργοποιώντας συσκευές μεταφοράς δεδομένων.

ΣΗΜΕΙΩΣΗ Μερικές συσκευές με διασύνδεση χρήστη/συσκευές εισόδου όπως ποντίκι, πληκτρολόγιο, TouchPad και συσκευή ανάγνωσης δαχτυλικών αποτυπωμάτων δεν ελέγχονται από το Device Access Manager. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Κατηγορίες συσκευών χωρίς δυνατότητα ελέγχου στη σελίδα 52.

Οι διαχειριστές λειτουργικού συστήματος Windows ® χρησιμοποιούν το HP Device Access Manager για τον έλεγχο της πρόσβασης στις συσκευές ενός συστήματος και για την προστασία από μη εξουσιοδοτημένη πρόσβαση:

- Δημιουργούνται προφίλ συσκευών για κάθε χρήστη για τον καθορισμό των συσκευών στις οποίες επιτρέπεται ή απαγορεύεται η πρόσβαση.
- Το Just In Time Authentication (JITA) επιτρέπει σε προκαθορισμένους χρήστες να επαληθεύουν την ταυτότητά τους για να αποκτήσουν πρόσβαση σε συσκευές από τις οποίες διαφορετικά αποκλείονται.
- Οι διαχειριστές και οι αξιόπιστοι χρήστες μπορούν να εξαιρεθούν από τους περιορισμούς αναφορικά με την πρόσβαση σε συσκευές που επιβάλλονται από το Device Access Manager προσθέτοντάς τους στην ομάδα διαχειριστών της συσκευής. Η διαχείριση της συμμετοχής αυτής της ομάδας γίνεται χρησιμοποιώντας τις Ρυθμίσεις για προχωρημένους.
- Η πρόσβαση στη συσκευή μπορεί να εκχωρηθεί ή να αποκλειστεί με βάση τα μέλη της ομάδας ή για μεμονωμένους χρήστες.
- Για κατηγορίες συσκευών όπως μονάδες CD-ROM και DVD, η πρόσβαση για ανάγνωση και εγγραφή μπορεί να επιτρέπεται ή να αποκλείεται ξεχωριστά.

Η διαμόρφωση ρυθμίσεων του HP Device Access Manager γίνεται αυτόματα με τις ακόλουθες ρυθμίσεις κατά τη διάρκεια της ολοκλήρωσης του οδηγού εγκατάστασης του HP Client Security.

- Το Just In Time Authentication (JITA) Removable Media μπορεί να ενεργοποιηθεί για διαχειριστές και χρήστες.
- Η πολιτική συσκευής επιτρέπει πλήρη πρόσβαση σε άλλες συσκευές.

Άνοιγμα του Device Access Manager

1. Από την οθόνη Έναρξη, κάντε κλικ ή πατήστε στην εφαρμογή **HP Client Security** (Windows 8).

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε διπλό κλικ ή διπλό πάτημα στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στο δεξί άκρο της γραμμής εργαλείων.

2. Στην επιλογή **Device** (Συσκευή), κάντε κλικ ή πατήστε στο **Device Permissions** (Δικαιώματα συσκευής).

   - Οι τυπικοί χρήστες μπορούν να προβάλουν την τρέχουσα κατάσταση πρόσβασης στη συσκευή (βλ. Προβολή χρήστη στη σελίδα 49).
   - Οι διαχειριστές μπορούν να προβάλουν και να κάνουν αλλαγές στην πρόσβαση στην συσκευή που έχει διαμορφωθεί για τον υπολογιστή κάνοντας κλικ ή πατώντας στην επιλογή **Change** (Αλλαγή) και, στη συνέχεια, πληκτρολογώντας τον κωδικό πρόσβασης διαχειριστή (βλ. Προβολή συστήματος στη σελίδα 49).

Προβολή χρήστη

Η Προβολή χρήστη εμφανίζεται, όταν έχετε επιλέξει **Device Permission** (Δικαιώματα συσκευής). Ανάλογα με την πολιτική, οι τυπικοί χρήστες και διαχειριστές μπορούν να προβάλουν τα δικά τους δικαιώματα πρόσβασης για κατηγορίες συσκευών ή ανεξάρτητες συσκευές στον υπολογιστή.

- **Current user** (Τρέχων χρήστης)—Εμφανίζεται το όνομα του χρήστη που είναι αυτήν τη στιγμή συνδεδεμένος.
- **Device Class** (Κατηγορία συσκευών)—Εμφανίζονται οι τύποι συσκευών.
- **Access** (Πρόσβαση)—Εμφανίζεται η τρέχουσα διαμορφωμένη πρόσβαση σε τύπους συσκευών ή σε συγκεκριμένες συσκευές.
- **Duration** (Διάρκεια)—Εμφανίζεται το χρονικό όριο για την πρόσβαση σε μονάδες δίσκων CD/DVD-ROM ή σε αφαιρούμενες μονάδες δίσκων.
- **Settings** (Ρυθμίσεις)—Οι διαχειριστές μπορούν να αλλάξουν τις μονάδες δίσκων που ελέγχονται από το Device Access Manager στις οποίες επιτρέπεται η πρόσβαση.

Προβολή συστήματος

Στην Προβολή συστήματος, οι διαχειριστές μπορούν να επιτρέψουν ή να απαγορεύσουν την πρόσβαση σε συσκευές στον υπολογιστή για την ομάδα χρηστών ή την ομάδα διαχειριστών.

▲ Οι διαχειριστές μπορούν να αποκτήσουν πρόσβαση στην Προβολή συστήματος κάνοντας κλικ ή πατώντας στην επιλογή **Change** (Αλλαγή), να πληκτρολογήσουν τον κωδικό πρόσβασης διαχειριστή και, στη συνέχεια, να επιλέξουν από τις παρακάτω επιλογές:

- **Device Access Manager**—Για ενεργοποίηση ή απενεργοποίηση του HP Device Access Manager με Just In Time Authentication, κάντε κλικ ή πατήστε στο **On** (Ενεργοποίηση) ή στο **Off** (Απενεργοποίηση).
- **Users and groups on this PC** (Χρήστες και ομάδες σε αυτό το PC)—Προβάλει την ομάδα χρηστών ή την ομάδα διαχειριστών για τις οποίες επιτρέπεται ή απαγορεύεται η πρόσβαση στις επιλεγμένες κατηγορίες συσκευών.
- **Device Class** (Κατηγορία συσκευών)—Προβάλει την κατηγορία συσκευών και τις συσκευές που είναι εγκατεστημένες στο σύστημα ή έχουν προγενέστερα εγκατασταθεί στο σύστημα. Για να

επεκτείνετε τη λίστα, κάντε κλικ στο εικονίδιο **+**. Εμφανίζονται όλες οι συσκευές που είναι συνδεδεμένες στον υπολογιστή και οι ομάδες χρηστών και διαχειριστών επεκτείνονται για να εμφανιστεί η ιδιότητα μέλους. Για ανανέωση της λίστας συσκευών, κάντε κλικ στο εικονίδιο με το κυκλικό βέλος (ανανέωση).

- Η προστασία εφαρμόζεται συνήθως για μια κατηγορία συσκευών. Αν η πρόσβαση έχει οριστεί σε **Allow** (Να επιτρέπεται), ο επιλεγμένος χρήστης ή η ομάδα θα μπορούν να αποκτήσουν πρόσβαση σε οποιαδήποτε συσκευή σε αυτήν την κατηγορία συσκευών.
- Η προστασία μπορεί επίσης να εφαρμοστεί σε συγκεκριμένες συσκευές.
- Διαμορφώστε τις ρυθμίσεις του Just In Time authentication (JITA), για να επιτρέπετε σε επιλεγμένους χρήστες να αποκτήσουν πρόσβαση σε μονάδες δίσκων DVD/CD-ROM ή αφαιρούμενες μονάδες δίσκων επαληθεύοντας την ταυτότητά σας. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Διαμόρφωση ρυθμίσεων JITA στη σελίδα 51.
- Επιτρέψτε ή απαγορεύστε την πρόσβαση σε άλλες κατηγορίες συσκευών, όπως αφαιρούμενα μέσα (όπως μονάδες USB flash), σειριακές και παράλληλες θύρες, συσκευές Bluetooth®, συσκευές μόντεμ, συσκευές PCMCIA/ExpressCard, συσκευές 1394, αναγνώστες δακτυλικών αποτυπωμάτων και αναγνώστες έξυπνων καρτών. Αν απαγορευτεί η πρόσβαση σε αναγνώστες δακτυλικών αποτυπωμάτων και αναγνώστες έξυπνων καρτών, αυτές μπορούν να χρησιμοποιηθούν ως διαπιστευτήρια ελέγχου ταυτότητας αλλά δεν μπορούν να χρησιμοποιηθούν σε επίπεδο πολιτικής περιόδου λειτουργίας.

  ΣΗΜΕΙΩΣΗ Αν ως διαπιστευτήρια ελέγχου ταυτότητας χρησιμοποιούνται συσκευές Bluetooth, η πρόσβαση σε συσκευές Bluetooth δεν πρέπει να απαγορεύεται στην πολιτική του Device Access Manager.

- Όταν επιλέγετε μια ρύθμιση σε επίπεδο ομάδας ή κατηγορίας συσκευών και σας ζητείται να εφαρμόσετε τις ρυθμίσεις σε θυγατρικά επίπεδα:

  Yes (Ναι)—Η ρύθμιση θα μεταδοθεί.

  Yes (Όχι)—Η ρύθμιση δεν θα μεταδοθεί.

- Μερικές κατηγορίες συσκευών, όπως DVD και CD-ROM, ενδέχεται να ελέγχονται περαιτέρω έτσι ώστε να επιτρέπεται ή να απαγορεύεται ξεχωριστά η πρόσβαση για ανάγνωση ή εγγραφή.

  ΣΗΜΕΙΩΣΗ Η ομάδα διαχειριστών δεν μπορεί να προστεθεί στη λίστα χρηστών.

- **Access** (Πρόσβαση)—Κάντε κλικ ή πατήστε στο κάτω βέλος και, στη συνέχεια, επιλέξτε έναν από τους παρακάτω τύπους για να επιτρέψετε ή να απαγορεύσετε την πρόσβαση:
  - **Allow – Full Access** (Να επιτρέπεται – Πλήρης πρόσβαση)
  - **Allow – Read Only** (Να επιτρέπεται – Πρόσβαση μόνο για ανάγνωση)
  - **Allow – JITA Required** (Να επιτρέπεται – Απαιτείται JITA)—Για περισσότερες πληροφορίες βλέπε Διαμόρφωση ρυθμίσεων JITA στη σελίδα 51.

    Αν επιλέξετε αυτόν τον τύπο πρόσβασης, στην επιλογή **Duration** (Διάρκεια), κάντε κλικ ή πατήστε στο κάτω βέλος για να επιλέξετε ένα χρονικό όριο.
  - **Deny** (Να απαγορεύεται)
- **Duration** (Διάρκεια)—Κάντε κλικ ή πατήστε στο κάτω βέλος για να επιλέξετε ένα χρονικό όριο για πρόσβαση σε μονάδες δίσκου CD/DVD-ROM ή αφαιρούμενες μονάδες δίσκου (βλ. Διαμόρφωση ρυθμίσεων JITA στη σελίδα 51).

Διαμόρφωση ρυθμίσεων JITA

Η διαμόρφωση ρυθμίσεων του JITA επιτρέπει στο διαχειριστή να προβάλει και να τροποποιεί λίστες χρηστών και ομάδες στις οποίες επιτρέπεται η πρόσβαση σε συσκευές με χρήση του Just In Time Authentication (JITA).

Οι χρήστες με δυνατότητα JITA θα μπορούν να αποκτήσουν πρόσβαση σε μερικές συσκευές για τις οποίες οι πολιτικές που έχουν δημιουργηθεί στην προβολή **Device Class Configuration** (Διαμόρφωση ρυθμίσεων κατηγοριών συσκευών) τους την απαγορεύουν.

Η περίοδος JITA καθορίζεται για έναν καθορισμένο αριθμό λεπτών ή είναι απεριόριστη. Απεριόριστοι χρήστες θα έχουν πρόσβαση στη συσκευή από τη στιγμή της επαλήθευσης της ταυτότητάς τους έως την αποσύνδεσή τους από το σύστημα.

Αν στο χρήστη έχει δοθεί μια περιορισμένη χρονική περίοδος JITA, ένα λεπτό πριν τη λήξη της περιόδου JITA, ο χρήστης θα ερωτηθεί αν θέλει να επεκτείνει το χρονικό όριο. Μόλις ο χρήστης αποσυνδεθεί από το σύστημα ή συνδεθεί ένας άλλος χρήστης, η περίοδος JITA λήγει. Την επόμενη φορά που ο χρήστης συνδεθεί και επιχειρεί να προσπελάσει μια συσκευή με δυνατότητα JITA, θα του ζητηθεί να εισάγει τα διαπιστευτήριά του.

Η δυνατότητα JITA διατίθεται για τις ακόλουθες κατηγορίες συσκευών:

- Μονάδες δίσκων DVD/CD-ROM
- Μονάδες αφαιρούμενων δίσκων

Δημιουργία πολιτικής JITA για ένα χρήστη ή μια ομάδα

Οι διαχειριστές μπορούν επιτρέψουν σε χρήστες ή σε ομάδες την πρόσβαση σε συσκευές με χρήση του Just In Time Authentication (JITA).

1. Εκκινήστε το **Device Access Manager** και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Change** (Αλλαγή).
2. Επιλέξτε το χρήστη ή την ομάδα και, στη συνέχεια, στην επιλογή **Access** (Πρόσβαση) είτε για **Removable Disk drives** (Αφαιρούμενες μονάδες δίσκων) είτε για **DVD/CD-ROM drives** (Μονάδες DVD/CD-ROM), κάντε κλικ ή πατήστε στο κάτω βέλος και, στη συνέχεια, επιλέξτε **Allow – JITA Required** (Να επιτρέπεται – Απαιτείται JITA).
3. Στην επιλογή **Duration** (Διάρκεια), κάντε κλικ ή πατήστε στο κάτω βέλος για να επιλέξετε μια χρονική περίοδο για την πρόσβαση JITA.

Ο χρήστης πρέπει να αποσυνδεθεί και στη συνέχεια να συνδεθεί ξανά έτσι ώστε να τεθεί σε ισχύ η νέα ρύθμιση JITA.

Απενεργοποίηση πολιτικής JITA για ένα χρήστη ή μια ομάδα

Οι διαχειριστές μπορούν απενεργοποιήσουν την πρόσβαση σε συσκευές για χρήστες ή ομάδες με χρήση του Just In Time Authentication (JITA).

1. Εκκινήστε το **Device Access Manager** και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Change** (Αλλαγή).
2. Επιλέξτε το χρήστη ή την ομάδα και, στη συνέχεια, στην επιλογή **Access** (Πρόσβαση) είτε για **Removable Disk drives** (Αφαιρούμενες μονάδες δίσκων) είτε για **DVD/CD-ROM drives** (Μονάδες DVD/CD-ROM), κάντε κλικ ή πατήστε στο κάτω βέλος και, στη συνέχεια, επιλέξτε **Deny** (Να απαγορεύεται).

Όταν ο χρήστης συνδεθεί και επιχειρήσει να αποκτήσει πρόσβαση στη συσκευή, η πρόσβαση απαγορεύεται.

Ρυθμίσεις

Η προβολή **Settings** (Ρυθμίσεις) επιτρέπει στους διαχειριστές να εμφανίζουν και να αλλάζουν τις μονάδες δίσκων στις οποίες ισχύει ο έλεγχος πρόσβασης από το Device Access Manager.

ΣΗΜΕΙΩΣΗ Το Device Access Manager πρέπει να είναι ενεργοποιημένο όταν διαμορφώνονται οι ρυθμίσεις της λίστας με τα ονόματα των μονάδων δίσκων (βλ. Προβολή συστήματος στη σελίδα 49).

Κατηγορίες συσκευών χωρίς δυνατότητα ελέγχου

Το HP Device Access Manager δεν διαχειρίζεται τις ακόλουθες κατηγορίες συσκευών:

- Συσκευές εισόδου/εξόδου
  - CD-ROM
  - Οδηγούς δίσκων
  - Ελεγκτές δισκέτας (FDC)
  - Ελεγκτές σκληρών δίσκων (HDC)
  - Κατηγορίες συσκευών ανθρώπινης αλληλεπίδρασης (HID)
  - Συσκευές ανθρώπινης αλληλεπίδρασης με υπέρυθρη ακτινοβολία
  - Ποντίκι
  - Σειριακή πολλαπλή θύρα
  - πληκτρολόγιο
  - Εκτυπωτές τοποθέτησης και άμεσης λειτουργίας (PnP)
  - Εκτυπωτής
  - Αναβάθμιση εκτυπωτή
- λειτουργία
  - Διαχείριση ισχύος για προχωρημένους (APM)
  - Μπαταρία
- Διάφορα
  - Υπολογιστής
  - Αποκωδικοποιητής
  - Οθόνη
  - Ενοποιημένος οδηγός οθόνης της Intel®
  - Legacard
  - Οδηγός πολυμέσων
  - Συσκευή αλλαγής μέσων
  - Τεχνολογίες μνήμης
  - Οθόνη
  - Πολυλειτουργικές συσκευές

- Net client
- Net service
- Net trans
- Επεξεργαστής
- Τροφοδοτικό SCSI
- Επιταχυντής ασφαλείας
- Συσκευές ασφαλείας
- Σύστημα
- Άγνωστο
- Τόμος
- Στιγμιότυπο τόμου

8 HP Trust Circles

Το HP Trust Circles είναι μια εφαρμογή ασφαλείας αρχείων και εγγράφων, που συνδυάζει την κρυπτογράφηση φακέλων αρχείων με την εύκολη δυνατότητα κοινής χρήσης εγγράφων σε κύκλους εμπιστοσύνης. Η εφαρμογή κρυπτογραφεί αρχεία που βρίσκονται σε φακέλους συγκεκριμένων χρηστών, παρέχοντας προστασία μέσα σε έναν κύκλο εμπιστοσύνης. Έχοντας την προστασία, τα αρχεία μπορούν να χρησιμοποιηθούν και να τα μοιραστούν μόνο μέλη του κύκλου εμπιστοσύνης. Αν ένα προστατευμένο αρχείο παραληφθεί από ένα μη μέλος, το αρχείο παραμένει κρυπτογραφημένο και το μη μέλος δεν μπορεί να προσπελάσει τα περιεχόμενά του.

Άνοιγμα του Trust Circles

1. Στην οθόνη Έναρξη, κάντε κλικ ή πατήστε στην εφαρμογή **HP Client Security**.

   – ή –

   Από την επιφάνεια εργασίας των Windows, κάντε διπλό κλικ στο εικονίδιο του **HP Client Security** στην περιοχή ειδοποιήσεων που βρίσκεται στο δεξί άκρο της γραμμής εργαλείων.

2. Στην επιλογή **Data** (Δεδομένα), κάντε κλικ ή πατήστε στο **Trust Circles**.

Έναρξη χρήσης

Υπάρχουν δύο τρόποι να αποστείλετε προσκλήσεις μέσω ηλ. ταχυδρομείου και να απαντήσετε σε αυτές:

- **Χρήση του Microsoft® Outlook**—Η χρήση του Trust Circles με το Microsoft Outlook αυτοματοποιεί τη διαδικασία των προσκλήσεων του Trust Circle και των απαντήσεων από άλλους χρήστες του Trust Circle.
- **Χρήση Gmail, Yahoo, Outlook.com ή άλλων υπηρεσιών email (SMTP)**—Εισάγοντας το όνομα, τη διεύθυνση και τον κωδικό πρόσβασής σας, το Trust Circles χρησιμοποιεί την υπηρεσία email για αποστολή προσκλήσεων μέσω email στα επιλεγμένα μέλη για να συμμετάσχουν στον κύκλο εμπιστοσύνης.

Για να εγκαταστήσετε το βασικό σας προφίλ:

1. Εισαγάγετε το όνομα και τη διεύθυνση email και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Next** (Επόμενο).

   Το όνομα είναι ορατό στα μέλη που έχουν προσκληθεί να συμμετάσχουν στον κύκλο εμπιστοσύνης. Η διεύθυνση email χρησιμοποιείται για αποστολή, παραλαβή ή απάντηση σε προσκλήσεις.

2. Πληκτρολογήστε τον κωδικό πρόσβασης στο λογαριασμό σας email και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Next** (Επόμενο).

   Αποστέλλεται ένα δοκιμαστικό email για επιβεβαίωση ότι οι ρυθμίσεις email είναι ακριβείς.

ΣΗΜΕΙΩΣΗ Ο υπολογιστής πρέπει να είναι συνδεδεμένος σε δίκτυο.

3. Στο πεδίο **Trust Circle Name** (Όνομα Trust Circle), πληκτρολογήστε ένα όνομα για τον κύκλο εμπιστοσύνης και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Next** (Επόμενο).

4. Προσθέστε μέλη και φακέλους και, στη συνέχεια, κάντε κλικ στο **Next** (Επόμενο). Ο κύκλος εμπιστοσύνης έχει δημιουργηθεί και περιλαμβάνει τους φακέλους που επιλέξατε ενώ αποστέλλονται προσκλήσεις μέσω email στα μέλη που επιλέχτηκαν. Αν, για οποιοδήποτε λόγο, δεν μπορεί να σταλεί η πρόσκληση, εμφανίζεται μια ειδοποίηση. Μπορείτε να προσκαλέσετε ξανά τα μέλη οποιαδήποτε στιγμή από την προβολή του Trust Circle κάνοντας κλικ στο **Your Trust Circles** (Τα Trust Circles σας), και στη συνέχεια διπλό κλικ ή διπλό πάτημα στον κύκλο εμπιστοσύνης. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Trust Circles στη σελίδα 55.

Trust Circles

Μπορείτε να δημιουργήσετε έναν κύκλο εμπιστοσύνης κατά την αρχική εγκατάσταση αφού εισάγετε τη διεύθυνση email ή στην προβολή του Trust Circle:

▲ Από την προβολή του Trust Circle, κάντε κλικ ή πατήστε στο **Create Trust Circle** (Δημιουργία Trust Circle) και, στη συνέχεια, πληκτρολογήστε ένα όνομα για τον κύκλο εμπιστοσύνης.

- Για να προσθέσετε μέλη στον κύκλο εμπιστοσύνης, κάντε κλικ ή πατήστε στο εικονίδιο **M+** δίπλα στο **Members** (Μέλη) και, στη συνέχεια, ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.
- Για να προσθέσετε μέλη στον κύκλο εμπιστοσύνης, κάντε κλικ ή πατήστε στο εικονίδιο **+** δίπλα στο **Folders** (Φάκελοι) και, στη συνέχεια, ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Προσθήκη φακέλων σε έναν κύκλο εμπιστοσύνης

Προσθήκη φακέλων σε ένα νέο κύκλο εμπιστοσύνης:

- Κατά τη διάρκεια της δημιουργίας ενός κύκλου εμπιστοσύνης, μπορείτε να προσθέσετε φακέλους κάνοντας κλικ ή πατώντας στο εικονίδιο **+** δίπλα στο **Folders** (Φάκελοι) και, στη συνέχεια, ακολουθώντας τις οδηγίες που εμφανίζονται στην οθόνη.

  – ή –

- Στο Windows Explorer, κάντε δεξί κλικ ή πατήστε και κρατήστε πατημένο ένα φάκελο που δεν ανήκει στον κύκλο εμπιστοσύνης, επιλέξτε **Trust Circle** και, στη συνέχεια, επιλέξτε **Create Trust Circle from Folder** (Δημιουργία Trust Circle από φάκελο).

ΥΠΟΔΕΙΞΗ Μπορείτε να επιλέξετε έναν ή περισσότερους φακέλους.

Προσθήκη φακέλων σε έναν υπάρχοντα Trust Circle:

- Από την προβολή του Trust Circle, κάντε κλικ στο **Your Trust Circles** (Τα Trust Circles σας), κάντε διπλό κλικ ή διπλό πάτημα στον υπάρχοντα κύκλο εμπιστοσύνης για να εμφανιστούν οι φάκελοι, κάντε κλικ ή πατήστε στο εικονίδιο **+** δίπλα στο **Folders** (Φάκελοι) και, στη συνέχεια, ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

  – ή –

- Στο Windows Explorer, κάντε δεξί κλικ ή πατήστε και κρατήστε πατημένο ένα φάκελο που δεν ανήκει στον κύκλο εμπιστοσύνης, επιλέξτε **Trust Circle** και, στη συνέχεια, επιλέξτε **Add to existing Trust Circle from Folder** (Προσθήκη σε υπάρχοντα Trust Circle από φάκελο).

ΥΠΟΔΕΙΞΗ Μπορείτε να επιλέξετε έναν ή περισσότερους φακέλους.

Όταν ένας φάκελος έχει προστεθεί σε έναν κύκλο εμπιστοσύνης, το Trust Circles κρυπτογραφεί αυτόματα το φάκελο και τα περιεχόμενά του. Όταν έχουν κρυπτογραφηθεί όλα τα αρχεία, εμφανίζεται μια ειδοποίηση. Επιπλέον, εμφανίζεται ένα πράσινο σύμβολο κλειδαριάς σε όλα τα εικονίδια των κρυπτογραφημένων φακέλων και αρχείων μέσα στους φακέλους που υποδεικνύει ότι διαθέτουν πλήρη προστασία.

Προσθήκη μελών σε έναν κύκλο εμπιστοσύνης

Απαιτούνται τρία βήματα για να προσθέσετε μέλη σε έναν κύκλο εμπιστοσύνης:

1. **Invite** (Πρόσκληση)—Αρχικά, ο ιδιοκτήτης του κύκλου εμπιστοσύνης προσκαλεί τα μέλη. Η πρόσκληση μέσω email μπορεί να αποσταλεί σε πολλαπλούς χρήστες ή σε λίστες/ομάδες διανομής.
2. **Accept** (Αποδοχή)—Ο προσκεκλημένος παραλαμβάνει την πρόσκληση και επιλέγει αν θα την αποδεχτεί ή θα την απορρίψει. Αν ο προσκεκλημένος αποδεχτεί την πρόσκληση αποστέλλεται στον αποστολέα απάντηση μέσω email. Αν η πρόσκληση σταλεί σε ομάδα, κάθε μέλος της ομάδας λαμβάνει μια πρόσκληση και επιλέγει αν θα την αποδεχτεί ή θα την απορρίψει.
3. **Enroll** (Δήλωση)—Ο προσκαλών έχει την τελική δυνατότητα να αποφασίσει αν θα προσθέσει ένα μέλος στον κύκλο εμπιστοσύνης. Αν ο προσκαλών αποφασίσει να δηλώσει το μέλος, στον προσκεκλημένο αποστέλλεται ένα email επιβεβαίωσης. Ο προσκαλών και ο προσκεκλημένος μπορούν προαιρετικά να επαληθεύσουν την ασφάλεια της διαδικασίας πρόσκλησης. Για τον προσκεκλημένο εμφανίζεται ένας κωδικός επαλήθευσης, τον οποίο πρέπει να διαβάσει στον προσκαλούντα από το τηλέφωνο. Όταν ο κωδικός επαληθευτεί, ο προσκαλών μπορεί να στείλει το τελικό email δήλωσης.

Προσθήκη μελών σε ένα νέο κύκλο εμπιστοσύνης:

▲ Κατά τη διάρκεια της δημιουργίας ενός κύκλου εμπιστοσύνης, μπορείτε να προσθέσετε μέλη κάνοντας κλικ ή πατώντας στο εικονίδιο **M+** δίπλα στο **Members** (Μέλη) και, στη συνέχεια, ακολουθώντας τις οδηγίες που εμφανίζονται στην οθόνη.

- Αν χρησιμοποιείτε Outlook, επιλέξτε επαφές από το βιβλίο διευθύνσεων του Outlook, και στη συνέχεια, κάντε κλικ στο **OK**
- Αν χρησιμοποιείτε άλλη υπηρεσία email, είτε πληκτρολογήστε νέες διευθύνσεις email στο Trust Circle, είτε μπορείτε να τις ανακτήσετε από τις διευθύνσεις email που είναι καταχωρημένες στο Trust Circle.

Προσθήκη φακέλων σε ένα υπάρχοντα Trust Circle:

▲ Από την προβολή του Trust Circle, κάντε κλικ στο **Your Trust Circles** (Τα Trust Circles σας), κάντε διπλό κλικ ή διπλό πάτημα στον υπάρχοντα κύκλο εμπιστοσύνης για να εμφανιστούν τα μέλη, κάντε κλικ ή πατήστε στο εικονίδιο **M+** δίπλα στο **Members** (Μέλη) και, στη συνέχεια, ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

- Αν χρησιμοποιείτε Outlook, επιλέξτε επαφές από το βιβλίο διευθύνσεων του Outlook, και στη συνέχεια, κάντε κλικ στο **OK**
- Αν χρησιμοποιείτε άλλη υπηρεσία email, είτε πληκτρολογήστε νέες διευθύνσεις email στο Trust Circle, είτε μπορείτε να τις ανακτήσετε από τις διευθύνσεις email που είναι καταχωρημένες στο Trust Circle.

Προσθήκη αρχείων σε έναν κύκλο εμπιστοσύνης

Μπορείτε να προσθέσετε αρχεία σε έναν κύκλο εμπιστοσύνης με έναν από τους παρακάτω τρόπους:

- Αντιγράψτε ή μετακινήστε το αρχείο από έναν φάκελο δημιουργημένου κύκλου εμπιστοσύνης.

  – ή –

- Στην Εξερεύνηση των Windows, κάντε δεξί κλικ ή πατήστε παρατεταμένα ένα αρχείο που δεν είναι κρυπτογραφημένο, επιλέξτε **Trust Circle**και, στη συνέχεια, επιλέξτε **Κρυπτογράφηση**. Θα σας ζητηθεί να επιλέξετε τον κύκλο εμπιστοσύνης στον οποίο θέλετε να προσθέσετε το αρχείο.

ΥΠΟΔΕΙΞΗ Μπορείτε να επιλέξετε ένα ή περισσότερα αρχεία.

Κρυπτογραφημένοι φάκελοι

Οποιοδήποτε μέλος ενός κύκλου εμπιστοσύνης μπορεί να προβάλει και να επεξεργάζεστε αρχεία που ανήκουν σε αυτόν τον κύκλο εμπιστοσύνης.

ΣΗΜΕΙΩΣΗ Το Trust Circle Manager/Reader δεν συγχρονίζει τα αρχεία μεταξύ των μελών.

Η κοινή χρήση των αρχείων πρέπει να γίνεται με τα τρέχοντα μέσα, όπως email, ftp ή παρόχους υπηρεσιών αποθήκευσης cloud. Τα αρχεία που αντιγράφονται, μετακινούνται ή δημιουργούνται σε έναν κύκλο εμπιστοσύνης προστατεύονται αμέσως.

Διαγραφή φακέλων από έναν κύκλο εμπιστοσύνης

Η διαγραφή ενός φακέλου από έναν κύκλο εμπιστοσύνης αποκρυπτογραφεί όλα του τα περιεχόμενα και αφαιρεί την προστασία.

- Από την προβολή του Trust Circle, κάντε κλικ ή πατήστε στο **Your Trust Circles** (Τα Trust Circles σας), κάντε διπλό κλικ ή διπλό πάτημα στον υπάρχοντα κύκλο εμπιστοσύνης για να εμφανιστούν οι φάκελοι και, στη συνέχεια, κάντε κλικ ή πατήστε στο εικονίδιο **trash can** (κάδος απορριμάτων) δίπλα στον φάκελο.

  – ή –

- Στο Windows Explorer, κάντε δεξί κλικ ή πατήστε και κρατήστε πατημένο ένα φάκελο που ανήκει στον κύκλο εμπιστοσύνης, επιλέξτε **Trust Circle** και, στη συνέχεια, επιλέξτε **Remove from trust circle** (Διαγραφή από το Trust Circle).

ΥΠΟΔΕΙΞΗ Μπορείτε να επιλέξετε έναν ή περισσότερους φακέλους.

Διαγραφή αρχείου από έναν κύκλο εμπιστοσύνης

Για να καταργήσετε ένα αρχείο από έναν αξιόπιστο κύκλο στην Εξερεύνηση των Windows, κάντε δεξί κλικ ή πατήστε παρατεταμένα ένα αρχείο που δεν είναι κρυπτογραφημένο τη δεδομένη στιγμή, επιλέξτε **Trust Circle**, επιλέξτε **Αποκρυπτογράφηση αρχείου**.

Διαγραφή μελών από έναν κύκλο εμπιστοσύνης

Ένα πλήρως δηλωμένο μέλος δεν μπορεί να διαγραφεί από τον κύκλο εμπιστοσύνης. Μια εναλλακτική θα ήταν να δημιουργηθεί ένας νέος κύκλος εμπιστοσύνης με όλα τα άλλα μέλη, να μετακινηθούν όλα τα αρχεία και οι φάκελοι σε αυτόν και να διαγραφεί ο παλιός κύκλος εμπιστοσύνης. Αυτό θα διασφαλίσει ότι τυχόν νέα αρχεία που λαμβάνει το μέλος δεν είναι προσπελάσιμα, αλλά οτιδήποτε ήταν κοινόχρηστο προηγουμένως παραμένει προσπελάσιμο από το μέλος του παλιού κύκλου εμπιστοσύνης.

Αν ένα μέλος δεν είναι πλήρως δηλωμένο (είτε το μέλος έχει προσκληθεί να συμμετάσχει στον κύκλο εμπιστοσύνης είτε δεν έχει αποδεχτεί τη συμμετοχή του στον κύκλο εμπιστοσύνης), μπορείτε να διαγράψετε το μέλος από τον κύκλο εμπιστοσύνης με έναν από τους παρακάτω τρόπους:

- Από την προβολή του Trust Circle, κάντε κλικ ή πατήστε στο **Your Trust Circles** (Τα Trust Circles σας) και, στη συνέχεια κάντε διπλό κλικ ή διπλό πάτημα στον κύκλο εμπιστοσύνης για να εμφανιστεί η τρέχουσα λίστα μελών. Κάντε κλικ ή πατήστε στο εικονίδιο **trash can** (κάδος απορριμμάτων) δίπλα στο όνομα του μέλους που θέλετε να διαγράψετε.
- Από την προβολή του Trust Circle, κάντε κλικ ή πατήστε στο **Members** (Μέλη) και, στη συνέχεια κάντε διπλό κλικ ή διπλό πάτημα στο μέλος για να εμφανιστούν οι κύκλοι εμπιστοσύνης στους οποίους συμμετέχει. Κάντε κλικ ή πατήστε στο εικονίδιο **trash can** (κάδος απορριμμάτων) δίπλα σε έναν κύκλο εμπιστοσύνης για να διαγράψετε το μέλος από αυτόν τον κύκλο εμπιστοσύνης.

Διαγραφή ενός κύκλου εμπιστοσύνης

Για να διαγράψετε έναν κύκλο εμπιστοσύνης απαιτείται να είστε ιδιοκτήτης του.

▲ Από την προβολή του Trust Circle, κάντε κλικ ή πατήστε στο **Your Trust Circles** (Τα Trust Circles σας), κάντε κλικ ή πατήστε στο εικονίδιο **trash can** (κάδος απορριμμάτων) δίπλα από τον κύκλο εμπιστοσύνης που θέλετε να διαγράψετε.

Με αυτόν τον τρόπο ο κύκλος εμπιστοσύνης διαγράφεται από τη σελίδα και σε όλα τα μέλη αποστέλλονται email που τους ενημερώνουν ότι ο κύκλος εμπιστοσύνης έχει διαγραφεί. Τα αρχεία και οι φάκελοι σε αυτόν τον κύκλο εμπιστοσύνης αποκρυπτογραφούνται.

Ρυθμίσεις προτιμήσεων

Από την προβολή του Trust Circle, κάντε κλικ ή πατήστε στο **Preferences** (Προτιμήσεις). Εμφανίζονται τρεις καρτέλες

- **Email Settings** (Ρυθμίσεις Email)

Επιλογή	Περιγραφή
Όνομα χρήστη	Εμφανίζεται το τρέχον όνομα χρήστη. Για να το αλλάξετε, πληκτρολογήστε ένα νέο όνομα χρήστη στο πλαίσιο κειμένου. Οι αλλαγές αποθηκεύονται αυτόματα.
Διεύθυνση Email	Εμφανίζεται ο τρέχων λογαριασμός email. Για να τον αλλάξετε, κάντε κλικ ή πατήστε στο **Change Email Settings** (Αλλαγή ρυθμίσεων Email) και, στη συνέχεια, ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.
Επιβεβαίωση νέου μέλους	Επιλέξτε από τα ακόλουθα: ◦ **Confirm Automatically** (Αυτόματη επιβεβαίωση)—Μετά τη λήψη αποδοχής από τον προσκεκλημένο, η επιβεβαίωση συμμετοχής στον κύκλο εμπιστοσύνης γίνεται αυτόματα και στον προσκεκλημένο αποστέλλεται ένα email επιβεβαίωσης. ◦ **Confirm Manually** (Μη αυτόματη επιβεβαίωση)—Μετά τη λήψη αποδοχής από τον προσκεκλημένο, απαιτείται η δήλωση με εισαγωγή του νέου μέλους στον κύκλο εμπιστοσύνης και στη συνέχεια αποστέλλεται στον προσκεκλημένο ένα email επιβεβαίωσης. ◦ **Require Verification** (Απαιτείται επαλήθευση)—Μετά τη λήψη αποδοχής από τον προσκεκλημένο, απαιτείται κωδικός επιβεβαίωσης για την πλήρη δήλωση του προσκεκλημένου. Ο ιδιοκτήτης του κύκλου εμπιστοσύνης πρέπει να έρθει σε επαφή με τους προσκεκλημένους και να λάβει από αυτούς τον κωδικό επαλήθευσης. Μετά από την εισαγωγή του κωδικού επαλήθευσης, αποστέλλονται τα email επιβεβαίωσης.

Επιλογή	Περιγραφή
Περιοδικός έλεγχος ταυτότητας	Ο περιοδικός έλεγχος ταυτότητας απαιτεί από το χρήστη να εισάγει τον κωδικό πρόσβασης των Windows μετά την καθορισμένη χρονική διάρκεια (σε λεπτά) καθώς και όταν εκτελεί ευαίσθητες λειτουργίες. Αυτή η ρύθμιση επιτρέπει στους χρήστες να ενεργοποιήσουν ή να απενεργοποιήσουν τον έλεγχο ταυτότητας.
Χρονική διάρκεια ελέγχου ταυτότητας	Επιλέξτε τη συγκεκριμένη χρονική διάρκεια (σε λεπτά) που θα μεσολαβήσει πριν από την απαίτηση ελέγχου ταυτότητας.
Να μην εμφανίζεται μήνυμα επιβεβαίωσης	Επιλέξτε το πλαίσιο ελέγχου για να απενεργοποιήσετε την εμφάνιση μηνυμάτων επιβεβαίωσης, ή καταργήστε την επιλογή για να εμφανίζονται τα μηνύματα επιβεβαίωσης.
Θέλω να βοηθήσω στη βελτίωση του HP Trust Circle μέσω ανώνυμης παρακολούθησης χρήσης	Επιλέξτε το πλαίσιο ελέγχου για να συμμετάσχετε στο πρόγραμμα ή καταργήστε την επιλογή αν δεν θέλετε να συμμετάσχετε.

- **Backup/Restore** (Δημιουργία αντιγράφων ασφαλείας/Επαναφορά)

Επιλογή	Περιγραφή
Δημιουργία αντιγράφων ασφαλείας	Αντιγράφει τα δεδομένα της εφαρμογής Trust Circle Manager/Reader (ρυθμίσεις και κύκλους εμπιστοσύνης) σε ένα αρχείο αντιγράφου ασφαλείας. Σε περίπτωση καταστροφής ή σφάλματος συστήματος, μπορείτε να χρησιμοποιήσετε αυτό το αρχείο για επαναφορά της νέας εγκατάστασης του Trust Circles στην κατάσταση που είναι αποθηκευμένη στο αρχείο. **ΣΗΜΕΙΩΣΗ** Αποθηκεύονται μόνο τα δεδομένα της εφαρμογής Trust Circle (κύκλοι εμπιστοσύνης, ρυθμίσεις και μέλη). Τα πραγματικά αρχεία στους φακέλους του κύκλου εμπιστοσύνης δεν αντιγράφονται. Για αυτά τα αρχεία πρέπει να δημιουργηθούν ξεχωριστά αντίγραφα ασφαλείας. Για να δημιουργήσετε αντίγραφα ασφαλείας των ρυθμίσεων του Trust Circle και των δεδομένων των χρηστών: 1. Κάντε κλικ ή πατήστε στο **Backup** (Δημιουργία αντιγράφου ασφαλείας). 2. Επιλέξτε ένα όνομα αρχείου και έναν κατάλογο για το αρχείο αντιγράφου ασφαλείας και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Save** (Αποθήκευση). 3. Εισαγάγετε έναν κωδικό πρόσβασης, επιβεβαιώστε τον και, στη συνέχεια κάντε κλικ ή πατήστε στο **OK**. Για να επαναφέρετε το αρχείο θα χρειαστεί αυτός ο κωδικός πρόσβασης.
Επαναφορά	Επαναφέρει ρυθμίσεις και κύκλους εμπιστοσύνης από ένα αρχείο αντιγράφου ασφαλείας, μετά από μια καταστροφή συστήματος ή μετεγκατάσταση σε άλλον υπολογιστή. Για να επαναφέρετε τις ρυθμίσεις και τα δεδομένα χρηστών του Trust Circle Manager. 1. Κάντε κλικ ή πατήστε στο **Restore** (Επαναφορά). 2. Αναζητήστε στον κατάλογο το όνομα του αρχείου αντιγράφου ασφαλείας και, στη συνέχεια, κάντε κλικ ή πατήστε στο **Open** (Άνοιγμα). 3. Εισαγάγετε τον κωδικό πρόσβασης που καταχωρήσατε όταν δημιουργήσατε το αντίγραφο ασφαλείας.

- **About** (Πληροφορίες)—Εμφανίζεται η έκδοση του λογισμικού Trust Circle Manager/Reader. Εμφανίζονται σύνδεσμοι που σας επιτρέπουν να αναβαθμίσετε το Trust Circle Manager στην έκδοση Pro ή να προβάλετε τη δήλωση απορρήτου της HP.

9 Theft recovery (μόνο σε επιλεγμένα μοντέλα)

Το Computrace (πωλείται ξεχωριστά) σάς επιτρέπει να πραγματοποιείτε απομακρυσμένη παρακολούθηση, διαχείριση και καταγραφή αρχείου του υπολογιστή σας.

Μόλις ενεργοποιηθεί, το Computrace διαμορφώνεται από το Absolute Software Customer Center. Από το Customer Center, ο διαχειριστής μπορεί να διαμορφώσει το Computrace για την παρακολούθηση ή διαχείριση του υπολογιστή. Εάν το σύστημα έχει χαθεί ή κλαπεί, το Customer Center μπορεί να βοηθήσει τις τοπικές αρχές στον εντοπισμό και την ανάκτηση του υπολογιστή. Εάν έχει διαμορφωθεί, το Computrace μπορεί να συνεχίσει να λειτουργεί ακόμα και αν ο σκληρός δίσκος διαγραφεί ή αντικατασταθεί.

Για να ενεργοποιήσετε το Computrace:

1. Σύνδεση στο Internet.
2. Άνοιγμα του HP Client Security. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Άνοιγμα του HP Client Security στη σελίδα 11.
3. Κάντε κλικ στην επιλογή **Theft Recovery**.
4. Για να εκκινήσετε τον οδηγό ενεργοποίηση του Computrace, κάντε κλικ στο **Έναρξη**.
5. Εισαγάγετε τα στοιχεία επικοινωνίας και την πιστωτική σας κάρτα ή εισαγάγετε ένα προπληρωμένο αριθμό-κλειδί προϊόντος.

Ο οδηγός ενεργοποίησης επεξεργάζεται με ασφάλεια τη συναλλαγή και ρυθμίζει τον λογαριασμό χρήστη για τον ιστότοπο του Absolute Software Customer Center. Όταν ολοκληρωθεί η διαδικασία, θα λάβετε ένα email επιβεβαίωσης που περιέχει τις πληροφορίες του λογαριασμού Customer Center.

Εάν έχετε ήδη εκτελέσει τον οδηγό ενεργοποίησης του Computrace και ο λογαριασμός χρήστη στο Customer Center υπάρχει ήδη, μπορείτε να αγοράσετε πρόσθετες άδειες χρήσης, επικοινωνώντας με τον αντιπρόσωπο λογαριασμών της HP.

Για να συνδεθείτε με το Customer Center:

1. Επισκεφτείτε τη διεύθυνση https://cc.absolute.com/.
2. Στα πεδία **Αναγνωριστικό σύνδεσης** και **Κωδικός πρόσβασης**, πληκτρολογήστε τα διαπιστευτήρια που λάβατε στο email επιβεβαίωσης και, στη συνέχεια, κάντε κλικ στην επιλογή **Σύνδεση**.

Χρησιμοποιώντας το Customer Center μπορείτε να κάνετε τα εξής:

- Παρακολούθηση των υπολογιστών σας.
- Προστασία των απομακρυσμένων δεδομένων.
- Αναφορά της κλοπής οποιουδήποτε υπολογιστή προστατεύεται από το Computrace.

▲ Κάντε κλικ στην επιλογή **Περισσότερες πληροφορίες** για περισσότερες πληροφορίες σχετικά με το Computrace.

10 Εξαιρέσεις τοπικών κωδικών πρόσβασης

Στο επίπεδο ελέγχου ταυτότητας κατά την εκκίνηση και στο επίπεδο του HP Drive Encryption, η υποστήριξη τοπικών κωδικών πρόσβασης είναι περιορισμένη. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα IME των Windows δεν υποστηρίζονται στο επίπεδο ελέγχου ταυτότητας κατά την εκκίνηση ή στο επίπεδο του Drive Encryption στη σελίδα 61.

Τι να κάνετε όταν απορρίπτεται ο κωδικός πρόσβασης

Οι κωδικοί πρόσβασης μπορεί να απορριφθούν για τους εξής λόγους:

- Ο χρήστης χρησιμοποιεί IME που δεν υποστηρίζεται. Αυτό είναι σύνηθες πρόβλημα με τις γλώσσες διπλού byte (Κορεάτικα, Ιαπωνικά, Κινέζικα). Για να επιλύσετε αυτό το πρόβλημα:

  1. Από τον **Πίνακα ελέγχου**, προσθέστε μια υποστηριζόμενη διάταξη πληκτρολογίου (προσθέστε πληκτρολόγια ΗΠΑ/Αγγλικά στην κινέζικη γλώσσα εισαγωγής).
  2. Ορίστε το υποστηριζόμενο πληκτρολόγιο για την προεπιλεγμένη εισαγωγή.
  3. Εκκινήστε το HP Client Security και πληκτρολογήστε τον κωδικό πρόσβασης των Windows.

- Ο χρήστης χρησιμοποιεί έναν χαρακτήρα που δεν υποστηρίζεται. Για να επιλύσετε αυτό το πρόβλημα:

  1. Αλλάξτε τον κωδικό πρόσβασης των Windows έτσι ώστε να χρησιμοποιούνται μόνο υποστηριζόμενοι χαρακτήρες. Για περισσότερες πληροφορίες σχετικά με τους χαρακτήρες που δεν υποστηρίζονται, βλ. Χειρισμός ειδικών πλήκτρων στη σελίδα 63.
  2. Εκκινήστε το HP Client Security και πληκτρολογήστε τον κωδικό πρόσβασης των Windows.

IME των Windows δεν υποστηρίζονται στο επίπεδο ελέγχου ταυτότητας κατά την εκκίνηση ή στο επίπεδο του Drive Encryption

Στα Windows, ο χρήστης μπορεί να επιλέξει ένα IME (input method editor-επεξεργαστή μεθόδου εισαγωγής) για να εισάγει σύνθετους χαρακτήρες και σύμβολα όπως γιαπωνέζικους και κινέζικους χαρακτήρες χρησιμοποιώντας ένα τυπικό δυτικό πληκτρολόγιο.

Τα IME δεν υποστηρίζονται στο επίπεδο ελέγχου ταυτότητας κατά την εκκίνηση ή στο επίπεδο του Drive Encryption. Δεν μπορείτε να πληκτρολογήσετε έναν κωδικό πρόσβασης στα Windows με IME στην οθόνη σύνδεσης με έλεγχο ταυτότητας κατά την εκκίνηση ή στο Drive Encryption και στην περίπτωση που το κάνετε ενδέχεται να συμβεί μπλοκάρισμα. Σε ορισμένες περιπτώσεις, τα Microsoft® Windows δεν εμφανίζουν το IME όταν ο χρήστης εισάγει τον κωδικό πρόσβασης.

Η λύση είναι η αλλαγή σε μια από τις ακόλουθες υποστηριζόμενες διατάξεις πληκτρολογίου που μεταφράζει σε διάταξη πληκτρολογίου 00000411:

- Microsoft IME για Ιαπωνικά
- Διάταξη γιαπωνέζικου πληκτρολογίου
- Office 2007 IME για Ιαπωνικά—Αν η Microsoft ή ένας τρίτος κατασκευαστής χρησιμοποιεί τον όρο IME ή τον επεξεργαστή μεθόδου εισαγωγής, η μέθοδος εισαγωγής ενδέχεται να μην είναι πραγματικά IME. Αυτό μπορεί να προκαλέσει σύγχυση, αλλά το λογισμικό διαβάζει την αντιπροσώπευση δεκαεξαδικού κώδικα. Έτσι, αν το IME αντιστοιχίζει σε μια υποστηριζόμενη διάταξη πληκτρολογίου, τότε το HP Client Security μπορεί να υποστηρίξει τη ρύθμιση.

ΠΡΟΕΙΔ/ΣΗ! Όταν χρησιμοποιείται το HP Client Security, οι κωδικοί πρόσβασης που εισάγονται με Windows IME θα απορρίπτονται.

Αλλαγές κωδικών πρόσβασης με χρήση διάταξης πληκτρολογίου που επίσης υποστηρίζεται

Αν ο κωδικός πρόσβασης έχει αρχικά οριστεί με μια διάταξη πληκτρολογίου, όπως Αγγλικά ΗΠΑ (409) και στη συνέχεια ο χρήστης αλλάξει τον κωδικό πρόσβασης χρησιμοποιώντας μια διαφορετική διάταξη πληκτρολογίου που επίσης υποστηρίζεται, όπως το Λατινοαμερικάνικο (080A), η αλλαγή του κωδικού πρόσβασης θα λειτουργεί στο HP Drive Encryption, αλλά θα αποτύχει στο BIOS αν ο χρήστης χρησιμοποιεί χαρακτήρες που υπάρχουν στο δεύτερο αλλά όχι στο πρώτο (π.χ., ē).

ΣΗΜΕΙΩΣΗ Οι διαχειριστές μπορούν να επιλύσουν αυτό το πρόβλημα από τη σελίδα Χρήστες του HP Client Security (πρόσβαση από το εικονίδιο **Gear** στην αρχική σελίδα) για να διαγράψουν το χρήστη από το HP Client Security, επιλέγοντας την επιθυμητή διάταξη πληκτρολογίου στο λειτουργικό σύστημα και στη συνέχεια εκτελώντας ξανά τον οδηγό εγκατάστασης του HP Client Security για τον ίδιο χρήστη. Το BIOS αποθηκεύει την επιθυμητή διάταξη πληκτρολογίου και οι κωδικοί πρόσβασης που θα πληκτρολογηθούν με αυτή τη διάταξη πληκτρολογίου θα οριστούν κανονικά στο BIOS.

Ένα άλλο δυνητικό πρόβλημα είναι η χρήση διαφορετικών διατάξεων πληκτρολογίου που μπορούν όλα να δημιουργήσουν τους ίδιους χαρακτήρες. Π.χ., τόσο η διάταξη πληκτρολογίου Διεθνής ΗΠΑ (20409) και η διάταξη λατινοαμερικάνικου πληκτρολογίου (080A) μπορούν να παράγουν το χαρακτήρα é, παρόλο που μπορεί να απαιτούνται διαφορετικές ακολουθίες πληκτρολογήσεων. Αν ο κωδικός πρόσβασης έχει οριστεί αρχικά με τη διάταξη λατινοαμερικάνικου πληκτρολογίου, τότε η διάταξη λατινοαμερικάνικου πληκτρολογίου έχει οριστεί στο BIOS, ακόμη κι αν ο κωδικός πρόσβασης στη συνέχεια αλλάξει χρησιμοποιώντας τη διάταξη πληκτρολογίου Διεθνής ΗΠΑ.

Χειρισμός ειδικών πλήκτρων

- Κινέζικα, Σλοβάκικα, Γαλλικά Καναδά και Τσέχικα

  Όταν ο χρήστης επιλέγει μία από τις παραπάνω διατάξεις πληκτρολογίου και στη συνέχεια καταχωρίζει στο σύστημα έναν κωδικό πρόσβασης (για παράδειγμα, abcdef), ο ίδιος κωδικός πρόσβασης πρέπει να εισαχθεί πατώντας ταυτόχρονα το πλήκτρο shift για πεζά και το shift και το πλήκτρο caps lock για κεφαλαία στον έλεγχο ταυτότητας κατά την εκκίνηση και το HP Drive Encryption. Οι αριθμητικοί κωδικοί πρόσβασης πρέπει να καταχωρηθούν από το αριθμητικό πληκτρολόγιο.

- Κορεάτικα

  Όταν ο χρήστης επιλέγει μια διάταξη πληκτρολογίου που υποστηρίζει κορεάτικα και στη συνέχεια καταχωρίζει στο σύστημα έναν κωδικό πρόσβασης, ο ίδιος κωδικός πρόσβασης πρέπει να εισαχθεί πατώντας ταυτόχρονα το δεξί πλήκτρο alt για πεζά και το δεξί πλήκτρο alt και το πλήκτρο caps lock για κεφαλαία στον έλεγχο ταυτότητας κατά την εκκίνηση και το HP Drive Encryption.

- Οι μη υποστηριζόμενοι χαρακτήρες παρατίθενται στον πίνακα που ακολουθεί:

Language (Γλώσσα)	Windows	BIOS	Drive Encryption
Αραβικά	Τα πλήκτρα ٫ ,٬ και ٭ δημιουργούν δύο χαρακτήρες.	Τα πλήκτρα ٫ ,٬ και ٭ δημιουργούν ένα χαρακτήρα.	Τα πλήκτρα ٫ ,٬ και ٭ δημιουργούν ένα χαρακτήρα.
Γαλλικά Καναδά	Τα ç, è, à και é με caps lock είναι Ç, È, À και É στα Windows.	Τα ç, è, à και é με caps lock είναι ç, è, à και é στον έλεγχο ταυτότητας κατά την εκκίνηση.	Τα ç, è, à και é με caps lock είναι ç, è, à και é στο HP Drive Encryption.
Ισπανικά	Το 40a δεν υποστηρίζεται. Όμως παρόλα αυτά λειτουργεί γιατί το λογισμικό το μετατρέπει σε c0a. Ωστόσο, λόγω των μικρών διαφορών μεταξύ των διατάξεων πληκτρολογίου, συνιστάται οι ισπανόφωνοι χρήστες να αλλάζουν τη διάταξη πληκτρολογίου των Windows σε 1040a (ισπανική παραλλαγή) ή σε 080a (λατινοαμερικάνικη παραλλαγή).	μ/δ	μ/δ
Διεθνές ΗΠΑ	◦ Τα πλήκτρα ¡, ¤, ‘, ’, ¥ και × στην πάνω σειρά απορρίπτονται. ◦ Τα πλήκτρα å, ® και Þ στη δεύτερη σειρά απορρίπτονται. ◦ Τα πλήκτρα á, ð και ø στην τρίτη σειρά απορρίπτονται. ◦ Το πλήκτρο æ στην κάτω σειρά απορρίπτεται.	μ/δ	μ/δ

Language (Γλώσσα)	Windows	BIOS	Drive Encryption
Τσέχικα	◦ Το πλήκτρο ğ απορρίπτεται. ◦ Το πλήκτρο į απορρίπτεται. ◦ Το πλήκτρο ų απορρίπτεται. ◦ Τα πλήκτρα ė, ı και ż απορρίπτονται. ◦ Τα πλήκτρα ģ, ķ, ļ, ņ και ţ απορρίπτονται.	μ/δ	μ/δ
Σλοβάκικα	Το πλήκτρο ż απορρίπτεται.	◦ Τα πλήκτρα š, ś και ş απορρίπτονται όταν πληκτρολογούνται, αλλά γίνονται αποδεκτά όταν εισάγονται με το εικονικό πληκτρολόγιο. ◦ Το νεκρό πλήκτρο ţ δημιουργεί δύο χαρακτήρες.	μ/δ
Ουγγρικά	Το πλήκτρο ż απορρίπτεται.	Το πλήκτρο ţ δημιουργεί δύο χαρακτήρες.	μ/δ
Σλοβένικα	Το πλήκτρο żŻ απορρίπτεται στα Windows και το πλήκτρο alt δημιουργεί ένα νεκρό πλήκτρο στο BIOS.	Τα πλήκτρα ú, Ú, ů, Ů, ş, Ş, ś, Ś, š και Š απορρίπτονται στο BIOS.	μ/δ
Japanese (Ιαπωνικά)	Όταν διατίθεται, το IME του Microsoft Office 2007 είναι καλύτερη επιλογή. Παρά την ονομασία IME, είναι στην πραγματικότητα διάταξη πληκτρολογίου 411, που υποστηρίζεται.	μ/δ	μ/δ

Γλωσσάρι

αποκρυπτογράφηση
Μια διαδικασία που χρησιμοποιείται στην κρυπτογραφία για τη μετατροπή κρυπτογραφημένων δεδομένων σε απλό κείμενο.

αρχείο επείγουσας ανάκτησης
Ένας προστατευμένος χώρος αποθήκευσης που επιτρέπει την επανακρυπτογράφηση των κλειδιών βασικού χρήστη από το ένα κλειδί κατόχου πλατφόρμας στο άλλο.

Αρχική σελίδα
Μια κεντρική τοποθεσία από όπου μπορείτε να αποκτήσετε πρόσβαση και να διαχειριστείτε τις λειτουργίες και τις ρυθμίσεις στο HP Client Security.

αυτόματη μόνιμη διαγραφή
Καταστροφή την οποία εσείς προγραμματίζετε στο File Sanitizer.

δακτυλικό αποτύπωμα
Μια ψηφιακή εξαγωγή της εικόνας του δακτυλικού σας αποτυπώματος. Η πραγματική εικόνα του δακτυλικού αποτυπώματος δεν αποθηκεύεται ποτέ από το HP Client Security.

δημιουργία αντιγράφων ασφαλείας
Χρήση της λειτουργίας αντιγράφων ασφαλείας για αποθήκευση ενός αντιγράφου σημαντικών πληροφοριών προγράμματος σε μια τοποθεσία έξω από το πρόγραμμα. Στη συνέχεια μπορεί να χρησιμοποιηθεί για την επαναφορά των πληροφοριών σε μεταγενέστερη χρονική στιγμή στον ίδιο υπολογιστή ή σε έναν άλλο.

διαπιστευτήριο
Μια πληροφορία ή μια συσκευή υλικού που χρησιμοποιείται για τον έλεγχο ταυτότητας ενός ανεξάρτητου χρήστη.

διαχειριστής
Δείτε *Διαχειριστής των Windows*.

διαχειριστής των Windows
Ένας χρήστης με πλήρη δικαιώματα για την τροποποίηση δικαιωμάτων και τη διαχείριση άλλων χρηστών.

εκκαθάριση ελεύθερου χώρου
Η εγγραφή τυχαίων δεδομένων πάνω σε διαγραμμένους πόρους και σε αχρησιμοποίητο χώρο. Η διαδικασία αυτή μειώνει την ύπαρξη του διαγραμμένου πόρου έτσι ώστε να είναι ακόμη πιο δύσκολη η επαναφορά του αρχικού πόρου.

έλεγχος ταυτότητας
Η διαδικασία επαλήθευσης ότι είστε το άτομο που ισχυρίζεστε ότι είστε μέσω της χρήσης διαπιστευτηρίων, στα οποία συμπεριλαμβάνονται ο κωδικός πρόσβασης των Windows, το δακτυλικό σας αποτύπωμα, μια έξυπνη κάρτα, μια κάρτα χωρίς επαφή ή μια κάρτα εγγύτητας.

έλεγχος ταυτότητας κατά την εκκίνηση
Μια λειτουργία ασφαλείας, η οποία απαιτεί κάποια μορφή ελέγχου ταυτότητας, όπως μια έξυπνη κάρτα, τσιπ ασφαλείας ή κωδικό πρόσβασης όταν ο υπολογιστής είναι ενεργοποιημένος.

Έλεγχος ταυτότητας πριν την εκκίνηση του Drive Encryption
Μια οθόνη σύνδεσης που εμφανίζεται πριν από την έναρξη των Windows. Οι χρήστες πρέπει να πληκτρολογήσουν το όνομα χρήστη και τον κωδικό πρόσβασης των Windows ή τον κωδικό PIN της έξυπνης κάρτας ή να σαρώσουν ένα καταχωρημένο δάκτυλο. Αν έχει επιλεγεί η σύνδεση σε ένα βήμα, τότε η εισαγωγή

των σωστών πληροφοριών στην οθόνη σύνδεσης του Drive Encryption επιτρέπει την άμεση πρόσβαση στα Windows χωρίς να είναι αναγκαίο να συνδεθείτε ξανά στην οθόνη σύνδεσης των Windows.

ενεργοποίηση
Η εργασία που πρέπει ολοκληρωθεί πριν μπορέσετε να αποκτήσετε πρόσβαση σε οποιαδήποτε από τις λειτουργίες του Drive Encryption. Οι διαχειριστές μπορούν να ενεργοποιήσουν το Drive Encryption με τον οδηγό εγκατάστασης του HP Client Security ή με το HP Client Security. Η διαδικασία ενεργοποίησης αποτελείται από την ενεργοποίηση του λογισμικού, την κρυπτογράφηση του δίσκου και τη δημιουργία του αντιγράφου ασφαλείας του αρχικού κλειδιού κρυπτογράφησης σε μια αφαιρούμενη συσκευή αποθήκευσης.

έξυπνη κάρτα
Μια συσκευή υλικού που μπορεί να χρησιμοποιηθεί με κωδικό PIN για έλεγχο ταυτότητας.

επαναφορά
Μια διαδικασία που αντιγράφει πληροφορίες προγράμματος από ένα ήδη αποθηκευμένο αρχείο αντιγράφου ασφαλείας σε αυτό το πρόγραμμα.

Επαναφορά μέσω του HP SpareKey
Η δυνατότητα πρόσβασης στον υπολογιστή σας απαντώντας σωστά στις ερωτήσεις ασφαλείας.

επανεκκίνηση
Η διαδικασία επανεκκίνησης του υπολογιστή.

κάρτα εγγύτητας
Μια πλαστική κάρτα που περιέχει ένα υπολογιστικό τσιπ που μπορεί να χρησιμοποιηθεί για έλεγχο ταυτότητας σε συνδυασμό με άλλα διαπιστευτήρια για πρόσθετη ασφάλεια.

κάρτα χωρίς επαφή
Μια πλαστική κάρτα που περιέχει ένα υπολογιστικό τσιπ και που μπορεί να χρησιμοποιηθεί για έλεγχο ταυτότητας.

Κάρτα ID
Gadget επιφάνειας εργασίας των Windows που χρησιμεύει για να προσδιορίσετε οπτικά την επιφάνεια εργασίας σας με όνομα χρήστη και επιλεγμένη εικόνα.

κατηγορία συσκευής
Όλες οι συσκευές συγκεκριμένου τύπου, όπως μονάδες δίσκων.

κρυπτογράφηση
Μια διαδικασία, όπως η χρήση ενός αλγόριθμου, που χρησιμοποιείται στην κρυπτογραφία για τη μετατροπή απλού κειμένου σε κείμενο κρυπτογράφησης προκειμένου να αποτραπεί η ανάγνωση δεδομένων από μη εξουσιοδοτημένους παραλήπτες. Υπάρχουν πολλοί τύποι κρυπτογράφησης δεδομένων, και αποτελούν τη βάση της ασφάλειας δικτύου. Οι συνηθισμένοι τύποι περιλαμβάνουν πρότυπο κρυπτογράφησης δεδομένων και κρυπτογράφηση δημόσιου κλειδιού.

κρυπτογράφηση μέσω λογισμικού
Η χρήση λογισμικού για την κρυπτογράφηση του σκληρού δίσκου τομέα προς τομέα. Αυτή η διαδικασία είναι πιο αργή από την κρυπτογράφηση υλικού

κρυπτογράφηση μέσω υλικού
Η χρήση μονάδων αυτοκρυπτογράφησης που συμμορφώνονται με τις προδιαγραφές OPAL του Trusted Computing Group για τη διαχείριση αυτοκρυπτογράφησης μονάδων δίσκων για την ολοκλήρωση στιγμιαίας κρυπτογράφησης. Η κρυπτογράφηση μέσω υλικού είναι στιγμιαία και μπορεί να διαρκέσει μόνο μερικά λεπτά αλλά η κρυπτογράφηση μέσω λογισμικού ενδέχεται να διαρκέσει πολλές ώρες.

λογαριασμός δικτύου
Λογαριασμός χρήστη ή διαχειριστή των Windows είτε σε τοπικό υπολογιστή, με μια ομάδα εργασίας ή σε έναν τομέα.

λογαριασμός χρήστη των Windows

Ένας χρήστης με εξουσιοδότηση για σύνδεση στο δίκτυο ή σε έναν ανεξάρτητο υπολογιστή.

μέθοδος σύνδεσης ασφαλείας
Η μέθοδος που χρησιμοποιείται για τη σύνδεση στον υπολογιστή.

μη αυτόματη μόνιμη διαγραφή
Άμεση καταστροφή ενός πόρου ή επιλεγμένων πόρων, η οποία παρακάμπτει μια προγραμματισμένη καταστροφή.

μόνιμη διαγραφή
Η εκτέλεση ενός αλγορίθμου που αντικαθιστά τα δεδομένα που περιέχονταν σε έναν πόρο με ανούσια δεδομένα.

οθόνη σύνδεσης στο Drive Encryption
Βλ. έλεγχο ταυτότητας πριν την εκκίνηση του Drive Encryption.

ομάδα
Μια ομάδα χρηστών που διαθέτουν το ίδιο επίπεδο δικαιωμάτων πρόσβασης σε μια κατηγορία συσκευών ή σε μια συγκεκριμένη συσκευή.

πολιτική ελέγχου πρόσβασης στη συσκευή
Η λίστα των συσκευών στις οποίες ο χρήστης επιτρέπεται ή απαγορεύεται να αποκτήσει πρόσβαση.

πόρος
Ένα στοιχείο δεδομένων που αποτελείται από προσωπικές πληροφορίες ή αρχεία, ιστορικά δεδομένα και δεδομένα που σχετίζονται με το Web και άλλα, το οποίο βρίσκεται στη μονάδα σκληρού δίσκου.

συνδεδεμένη συσκευή
Μια συσκευή υλικού που είναι συνδεδεμένη σε μια θύρα στον υπολογιστή.

σύνδεση
Ένα αντικείμενο του HP Client Security που αποτελείται από ένα όνομα χρήστη και κωδικό πρόσβασης (και πιθανώς άλλες επιλεγμένες πληροφορίες) που μπορεί να χρησιμοποιηθεί για να συνδεθείτε σε τοποθεσίες web ή άλλα προγράμματα.

σύστημα κρυπτογράφησης αρχείων (EFS)
Ένα σύστημα που κρυπτογραφεί όλα τα αρχεία και τους υποφακέλους εντός του επιλεγμένου φακέλου.

ταυτότητα
Στο HP Client Security, μια ομάδα διαπιστευτηρίων και οι ρυθμίσεις που αντιμετωπίζονται όπως ένας λογαριασμός ή προφίλ για έναν συγκεκριμένο χρήστη.

τομέας
Μια ομάδα υπολογιστών που αποτελούν μέρος ενός δικτύου και χρησιμοποιούν από κοινού έναν κατάλογο βάσης δεδομένων. Κάθε τομέας έχει το δικό του μοναδικό όνομα και διαθέτει ένα σύνολο από κοινούς κανόνες και διαδικασίες.

Τσιπ ασφαλείας ενσωματωμένο στο Trusted Platform Module (TPM)
Το TPM ελέγχει την ταυτότητα του υπολογιστή, αντί του χρήστη, αποθηκεύοντας συγκεκριμένες πληροφορίες σχετικά με το σύστημα του κεντρικού υπολογιστή, όπως τα κλειδιά κρυπτογράφησης, ψηφιακά πιστοποιητικά και κωδικούς πρόσβασης. Το TPM ελαχιστοποιεί τον κίνδυνο παραβίασης των πληροφοριών του υπολογιστή λόγω κλοπής ή επίθεσης από εξωτερικό χάκερ.

Φάκελος του Trust Circle
Ένας φάκελος με προστασία κύκλου εμπιστοσύνης.

χρήστης
Οποιοσδήποτε έχει εγγραφεί στο Drive Encryption. Οι χρήστες που δεν είναι διαχειριστές έχουν περιορισμένα δικαιώματα στο Drive Encryption. Μπορούν μόνο να εγγραφούν (με έγκριση του διαχειριστή) και να συνδεθούν.

Bluetooth

Τεχνολογία που χρησιμοποιεί μετάδοση ραδιοκυμάτων για την ενεργοποίηση υπολογιστών, εκτυπωτών, ποντικιών, κινητών τηλεφώνων και άλλων συσκευών που υποστηρίζουν Bluetooth για ασύρματη επικοινωνία σε μικρή απόσταση.

Drive Encryption
Προστατεύει τα δεδομένα σας κρυπτογραφώντας τους σκληρούς δίσκους σας, καθιστώντας τις πληροφορίες σας μη αναγνώσιμες για εκείνους που δεν έχουν την κατάλληλη εξουσιοδότηση.

DriveLock
Μια δυνατότητα ασφαλείας που συνδέει τη μονάδα σκληρού δίσκου σε ένα χρήστη και απαιτεί από το χρήστη να πληκτρολογήσει σωστά τον κωδικό DriveLock όταν εκκινείται ο υπολογιστής.

Just In Time Authentication
Δείτε τη Βοήθεια του λογισμικού HP Device Access Manager.

PIN
Ένας προσωπικός αριθμός ταυτοποίησης για έναν δηλωμένο χρήστη για χρήση στον έλεγχο ταυτότητας.

PKI
Πρότυπο υποδομής δημόσιου κλειδιού που καθορίζει τις διεπαφές για τη δημιουργία, χρήση και διαχείριση πιστοποιητικών και κλειδιών κρυπτογράφησης.

Single Sign On (Μοναδική σύνδεση)
Μια δυνατότητα που αποθηκεύει πληροφορίες για τον έλεγχο ταυτότητας και σας επιτρέπει να χρησιμοποιείτε το HP Client Security για πρόσβαση στο Internet και τις εφαρμογές των Windows που απαιτούν κωδικό πρόσβασης.

Trust Circle
Παρέχει προστασία των δεδομένων επιτρέποντας την πρόσβαση στα δεδομένα σε μια προκαθορισμένη ομάδα έμπιστων χρηστών. Έτσι προστατεύονται τα δεδομένα από το να πέσουν σε λάθος χέρια είτε τυχαία είτε εκούσια. Με την χρήση της τεχνολογίας ασφαλείας CryptoMill's Zero Overhead Key Management, τα δεδομένα κρυπτογραφούνται γύρω από έναν κύκλο εμπιστοσύνης. Με τον τρόπο αυτό αποφεύγεται η αποκρυπτογράφηση εγγράφων ή άλλων ευαίσθητων πληροφοριών που βρίσκονται εκτός του κύκλου εμπιστοσύνης

Trust Circle Manager/Reader
Το Trust Circle Reader μπορεί να αποδεχτεί προσκλήσεις που αποστέλλονται μόνο από χρήστες του Trust Circle Manager. Ωστόσο, το Trust Circle Manager επιτρέπει τη δημιουργία κύκλων εμπιστοσύνης. Στις λειτουργίες του συμπεριλαμβάνονται η πρόσκληση κάποιου μέσω email σε έναν κύκλο εμπιστοσύνης και η αποδοχή αντίστοιχων προσκλήσεων από άλλους χρήστες. Όταν μεταξύ των χρηστών δημιουργηθεί ένας κύκλος εμπιστοσύνης, είναι δυνατή η ασφαλής κοινή χρήση των αρχείων που προστατεύονται από αυτόν τον κύκλο εμπιστοσύνης.

Windows Logon Security
Προστατεύει τους λογαριασμούς που διαθέτετε στα Windows απαιτώντας τη χρήση συγκεκριμένων διαπιστευτηρίων για την πρόσβαση.

Ευρετήριο