HP ProtectTools
Οδηγός χρήσης

Πρώτη έκδοση: Οκτώβριος 2009

Κωδικός εγγράφου: 572661-151

Πίνακας περιεχομένων

1 Εισαγωγή στην ασφάλεια

Το λογισμικό HP ProtectTools Security Manager παρέχει λειτουργίες ασφαλείας, οι οποίες προστατεύουν την πρόσβαση στον υπολογιστή, σε δίκτυα και σε σημαντικά δεδομένα από μη εξουσιοδοτημένους χρήστες. Η διαχείριση του HP ProtectTools Security Manager γίνεται μέσω της λειτουργίας Administrative Console.

Χρησιμοποιώντας την κονσόλα, ο τοπικός διαχειριστής μπορεί να πραγματοποιήσει τις εξής εργασίες:

- Ενεργοποίηση ή απενεργοποίηση λειτουργιών ασφαλείας
- Εγγραφή δακτυλικών αποτυπωμάτων για χρήστες αυτού του υπολογιστή
- Εγκατάσταση έξυπνης κάρτας
- Προσδιορισμός των απαιτούμενων διαπιστευτηρίων για έλεγχο ταυτότητας
- Διαχείριση των χρηστών του υπολογιστή
- Προσαρμογή παραμέτρων που αφορούν συγκεκριμένες συσκευές
- Διαμόρφωση εγκατεστημένων εφαρμογών του Security Manager
- Προσθήκη επιπλέον εφαρμογών του Security Manager

Τα στοιχεία λογισμικού που είναι διαθέσιμα για το δικό σας υπολογιστή ενδέχεται να διαφέρουν ανάλογα με το μοντέλο.

Τα στοιχεία λογισμικού του HP ProtectTools μπορεί να είναι προεγκατεστημένα, προφορτωμένα ή διαθέσιμα για λήψη από την τοποθεσία της HP στο web. Για περισσότερες πληροφορίες, επισκεφτείτε τη διεύθυνση http://www.hp.com.

ΣΗΜΕΙΩΣΗ Οι οδηγίες στον παρόντα οδηγό χρήσης έχουν συνταχτεί με την προϋπόθεση ότι έχετε ήδη εγκαταστήσει τα ισχύοντα στοιχεία λογισμικού του HP ProtectTools.

Δυνατότητες του HP ProtectTools

Ο παρακάτω πίνακας περιγράφει λεπτομερώς τις βασικές λειτουργίες των ενοτήτων του HP ProtectTools.

Στοιχείο	Βασικές δυνατότητες
Credential Manager for HP ProtectTools	• Το Password Manager λειτουργεί ως προσωπικός χώρος φύλαξης των κωδικών πρόσβασης, διευκολύνοντας τη διαδικασία σύνδεσης με τη λειτουργία Single Sign On, η οποία απομνημονεύει αυτόματα και χρησιμοποιεί τα διαπιστευτήρια του χρήστη. • Η λειτουργία Single Sign On προσφέρει πρόσθετη προστασία απαιτώντας συνδυασμούς διαφορετικών τεχνολογιών ασφάλειας, όπως κάρτα Java™ και βιομετρική τεχνολογία, για τον έλεγχο της ταυτότητας χρήστη. • Ο χώρος αποθήκευσης των κωδικών πρόσβασης προστατεύεται με κρυπτογράφηση λογισμικού και μπορεί να ενισχυθεί με τη χρήση ελέγχου ταυτότητας συσκευής ασφαλείας, όπως οι κάρτες Java ή οι συσκευές βιομετρικής ανάγνωσης. **ΣΗΜΕΙΩΣΗ** Η λειτουργικότητα του Credential Manager έγκειται στην επιλογή του Password Manager του HP ProtectTools Security Manager
Drive Encryption for HP ProtectTools (μόνο σε επιλεγμένα μοντέλα)	• Το Drive Encryption παρέχει πλήρη κρυπτογράφηση όλων των τόμων του σκληρού δίσκου. • Το Drive Encryption απαιτεί έλεγχο ταυτότητας κατά την προεκκίνηση για την αποκρυπτογράφηση και την πρόσβαση στα δεδομένα.
Privacy Manager for HP ProtectTools (μόνο σε επιλεγμένα μοντέλα)	• Το Privacy Manager χρησιμοποιεί εξελιγμένες τεχνικές σύνδεσης για επαλήθευση της προέλευσης, της ακεραιότητας και της ασφάλειας της επικοινωνίας όταν χρησιμοποιούνται e-mail, έγγραφα του Microsoft® Office ή άμεσα μηνύματα.
File Sanitizer for HP ProtectTools	• Το File Sanitizer σάς δίνει τη δυνατότητα να διαγράφετε μόνιμα και με ασφάλεια ψηφιακούς πόρους (ευαίσθητες πληροφορίες που περιλαμβάνουν αρχεία εφαρμογών, περιεχόμενο ιστορικού ή web ή άλλα εμπιστευτικά δεδομένα) από τον υπολογιστή σας και να εκκαθαρίζετε περιοδικά το σκληρό σας δίσκο.
Device Access Manager for HP ProtectTools (μόνο σε επιλεγμένα μοντέλα)	• Το Device Access Manager επιτρέπει στους διαχειριστές IT να ελέγχουν την πρόσβαση σε συσκευές με βάση τα προφίλ χρήστη. • Το Device Access Manager δεν επιτρέπει σε μη εξουσιοδοτημένους χρήστες να αφαιρούν δεδομένα με τη χρήση εξωτερικών αποθηκευτικών μέσων ή να εισάγουν ιούς στο σύστημα από εξωτερικά μέσα. • Ο διαχειριστής μπορεί να απενεργοποιήσει την πρόσβαση σε συσκευές εγγραφής για συγκεκριμένα άτομα ή ομάδες χρηστών.

Επίτευξη βασικών στόχων ασφάλειας

Τα στοιχεία του HP ProtectTools μπορούν να συνεργαστούν για να παρέχουν λύσεις σε διάφορα προβλήματα ασφάλειας, μεταξύ των οποίων:

- Προστασία από προσχεδιασμένη κλοπή
- Περιορισμός πρόσβασης σε ευαίσθητα δεδομένα
- Αποτροπή πρόσβασης μη εξουσιοδοτημένων χρηστών από εσωτερικές ή εξωτερικές τοποθεσίες
- Δημιουργία ισχυρών πολιτικών κωδικών πρόσβασης
- Διευθέτηση ρυθμιστικών εντολών ασφάλειας

Προστασία από στοχευμένη κλοπή

Ένα παράδειγμα στοχευμένης κλοπής είναι η κλοπή ενός υπολογιστή που περιέχει εμπιστευτικά δεδομένα και στοιχεία πελατών στο σημείο ελέγχου ασφαλείας ενός αεροδρομίου. Οι παρακάτω λειτουργίες συμβάλλουν στην προστασία από στοχευμένη κλοπή:

- Η λειτουργία ελέγχου ταυτότητας πριν από την εκκίνηση, εφόσον έχει ενεργοποιηθεί, βοηθά ώστε να αποτρέπεται η πρόσβαση στο λειτουργικό σύστημα. Ανατρέξτε στις ακόλουθες διαδικασίες:
  - Security Manager
  - Drive Encryption

Περιορισμός της πρόσβασης σε ευαίσθητα δεδομένα

Ας υποθέσουμε ότι ένας ελεγκτής εργάζεται στις εγκαταστάσεις σας και του έχει δοθεί πρόσβαση στον υπολογιστή προκειμένου να ελέγξει ευαίσθητα οικονομικά δεδομένα. Ωστόσο, δεν θέλετε να έχει τη δυνατότητα να εκτυπώσει τα αρχεία ή να τα αποθηκεύσει σε συσκευή με δυνατότητα εγγραφής, όπως ένα CD. Η παρακάτω λειτουργία συμβάλλει στον περιορισμό της πρόσβασης σε δεδομένα:

- Το Device Access Manager for HP ProtectTools δίνει στους διαχειριστές IT τη δυνατότητα να περιορίζουν την πρόσβαση σε συσκευές με δυνατότητα εγγραφής, έτσι ώστε να μην είναι εφικτή η εκτύπωση ή η αντιγραφή ευαίσθητων πληροφοριών από το σκληρό δίσκο σε αφαιρούμενα μέσα.

Αποτροπή πρόσβασης μη εξουσιοδοτημένων χρηστών από εσωτερικές ή εξωτερικές τοποθεσίες

Η μη εξουσιοδοτημένη πρόσβαση σε υπολογιστή επιχείρησης χωρίς ασφάλεια, αποτελεί πολύ αισθητό κίνδυνο για τους εταιρικούς πόρους δικτύου, όπως πληροφορίες οικονομικών υπηρεσιών, στελέχη ή ομάδες έρευνας & ανάπτυξης, καθώς και για ατομικές πληροφορίες, όπως αρχεία ασθενών ή

προσωπικά αρχεία οικονομικών στοιχείων. Οι παρακάτω λειτουργίες βοηθούν στην αποτροπή μη εξουσιοδοτημένης πρόσβασης:

- Η λειτουργία ελέγχου ταυτότητας πριν από την εκκίνηση, εφόσον έχει ενεργοποιηθεί, βοηθά ώστε να αποτρέπεται η πρόσβαση στο λειτουργικό σύστημα. Ανατρέξτε στις ακόλουθες διαδικασίες:
  - Password Manager
  - Drive Encryption
- Με το Password Manager διασφαλίζεται ότι ένας μη εξουσιοδοτημένος χρήστης δεν μπορεί να αποκτήσει κωδικούς πρόσβασης ή πρόσβαση σε εφαρμογές που προστατεύονται με κωδικούς πρόσβασης.
- Το Device Access Manager for HP ProtectTools δίνει στους διαχειριστές IT τη δυνατότητα να περιορίζουν την πρόσβαση σε συσκευές με δυνατότητα εγγραφής, έτσι ώστε να μην είναι εφικτή η αντιγραφή ευαίσθητων πληροφοριών από το σκληρό δίσκο.
- Το DriveLock διασφαλίζει ότι η πρόσβαση στα δεδομένα δεν θα είναι εφικτή ακόμα και εάν αφαιρεθεί ο σκληρός δίσκος και τοποθετηθεί σε σύστημα που δεν προστατεύεται.

Δημιουργία πολιτικών ισχυρών κωδικών πρόσβασης

Εάν τεθεί σε ισχύ μια οδηγία που απαιτεί τη χρήση πολιτικής ισχυρών κωδικών πρόσβασης για δεκάδες εφαρμογές και βάσεις δεδομένων στο web, το Security Manager παρέχει ένα προστατευμένο χώρο αποθήκευσης για κωδικούς πρόσβασης και εύκολη σύνδεση μέσω της λειτουργίας Single Sign On.

Συμπληρωματικά στοιχεία ασφάλειας

Ορισμός ρόλων ασφαλείας

Στη διαχείριση της ασφάλειας του υπολογιστή (ειδικά όταν πρόκειται για μεγάλους οργανισμούς), ο διαμοιρασμός των ευθυνών και των δικαιωμάτων ανάμεσα σε διαφορετικούς τύπους διαχειριστών και χρηστών αποτελεί ουσιώδη πρακτική.

ΣΗΜΕΙΩΣΗ Όταν πρόκειται για μικρό οργανισμό ή για προσωπική χρήση, αυτοί οι ρόλοι ενδέχεται να ανήκουν στο ίδιο άτομο.

Για το HP ProtectTools, τα καθήκοντα και τα προνόμια ασφαλείας μπορούν να διανεμηθούν στους ακόλουθους ρόλους:

- Security officer (Υπεύθυνος ασφαλείας)—Ορίζει το επίπεδο ασφάλειας για την εταιρεία ή το δίκτυο και καθορίζει ποιες λειτουργίες ασφαλείας θα αναπτύξει, όπως για παράδειγμα κάρτες Java™, βιομετρικές συσκευές ανάγνωσης ή διακριτικό USB.

  ΣΗΜΕΙΩΣΗ Πολλές από τις λειτουργίες του HP ProtectTools είναι δυνατό να προσαρμοστούν από τον υπεύθυνο ασφαλείας σε συνεργασία με την HP. Για περισσότερες πληροφορίες, επισκεφτείτε την τοποθεσία web της HP στη διεύθυνση http://www.hp.com.

- IT administrator (Διαχειριστής IT) — Εφαρμόζει και διαχειρίζεται τα χαρακτηριστικά ασφαλείας που έχουν οριστεί από τον υπεύθυνο ασφαλείας. Μπορεί επίσης να ενεργοποιήσει και να απενεργοποιήσει ορισμένα χαρακτηριστικά. Εάν, για παράδειγμα, ο υπεύθυνος ασφαλείας έχει αποφασίσει να χρησιμοποιήσει κάρτες Java, ο διαχειριστής IT μπορεί να ενεργοποιήσει τη λειτουργία ασφαλείας του BIOS της κάρτας Java.

- User (Χρήστης) — Χρησιμοποιεί τα χαρακτηριστικά ασφαλείας. Εάν, για παράδειγμα, ο υπεύθυνος ασφαλείας και ο διαχειριστής IT έχουν ενεργοποιήσει κάρτες Java για το σύστημα, ο χρήστης μπορεί να ορίσει το PIN της κάρτας Java και να χρησιμοποιήσει την κάρτα για έλεγχο ταυτότητας.

△ **ΠΡΟΣΟΧΗ** Οι διαχειριστές συνιστάται να ακολουθούν τις "βέλτιστες πρακτικές" σε ό,τι αφορά τον περιορισμό των προνομίων των τελικών χρηστών και της πρόσβασης των χρηστών.

Οι χρήστες που δεν είναι εξουσιοδοτημένοι δεν πρέπει να έχουν διαχειριστικά προνόμια.

Διαχείριση κωδικών πρόσβασης για HP ProtectTools

Τα περισσότερα χαρακτηριστικά του HP ProtectTools Security Manager είναι ασφαλισμένα με κωδικούς ασφαλείας. Ο παρακάτω πίνακας παραθέτει τους συχνότερα χρησιμοποιημένους κωδικούς, τα στοιχεία του λογισμικού στα οποία έχει οριστεί κωδικός και τη λειτουργία του κάθε κωδικού.

Οι κωδικοί πρόσβασης που έχουν οριστεί και χρησιμοποιούνται μόνο από τους διαχειριστές IT περιλαμβάνονται σε αυτό τον πίνακα επίσης. Όλοι οι υπόλοιποι κωδικοί ενδέχεται να έχουν οριστεί από χρήστες ή διαχειριστές.

Κωδικός πρόσβασης HP ProtectTools	Ορισμένος στο παρόν στοιχείο του HP ProtectTools	Λειτουργία
Κωδικός σύνδεσης στο Security Manager	Security Manager	Αυτός ο κωδικός σύνδεσης προσφέρει 2 επιλογές: • Μπορεί να χρησιμοποιηθεί ως σύνδεση στο Security Manager για πρόσβαση στο Security Manager μετά τη σύνδεση στα Windows. • Μπορεί να χρησιμοποιηθεί για να επιτρέπεται η πρόσβαση ταυτόχρονα στα Windows και στο Security Manager.
Κωδικός ανάκτησης αρχείων για το Security Manager	Security Manager, από το διαχειριστή IT	Προστατεύει την πρόσβαση στο αρχείο ανάκτησης του Security Manager.
PIN κάρτας Java™	Java Card Security	Εμποδίζει την πρόσβαση στο περιεχόμενο της κάρτας Java και πραγματοποιεί έλεγχο ταυτότητας των χρηστών της κάρτας Java. Όταν χρησιμοποιείται για έλεγχο ταυτότητας κατά την εκκίνηση, το PIN της κάρτας Java εμποδίζει επίσης την πρόσβαση στο βοηθητικό πρόγραμμα Computer Setup και στα περιεχόμενα του υπολογιστή. Πραγματοποιεί έλεγχο ταυτότητας των χρηστών του Drive Encryption, εάν είναι επιλεγμένο το διακριτικό της κάρτας Java.
Κωδικός σύνδεσης στα Windows	Πίνακας Ελέγχου των Windows®	Μπορεί να χρησιμοποιηθεί για μη αυτόματη σύνδεση ή να αποθηκευτεί σε κάρτα Java.

Δημιουργία ασφαλούς κωδικού πρόσβασης

Πριν δημιουργήσετε κωδικούς πρόσβασης, πρέπει πρώτα να ακολουθήσετε όλες τις διευκρινίσεις που δίνονται από το πρόγραμμα. Γενικότερα, ωστόσο, έχετε πάντα υπόψη σας τις ακόλουθες οδηγίες που θα σας βοηθήσουν να δημιουργήσετε ασφαλείς κωδικούς πρόσβασης και να μειώσετε τις πιθανότητες προσβολής τους:

- Χρησιμοποιήστε κωδικούς με περισσότερους από 6 χαρακτήρες και κατά προτίμηση περισσότερους από 8 χαρακτήρες.
- Συνδυάστε πεζά και κεφαλαία στη σύνθεση του κωδικού σας.
- Όποτε είναι δυνατόν, συνδυάστε αλφαριθμητικούς χαρακτήρες και περιλάβετε ειδικούς χαρακτήρες και σημεία στίξης.
- Σε μια λέξη-κλειδί αντικαταστήστε τα γράμματα με ειδικούς χαρακτήρες ή αριθμούς. Μπορείτε, για παράδειγμα, να χρησιμοποιήσετε τον αριθμό 1 αντί για τα γράμματα I ή L.
- Συνδυάστε λέξεις από 2 ή περισσότερες γλώσσες.
- Τοποθετήστε ειδικούς χαρακτήρες ή αριθμούς στο μέσο μιας λέξης ή φράσης, για παράδειγμα, "Μαρία2-Γατα45".
- Αποφεύγετε να χρησιμοποιείτε ως κωδικούς πρόσβασης λέξεις που περιλαμβάνονται σε λεξικά.
- Αποφεύγετε να χρησιμοποιείτε το όνομά σας ή οποιαδήποτε άλλη προσωπική πληροφορία, όπως την ημερομηνία γέννησής σας, το όνομα του κατοικίδιού σας ή το πατρικό όνομα της μητέρας σας, ακόμα και εάν τα γράψετε ανάποδα.
- Αλλάζετε τακτικά κωδικούς πρόσβασης. Μπορείτε να αλλάξετε μόνο λίγους χαρακτήρες που να αυξάνονται.
- Εάν καταγράψετε κάπου τον κωδικό πρόσβασης, μην τον φυλάξετε σε σημείο που είναι εύκολα ορατό και κοντά στον υπολογιστή.
- Αποφεύγετε να φυλάτε τον κωδικό πρόσβασης σε κάποιο αρχείο, όπως e-mail, στον υπολογιστή.
- Αποφεύγετε να μοιράζεστε λογαριασμούς με άλλους και να αποκαλύπτετε τον κωδικό πρόσβασης σας.

Δημιουργία αντιγράφων ασφαλείας και επαναφορά των διαπιστευτηρίων του HP ProtectTools

Μπορείτε να χρησιμοποιήσετε τη λειτουργία Drive Encryption for HP ProtectTools προκειμένου να επιλέξετε διαπιστευτήρια του HP ProtectTools και να δημιουργήσετε αντίγραφα ασφαλείας αυτών.

2 Έναρξη χρήσης

ΣΗΜΕΙΩΣΗ Η διαχείριση του HP ProtectTools απαιτεί προνόμια διαχειριστή.

Ο οδηγός εγκατάστασης του HP ProtectTools σάς καθοδηγεί στην εγκατάσταση των λειτουργιών του Security Manager που χρησιμοποιούνται πιο συχνά. Ωστόσο, υπάρχει πληθώρα επιπρόσθετων λειτουργιών που μπορείτε να χρησιμοποιήσετε από το HP ProtectTools Administrative Console. Οι ίδιες ρυθμίσεις που υπάρχουν στον οδηγό, καθώς και επιπλέον λειτουργίες ασφαλείας, μπορούν να διαμορφωθούν και από την κονσόλα, στην οποία μπορείτε να αποκτήσετε πρόσβαση από το μενού "Έναρξη" των Windows®. Οι ρυθμίσεις αυτές ισχύουν για τον υπολογιστή και όλους τους χρήστες που τον χρησιμοποιούν από κοινού.

1. Στη σελίδα υποδοχής, μπορείτε να απενεργοποιήσετε την περαιτέρω εμφάνιση του οδηγού ενεργοποιώντας μία από τις επιλογές.

2. Μία εβδομάδα μετά την εγκατάσταση του υπολογιστή ή όταν ένας χρήστης με δικαιώματα διαχειριστή χρησιμοποιήσει για πρώτη φορά τη συσκευή ανάγνωσης αποτυπωμάτων, ο οδηγός εγκατάστασης του HP ProtectTools θα εκκινηθεί αυτόματα προκειμένου να σας καθοδηγήσει στα βασικά βήματα διαμόρφωσης του προγράμματος. Ξεκινά αυτόματα ένα βίντεο εκμάθησης σχετικά με την εγκατάσταση του υπολογιστή.

3. Ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη έως ότου ολοκληρωθεί η εγκατάσταση.

Εάν δεν ολοκληρώσετε τον οδηγό, θα εκκινηθεί αυτόματα άλλες δύο φορές. Μετά από αυτό, μπορείτε να αποκτήσετε πρόσβαση στον οδηγό από το μπαλόνι ειδοποίησης που εμφανίζεται κοντά στην περιοχή ειδοποιήσεων της γραμμής εργασιών (εκτός εάν το έχετε απενεργοποιήσει, όπως περιγράφεται στο βήμα 2 παραπάνω) μέχρι να ολοκληρώσετε τον οδηγό εγκατάστασης.

Για να χρησιμοποιήσετε τις εφαρμογές του HP ProtectTools Security Manager, εκκινήστε το HP ProtectTools Security Manager από το μενού "Έναρξη" ή κάντε διπλό κλικ στο εικονίδιο του Security Manager στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών. Το HP ProtectTools Administrative Console και οι εφαρμογές του είναι διαθέσιμες σε όλους τους χρήστες που χρησιμοποιούν αυτό τον υπολογιστή.

Άνοιγμα του HP ProtectTools Administrative Console

Για διαχειριστικές εργασίες, όπως ορισμό πολιτικών συστήματος ή διαμόρφωση λογισμικού, ανοίξτε την κονσόλα ως εξής:

- Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Administrative Console**.

  – ή –

  Στο αριστερό τμήμα παραθύρου του Security Manager, επιλέξτε **Administration** (Διαχείριση).

Για εργασίες χρήστη, όπως καταχώριση δακτυλικών αποτυπωμάτων ή χρήση του Security Manager, ανοίξτε την κονσόλα ως εξής:

- Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Security Manager**.

  – ή –

  Κάντε διπλό κλικ στο εικονίδιο **HP ProtectTools Security Manager** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών.

Ενεργοποίηση λειτουργιών ασφαλείας

Ο οδηγός εγκατάστασης θα σας ζητήσει να επαληθεύσετε την ταυτότητά σας.

1. Διαβάστε την οθόνη υποδοχής και κάντε κλικ στο κουμπί **Next** (Επόμενο).
2. Επαληθεύστε την ταυτότητά σας πληκτρολογώντας τον κωδικό πρόσβασης των Windows, εάν δεν έχετε καταχωρίσει δακτυλικά αποτυπώματα ακόμα ή σαρώνοντας το δακτυλικό σας αποτύπωμα με τη συσκευή ανάγνωσης αποτυπωμάτων. Κάντε κλικ στο κουμπί **Next** (Επόμενο).

   Εάν ο κωδικός σας πρόσβασης στα Windows είναι κενός, θα σας ζητηθεί να δημιουργήσετε ένα κωδικό. Ο κωδικός πρόσβασης των Windows είναι απαραίτητος για την προστασία του λογαριασμού σας στα Windows έναντι πρόσβασης από μη εξουσιοδοτημένα άτομα και για τη χρήση των λειτουργιών του HP ProtectTools Security Manager.

Ο οδηγός εγκατάστασης θα σας καθοδηγήσει στη διαδικασία ενεργοποίησης των λειτουργιών ασφαλείας που ισχύουν για όλους τους χρήστες του υπολογιστή:

- Η ασφάλεια σύνδεσης των Windows προστατεύει τους λογαριασμούς σας στα Windows απαιτώντας τη χρήση συγκεκριμένων διαπιστευτηρίων για την παροχή πρόσβασης.
- Το Drive Encryption προστατεύει τα δεδομένα σας κρυπτογραφώντας τους σκληρούς δίσκους και καθιστώντας αδύνατη την ανάγνωση των πληροφοριών από άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση.
- Το Pre-Boot Security προστατεύει τον υπολογιστή σας απαγορεύοντας την πρόσβαση μη εξουσιοδοτημένων ατόμων πριν από την εκκίνηση των Windows.

Για να ενεργοποιήσετε μια λειτουργία ασφαλείας, επιλέξτε το αντίστοιχο πλαίσιο ελέγχου. Όσες περισσότερες λειτουργίες επιλέξετε, τόσο πιο ασφαλής θα είναι ο υπολογιστής σας.

ΣΗΜΕΙΩΣΗ Το Pre-Boot Security δεν θα είναι διαθέσιμο εάν δεν το υποστηρίζει το BIOS που διαθέτετε.

Καταχώριση αποτυπωμάτων

Εάν έχετε επιλέξει Fingerprint (Αποτύπωμα) και εφόσον ο υπολογιστής σας διαθέτει ενσωματωμένη ή συνδεδεμένη συσκευή ανάγνωσης αποτυπωμάτων, θα καθοδηγηθείτε στη διαδικασία ρύθμισης ή καταχώρισης των αποτυπωμάτων σας:

1. Εμφανίζεται το περίγραμμα δύο χεριών. Τα δάχτυλα που έχουν ήδη καταχωριστεί επισημαίνονται με πράσινο χρώμα. Κάντε κλικ σε ένα δάχτυλο πάνω στο περίγραμμα.

   ΣΗΜΕΙΩΣΗ Για να διαγράψετε ένα ήδη καταχωρισμένο αποτύπωμα, κάντε κλικ στο αντίστοιχο δάχτυλο.

2. Όταν επιλέξετε δάχτυλο για καταχώριση, θα σας ζητηθεί να σαρώσετε αυτό το αποτύπωμα έως ότου ολοκληρωθεί η διαδικασία καταχώρισης επιτυχώς. Τα καταχωρισμένα δάχτυλα επισημαίνονται με πράσινο χρώμα στο περίγραμμα.

3. Πρέπει να καταχωρίσετε τουλάχιστον δύο δάχτυλα, κατά προτίμηση το δείκτη ή το μέσο. Επαναλάβετε τα βήματα 1 έως 3 για άλλο δάχτυλο.

4. Κάντε κλικ στο κουμπί **Next** (Επόμενο).

ΣΗΜΕΙΩΣΗ Κατά την καταχώριση αποτυπωμάτων μέσω της διαδικασίας έναρξης χρήσης, οι πληροφορίες των αποτυπωμάτων δεν αποθηκεύονται έως ότου κάνετε κλικ στο κουμπί **Next** (Επόμενο). Εάν αφήσετε τον υπολογιστή ανενεργό για κάποιο διάστημα ή κλείσετε τον πίνακα εργαλείων, οι αλλαγές που έχετε κάνει **δεν** αποθηκεύονται.

Εγκατάσταση έξυπνης κάρτας

Εάν έχετε επιλέξει Smart card (Έξυπνη κάρτα) και εφόσον ο υπολογιστής διαθέτει ενσωματωμένη ή συνδεδεμένη συσκευή ανάγνωσης έξυπνων καρτών, ο οδηγός εγκατάστασης του HP ProtectTools θα σας ζητήσει να ορίσετε ένα PIN έξυπνης κάρτας.

Για να ορίσετε PIN έξυπνης κάρτας:

1. Πληκτρολογήστε και επιβεβαιώστε ένα κωδικό PIN στη σελίδα Set up smart card (Εγκατάσταση έξυπνης κάρτας).

   Μπορείτε επίσης να αλλάξετε το PIN σας. Πληκτρολογήστε το παλιό σας PIN και έπειτα επιλέξτε ένα καινούργιο.

2. Για να συνεχίσετε, κάντε κλικ στο κουμπί **Next** (Επόμενο).

Χρήση του Administrative Console

Το HP ProtectTools Administrative Console είναι η κεντρική τοποθεσία διαχείρισης των λειτουργιών και των εφαρμογών του HP ProtectTools Security Manager.

Η κονσόλα αποτελείται από τα εξής στοιχεία:

- **Tools** (Εργαλεία) — Εμφανίζει τις παρακάτω κατηγορίες για τη διαμόρφωση της ασφάλειας του υπολογιστή:
  - **Home** (Σπίτι) — Σας επιτρέπει να επιλέξετε τις εργασίες ασφαλείας που θα πραγματοποιηθούν.
  - **System** (Σύστημα) — Σας επιτρέπει να διαμορφώσετε τις λειτουργίες ασφαλείας και τον έλεγχο ταυτότητας για χρήστες και συσκευές.
  - **Applications** (Εφαρμογές) — Εμφανίζει γενικές ρυθμίσεις για το HP ProtectTools Security Manager και για εφαρμογές του Security Manager.
  - **Data** (Δεδομένα) — Παρέχει ένα επεκτεινόμενο μενού συνδέσεων με εφαρμογές του Security Manager που προστατεύουν τα δεδομένα σας.
- **Management Tools** (Εργαλεία διαχείρισης) — Προσφέρει πληροφορίες για επιπρόσθετα εργαλεία. Ο παρακάτω πίνακας παρουσιάζει τις εξής επιλογές:
  - **HP ProtectTools Setup Wizard** (Οδηγός εγκατάστασης του HP ProtectTools) — Σας καθοδηγεί στην εγκατάσταση του HP ProtectTools Security Manager.
  - **Help** (Βοήθεια) — Εμφανίζει το αρχείο βοήθειας που παρέχει πληροφορίες για το Security Manager και τις προεγκατεστημένες εφαρμογές του. Η βοήθεια για εφαρμογές που μπορεί να προσθέσετε παρέχεται μέσα σε αυτές τις εφαρμογές.
  - **About** (Πληροφορίες) — Εμφανίζει πληροφορίες για το HP ProtectTools Security Manager, όπως τον αριθμό έκδοσης και τη σημείωση πνευματικών δικαιωμάτων.
- **Main area** (Βασική περιοχή) — Εμφανίζει οθόνες συγκεκριμένων εφαρμογών.

Για να ανοίξετε το HP ProtectTools Administrative Console, κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Administrative Console**.

3 Διαμόρφωση συστήματος

Η πρόσβαση στην ομάδα System (Σύστημα) γίνεται από το παράθυρο του μενού Tools (Εργαλεία) στην αριστερή πλευρά της οθόνης του HP ProtectTools Administrative Console. Μπορείτε να χρησιμοποιήσετε τις εφαρμογές σε αυτή την ομάδα για να διαχειριστείτε τις πολιτικές και τις ρυθμίσεις για τον υπολογιστή, τους χρήστες του και τις συνδεδεμένες συσκευές.

Η ομάδα System (Σύστημα) περιλαμβάνει τις παρακάτω εφαρμογές:

- **Security** (Ασφάλεια) — Διαχείριση λειτουργιών, ελέγχου ταυτότητας και ρυθμίσεων που αφορούν τον τρόπο αλληλεπίδρασης των χρηστών με τον υπολογιστή.
- **Users** (Χρήστες) — Ορισμός, διαχείριση και καταχώριση των χρηστών του υπολογιστή.
- **Devices** (Συσκευές) — Διαχείριση ρυθμίσεων για συσκευές ασφαλείας που είναι ενσωματωμένες ή συνδεδεμένες με τον υπολογιστή.

Ρύθμιση ελέγχου ταυτότητας για τον υπολογιστή

Στην εφαρμογή Authentication (Έλεγχος ταυτότητας), μπορείτε να επιλέξετε τις λειτουργίες ασφαλείας που θα εφαρμόζονται στον υπολογιστή, να ορίσετε πολιτικές για την πρόσβαση στον υπολογιστή και να διαμορφώσετε επιπλέον ρυθμίσεις για προχωρημένους. Μπορείτε να καθορίσετε τα διαπιστευτήρια που θα απαιτούνται για τον έλεγχο ταυτότητας κάθε κατηγορίας χρηστών κατά τη σύνδεση στα Windows ή σε τοποθεσίες web και προγράμματα κατά τη διάρκεια της περιόδου λειτουργίας του κάθε χρήστη.

Για να ρυθμίσετε τον έλεγχο ταυτότητας στον υπολογιστή σας:

1. Στο μενού Security (Ασφάλεια), επιλέξτε **Authentication** (Έλεγχος ταυτότητας).
2. Για να διαμορφώσετε τον έλεγχο ταυτότητας κατά τη σύνδεση, κάντε κλικ στην καρτέλα **Logon Policy** (Πολιτική σύνδεσης), κάντε τις αλλαγές που θέλετε και κάντε κλικ στο κουμπί **Apply** (Εφαρμογή).
3. Για να διαμορφώσετε τον έλεγχο ταυτότητας κατά την περίοδο λειτουργίας, κάντε κλικ στην καρτέλα **Session Policy** (Πολιτική περιόδου λειτουργίας), κάντε τις αλλαγές που θέλετε και κάντε κλικ στο κουμπί **Apply** (Εφαρμογή).

Πολιτική σύνδεσης

Για να καθορίσετε τις πολιτικές που θα ισχύουν για τα διαπιστευτήρια που απαιτούνται για τον έλεγχο ταυτότητας ενός χρήστη κατά τη σύνδεση στα Windows:

1. Στο μενού Tools (Εργαλεία), επιλέξτε **Security** (Ασφάλεια) και έπειτα **Authentication** (Έλεγχος ταυτότητας).
2. Στην καρτέλα **Logon Policy** (Πολιτική σύνδεσης), κάντε κλικ σε μια κατηγορία χρηστών.
3. Προσδιορίστε τα διαπιστευτήρια ελέγχου ταυτότητας που απαιτούνται για την επιλεγμένη κατηγορία χρηστών. Πρέπει να προσδιορίσετε τουλάχιστον ένα διαπιστευτήριο.
4. Επιλέξτε ANY (ΟΠΟΙΟΔΗΠΟΤΕ) (μόνο ένα) ή ALL (ΟΛΑ) για να ορίσετε πόσα από τα προσδιορισμένα διαπιστευτήρια θα είναι απαραίτητα για τον έλεγχο ταυτότητας ενός χρήστη. Επίσης, μπορείτε να αποτρέψετε την πρόσβαση στον υπολογιστή για κάθε χρήστη.
5. Κάντε κλικ στο κουμπί **Apply** (Εφαρμογή).

Πολιτική περιόδου λειτουργίας

Για να καθορίσετε τις πολιτικές που θα διέπουν τα απαιτούμενα διαπιστευτήρια για πρόσβαση στις εφαρμογές του HP ProtectTools κατά τη διάρκεια μιας περιόδου λειτουργίας στα Windows:

1. Στο μενού Tools (Εργαλεία), επιλέξτε **Security** (Ασφάλεια) και έπειτα **Authentication** (Έλεγχος ταυτότητας).
2. Στην καρτέλα **Session Policy** (Πολιτική περιόδου λειτουργίας), κάντε κλικ σε μια κατηγορία χρηστών.
3. Προσδιορίστε τα διαπιστευτήρια ελέγχου ταυτότητας που απαιτούνται για την επιλεγμένη κατηγορία χρηστών.
4. Επιλέξτε ANY (ΟΠΟΙΟΔΗΠΟΤΕ) (μόνο ένα) ή ALL (ΟΛΑ) για να ορίσετε πόσα από τα προσδιορισμένα διαπιστευτήρια θα είναι απαραίτητα για τον έλεγχο ταυτότητας ενός χρήστη.

Μπορείτε επίσης να ορίσετε ότι δεν θα απαιτείται έλεγχος ταυτότητας για πρόσβαση στο λογισμικό HP ProtectTools.

5. Κάντε κλικ στο κουμπί **Apply** (Εφαρμογή).

Ρυθμίσεις

Μπορείτε να επιτρέψετε μία ή περισσότερες από τις παρακάτω ρυθμίσεις ασφαλείας:

- **Allow One Step logon** (Να επιτρέπεται σύνδεση σε ένα βήμα) — Επιτρέπει στους χρήστες του υπολογιστή να παρακάμψουν τη σύνδεση στα Windows εάν έχει προηγηθεί έλεγχος ταυτότητας στο BIOS ή σε επίπεδο κρυπτογραφημένου δίσκου.
- **Allow HP SpareKey authentication for Windows logon** (Να επιτρέπεται έλεγχος ταυτότητας HP SpareKey για σύνδεση στα Windows) — Επιτρέπει στους χρήστες του υπολογιστή να χρησιμοποιούν τη λειτουργία HP SpareKey για να συνδεθούν στα Windows παρά την ύπαρξη άλλης πολιτικής ελέγχου ταυτότητας που απαιτείται από το Security Manager.

Για να επεξεργαστείτε τις ρυθμίσεις:

1. Κάντε κλικ για να ενεργοποιήσετε ή να απενεργοποιήσετε μια συγκεκριμένη ρύθμιση.
2. Κάντε κλικ στο κουμπί **Apply** (Εφαρμογή) για να αποθηκεύσετε τις αλλαγές που έχετε κάνει.

Διαχείριση χρηστών

Από την εφαρμογή Users (Χρήστες), μπορείτε να παρακολουθείτε και να διαχειρίζεστε τους χρήστες του HP ProtectTools αυτού του υπολογιστή.

Αναγράφονται όλοι οι χρήστες του HP ProtectTools, οι οποίοι επαληθεύονται με βάση τις πολιτικές που έχουν οριστεί μέσω του Security Manager, καθώς επίσης επαληθεύεται εάν έχουν καταχωρίσει τα κατάλληλα διαπιστευτήρια που τους παρέχουν τη δυνατότητα να ανταποκρίνονται σε αυτές τις πολιτικές.

Για να προσθέσετε κι άλλους χρήστες, κάντε κλικ στο κουμπί **Add** (Προσθήκη).

Για να διαγράψετε ένα χρήστη, κάντε κλικ στο χρήστη και έπειτα κάντε κλικ στο κουμπί **Delete** (Διαγραφή).

Για να καταχωρίσετε αποτυπώματα ή να ορίσετε επιπλέον διαπιστευτήρια για ένα χρήστη, κάντε κλικ στο χρήστη και έπειτα κάντε κλικ στο κουμπί **Enroll** (Εγγραφή).

Για να δείτε τις πολιτικές για ένα συγκεκριμένο χρήστη, επιλέξτε το χρήστη και έπειτα κάντε κλικ στο κουμπί **View Policies** (Προβολή πολιτικών).

Προσδιορισμός ρυθμίσεων συσκευής

Από την εφαρμογή Device (Συσκευή), μπορείτε να προσδιορίσετε τις ρυθμίσεις που θα είναι διαθέσιμες για κάθε ενσωματωμένη ή συνδεδεμένη συσκευή ασφαλείας που αναγνωρίζει το HP ProtectTools Security Manager.

Αποτυπώματα

Η σελίδα Fingerprints (Αποτυπώματα) έχει τρεις καρτέλες: Enrollment (Εγγραφή), Sensitivity (Ευαισθησία) και Advanced (Για προχωρημένους).

Enrollment (Εγγραφή)

Μπορείτε να επιλέξετε τον ελάχιστο και το μέγιστο αριθμό αποτυπωμάτων που μπορεί να καταχωρίσει ένας χρήστης.

Μπορείτε επίσης να διαγράψετε όλα τα δεδομένα από τη συσκευή ανάγνωσης αποτυπωμάτων.

⚠ **ΠΡΟΕΙΔ/ΣΗ!** Θα διαγραφούν όλα τα δεδομένα αποτυπωμάτων για όλους τους χρήστες, περιλαμβανομένων των διαχειριστών. Εάν η πολιτική σύνδεσης απαιτεί τη χρήση αποτυπωμάτων αποκλειστικά, ενδέχεται να μην μπορεί να συνδεθεί στον υπολογιστή κανένας από τους χρήστες.

Sensitivity (Ευαισθησία)

Για να προσαρμόσετε την ευαισθησία της συσκευής ανάγνωσης αποτυπωμάτων κατά τη σάρωση αποτυπωμάτων, μετακινήστε το ρυθμιστικό.

Εάν δεν γίνεται συνεπής αναγνώριση του αποτυπώματός σας, μπορεί να απαιτείται ρύθμιση μικρότερης ευαισθησίας. Μια μεγαλύτερη ρύθμιση αυξάνει την ευαισθησία στις διαφορές των σαρώσεων αποτυπωμάτων και κατά συνέπεια μειώνει την πιθανότητα εσφαλμένης αποδοχής. Η μεσαία-υψηλή ρύθμιση παρέχει μια καλή αναλογία ασφάλειας και εξυπηρετικότητας.

Advanced (Για προχωρημένους)

Μπορείτε να διαμορφώσετε τη συσκευή ανάγνωσης αποτυπωμάτων έτσι ώστε να εξοικονομεί ενέργεια όταν ο υπολογιστής λειτουργία με τροφοδοσία από την μπαταρία.

Έξυπνη κάρτα

Μπορείτε να διαμορφώσετε τον υπολογιστή έτσι ώστε να κλειδώνει αυτόματα όταν αφαιρείται μια έξυπνη κάρτα. Ωστόσο, ο υπολογιστής θα κλειδώνει μόνο εάν η έξυπνη κάρτα χρησιμοποιούταν ως διαπιστευτήριο ελέγχου ταυτότητας κατά τη σύνδεση στα Windows. Η αφαίρεση μιας έξυπνης κάρτας που δεν χρησιμοποιούταν για σύνδεση στα Windows δεν θα προκαλέσει κλείδωμα του υπολογιστή.

▲ Επιλέξτε το πλαίσιο ελέγχου για να ενεργοποιήσετε ή να απενεργοποιήσετε το κλείδωμα του υπολογιστή κατά την αφαίρεση έξυπνης κάρτας.

4 Διαμόρφωση εφαρμογών

Η πρόσβαση στην ομάδα Applications (Εφαρμογές) γίνεται από το παράθυρο του μενού Security Applications (Εφαρμογές ασφαλείας) στην αριστερή πλευρά του HP ProtectTools Administrative Console. Μπορείτε να χρησιμοποιήσετε το μενού Settings (Ρυθμίσεις) για να προσαρμόσετε τη συμπεριφορά των εγκατεστημένων εφαρμογών του HP ProtectTools Security Manager.

Για να επεξεργαστείτε τις ρυθμίσεις εφαρμογών:

1. Στο μενού Tools (Εργαλεία), επιλέξτε **Settings** (Ρυθμίσεις) από την ομάδα **Applications** (Εφαρμογές).
2. Κάντε κλικ για να ενεργοποιήσετε ή να απενεργοποιήσετε μια συγκεκριμένη ρύθμιση.
3. Κάντε κλικ στο κουμπί **Apply** (Εφαρμογή) για να αποθηκεύσετε τις αλλαγές που έχετε κάνει.

Καρτέλα General (Γενικά)

Στην καρτέλα General (Γενικά) υπάρχουν οι παρακάτω ρυθμίσεις:

- **Do not automatically launch the Setup Wizard for administrators** (Να μην γίνεται αυτόματη εκκίνηση του οδηγού εγκατάστασης για διαχειριστές) — Ορίστε αυτή την επιλογή για να μην ανοίγει αυτόματα ο οδηγός κατά τη σύνδεση.
- **Do not automatically launch the Getting Started wizard for users** (Να μην γίνεται αυτόματη εκκίνηση του οδηγού έναρξης χρήσης για χρήστες) — Ορίστε αυτή την επιλογή για να μην ανοίγει αυτόματα ο οδηγός ρύθμισης χρήστη κατά τη σύνδεση.

Καρτέλα Applications (Εφαρμογές)

Οι ρυθμίσεις που εμφανίζονται εδώ μπορούν να αλλάξουν κατά την προσθήκη νέων εφαρμογών στο Security Manager. Οι ελάχιστες ρυθμίσεις που εμφανίζονται από προεπιλογή είναι οι εξής:

- **Security Manager** — Ενεργοποιεί την εφαρμογή Security Manager για όλους τους χρήστες του υπολογιστή.
- **Enable the Discover more button** (Ενεργοποίηση του κουμπιού ανακάλυψης περισσότερων εφαρμογών) — Δίνει στους χρήστες του υπολογιστή τη δυνατότητα να προσθέτουν εφαρμογές στο HP ProtectTools Security Manager κάνοντας κλικ στο κουμπί **[+] Discover more** ([+] Ανακάλυψη περισσότερων).

Για να επαναφέρετε όλες τις εφαρμογές στις εργοστασιακές τους ρυθμίσεις, κάντε κλικ στο κουμπί **Restore Defaults** (Επαναφορά προεπιλογών).

5 Προσθήκη εργαλείων διαχείρισης

Μπορεί να υπάρχουν κι άλλες εφαρμογές διαθέσιμες για την προσθήκη νέων εργαλείων διαχείρισης στο Security Manager. Ο διαχειριστής του υπολογιστή μπορεί να απενεργοποιήσει αυτή τη λειτουργία μέσω της εφαρμογής Settings (Ρυθμίσεις).

Για να προσθέσετε κι άλλα εργαλεία διαχείρισης, κάντε κλικ στο κουμπί **[+] Management tools** ([+] Εργαλεία διαχείρισης).

Μπορείτε να αποκτήσετε πρόσβαση στην τοποθεσία web DigitalPersona για να ελέγξετε εάν υπάρχουν νέες εφαρμογές ή μπορείτε να ορίσετε ένα χρονοδιάγραμμα για αυτόματες ενημερώσεις.

6 HP ProtectTools Security Manager

Το HP ProtectTools Security Manager σάς δίνει τη δυνατότητα να αυξήσετε σημαντικά την ασφάλεια του υπολογιστή σας.

Μπορείτε να χρησιμοποιήσετε προφορτωμένες εφαρμογές του Security Manager, καθώς και επιπλέον εφαρμογές που διατίθενται για άμεση λήψη από το web για τις εξής εργασίες:

- Διαχείριση ονομάτων σύνδεσης και κωδικών πρόσβασης
- Εύκολη αλλαγή του κωδικού πρόσβασης στο λειτουργικό σύστημα των Windows®
- Ορισμός προτιμήσεων προγράμματος
- Χρήση αποτυπωμάτων για επιπλέον ασφάλεια και εξυπηρετικότητα
- Εγκατάσταση έξυπνης κάρτας για έλεγχο ταυτότητας
- Δημιουργία αντιγράφων ασφαλείας και επαναφορά των δεδομένων του προγράμματος
- Προσθήκη περισσότερων εφαρμογών

Διαδικασίες ρύθμισης

Έναρξη χρήσης

Ο οδηγός ρύθμισης του HP ProtectTools εμφανίζεται αυτόματα ως η προεπιλεγμένη σελίδα στο HP ProtectTools Security Manager έως ότου ολοκληρωθεί η ρύθμιση.

Για να ρυθμίσετε το Security Manager, ακολουθήστε τα παρακάτω βήματα:

ΣΗΜΕΙΩΣΗ Εάν δεν υπάρχει διαθέσιμη συσκευή ανάγνωσης αποτυπωμάτων ή έξυπνη κάρτα, πραγματοποιήστε μόνο τα βήματα 1, 5 και 6.

1. Στη σελίδα υποδοχής, κάντε κλικ στο κουμπί **Next** (Επόμενο).
2. Η επόμενη σελίδα αναφέρει τις μεθόδους ελέγχου ταυτότητας που είναι διαθέσιμες στον υπολογιστή. Κάντε κλικ στο κουμπί **Next** (Επόμενο) για να συνεχίσετε.
3. Στη σελίδα Verify Your Identity (Επαλήθευση ταυτότητας), πληκτρολογήστε τον κωδικό πρόσβασης των Windows και κάντε κλικ στο κουμπί **Next** (Επόμενο).
4. Ανατρέξτε σε ένα ή περισσότερα από τα παρακάτω θέματα ανάλογα με τη διαμόρφωση του υπολογιστή σας.
   - Εάν υπάρχει διαθέσιμη συσκευή ανάγνωσης αποτυπωμάτων, δείτε Καταχώριση αποτυπωμάτων στη σελίδα 25.
   - Εάν υπάρχει διαθέσιμη έξυπνη κάρτα, δείτε Εγκατάσταση έξυπνης κάρτας στη σελίδα 26.
5. Εάν δεν υπάρχει διαθέσιμη ούτε συσκευή ανάγνωσης αποτυπωμάτων ούτε έξυπνη κάρτα, θα σας ζητηθεί να πληκτρολογήσετε τον κωδικό πρόσβασής σας στα Windows. Θα πρέπει να χρησιμοποιείτε αυτό τον κωδικό πρόσβασης κάθε φορά που απαιτείται έλεγχος ταυτότητας στο μέλλον.
6. Στην τελευταία σελίδα του οδηγού, κάντε κλικ στο κουμπί **Finish** (Τέλος).

   Εμφανίζεται ο πίνακας εργαλείων του Security Manager.

Καταχώριση διαπιστευτηρίων

Μπορείτε να χρησιμοποιήσετε τη σελίδα My Identity (Η ταυτότητά μου) για να καταχωρίσετε τις διάφορες μεθόδους ελέγχου ταυτότητας ή τα διαπιστευτήρια. Μετά την καταχώρισή τους, μπορείτε να χρησιμοποιήσετε αυτές τις μεθόδους για να συνδεθείτε στο Security Manager.

Καταχώριση αποτυπωμάτων

Εάν ο υπολογιστής διαθέτει ενσωματωμένη ή συνδεδεμένη συσκευή ανάγνωσης αποτυπωμάτων, ο οδηγός ρύθμισης του HP ProtectTools θα σας καθοδηγήσει στη διαδικασία ορισμού ή καταχώρισης των αποτυπωμάτων σας.

1. Διαβάστε την οθόνη υποδοχής και κάντε κλικ στο κουμπί **Next** (Επόμενο).
2. Επαληθεύστε την ταυτότητά σας πληκτρολογώντας τον κωδικό πρόσβασης των Windows, εάν δεν έχετε καταχωρίσει αποτυπώματα ακόμα ή σαρώνοντας το αποτύπωμά σας με τη συσκευή ανάγνωσης αποτυπωμάτων. Κάντε κλικ στο κουμπί **Next** (Επόμενο).

   Εάν ο κωδικός σας πρόσβασης στα Windows είναι κενός, θα σας ζητηθεί να δημιουργήσετε ένα κωδικό. Ο κωδικός πρόσβασης των Windows είναι απαραίτητος για την προστασία του λογαριασμού σας στα Windows έναντι πρόσβασης από μη εξουσιοδοτημένα άτομα και για τη χρήση των λειτουργιών του HP ProtectTools Security Manager.
3. Εμφανίζεται το περίγραμμα δύο χεριών. Τα δάχτυλα που έχουν ήδη καταχωριστεί επισημαίνονται με πράσινο χρώμα. Κάντε κλικ σε ένα δάχτυλο πάνω στο περίγραμμα.

   ΣΗΜΕΙΩΣΗ Για να διαγράψετε ένα ήδη καταχωρισμένο αποτύπωμα, κάντε κλικ στο αντίστοιχο αποτύπωμα.
4. Όταν επιλέξετε δάχτυλο για καταχώριση, θα σας ζητηθεί να σαρώσετε αυτό το αποτύπωμα έως ότου ολοκληρωθεί η διαδικασία καταχώρισης επιτυχώς. Τα καταχωρισμένα δάχτυλα επισημαίνονται με πράσινο χρώμα στο περίγραμμα.
5. Πρέπει να καταχωρίσετε τουλάχιστον δύο δάχτυλα, κατά προτίμηση το δείκτη ή το μέσο. Επαναλάβετε τα βήματα 3 και 4 για άλλο δάχτυλο.
6. Κάντε κλικ στο κουμπί **Next** (Επόμενο).

ΣΗΜΕΙΩΣΗ Κατά την καταχώριση αποτυπωμάτων μέσω της διαδικασίας έναρξης χρήσης, οι πληροφορίες των αποτυπωμάτων δεν αποθηκεύονται έως ότου κάνετε κλικ στο κουμπί **Next** (Επόμενο). Εάν αφήσετε τον υπολογιστή ανενεργό για κάποιο διάστημα ή κλείσετε τον πίνακα εργαλείων, οι αλλαγές που έχετε κάνει **δεν** αποθηκεύονται.

Αλλαγή κωδικού πρόσβασης στα Windows

Το Security Manager καθιστά την αλλαγή του κωδικού πρόσβασης στα Windows απλούστερη και ταχύτερη σε σύγκριση με τη διαδικασία μέσω του Πίνακα Ελέγχου των Windows.

Για να αλλάξετε τον κωδικό πρόσβασής σας στα Windows, ακολουθήστε τα παρακάτω βήματα:

1. Στον πίνακα εργαλείων του Security Manager, επιλέξτε διαδοχικά **My Identity** (Η ταυτότητά μου), **Credentials** (Διαπιστευτήρια) και τέλος **Password** (Κωδικός πρόσβασης).
2. Πληκτρολογήστε τον τρέχοντα κωδικό πρόσβασης στο πλαίσιο κειμένου **Current Windows password** (Τρέχων κωδικός πρόσβασης στα Windows).
3. Πληκτρολογήστε ένα νέο κωδικό πρόσβασης στο πλαίσιο κειμένου **New Windows password** (Νέος κωδικός πρόσβασης στα Windows) και έπειτα πληκτρολογήστε τον κωδικό ξανά στο πλαίσιο κειμένου **Confirm new password** (Επιβεβαίωση νέου κωδικού πρόσβασης).
4. Κάντε κλικ στο κουμπί **Change** (Αλλαγή) για να αλλάξετε άμεσα τον τρέχοντα κωδικό πρόσβασης με τον καινούργιο κωδικό που πληκτρολογήσατε.

Εγκατάσταση έξυπνης κάρτας

Εάν ο υπολογιστής σας διαθέτει ενσωματωμένη ή συνδεδεμένη συσκευής ανάγνωσης έξυπνων καρτών, το Security Manager θα σας ζητήσει να ορίσετε ένα κωδικό PIN για την έξυπνη κάρτα.

- Για να ορίσετε κωδικό PIN για την έξυπνη κάρτα — Πληκτρολογήστε και επιβεβαιώστε ένα κωδικό PIN στη σελίδα Set up smart card (Ρύθμιση έξυπνης κάρτας).
- Για να αλλάξετε τον κωδικό PIN — Πληκτρολογήστε πρώτα τον παλιό κωδικό PIN και έπειτα επιλέξτε ένα καινούργιο.

Χρήση του πίνακα εργαλείων του Security Manager

Ο πίνακας εργαλείων του Security Manager είναι η κεντρική τοποθεσία για εύκολη πρόσβαση στις λειτουργίες, τις εφαρμογές και τις ρυθμίσεις του Security Manager.

Ο πίνακας εργαλείων αποτελείται από τα εξής στοιχεία:

- **ID Card** (Ταυτότητα) — Εμφανίζει το όνομα χρήστη των Windows και μια επιλεγμένη εικόνα που απεικονίζει τον συνδεδεμένο χρήστη.
- **Security Applications** (Εφαρμογές ασφαλείας) — Εμφανίζει ένα επεκτεινόμενο μενού συνδέσεων για τη διαμόρφωση των παρακάτω κατηγοριών ασφαλείας:
  - **My Identity (Η ταυτότητά μου)**
  - **My Data (Τα δεδομένα μου)**
  - **My Computer (Ο υπολογιστής μου)**
- **Discover more** (Ανακάλυψη περισσότερων) — Ανοίγει μια σελίδα στην οποία μπορείτε να βρείτε περισσότερες εφαρμογές για τη βελτίωση της ασφάλειας της ταυτότητας, των δεδομένων και των επικοινωνιών σας.
- **Main area** (Βασική περιοχή) — Εμφανίζει οθόνες συγκεκριμένων εφαρμογών.
- **Administration** (Διαχείριση) — Ανοίγει το HP ProtectTools Administrative Console.
- **Help button** (Κουμπί βοήθειας) — Εμφανίζει πληροφορίες για την τρέχουσα οθόνη.
- **Advanced** (Για προχωρημένους) — Σας παρέχει πρόσβαση στις παρακάτω επιλογές:
  - **Preferences** (Προτιμήσεις) — Σας δίνει τη δυνατότητα να εξατομικεύσετε τις ρυθμίσεις του Security Manager.
  - **Backup and Restore** (Δημιουργία αντιγράφων ασφαλείας και επαναφορά) — Σας δίνει τη δυνατότητα να δημιουργείτε αντίγραφα ασφαλείας και να επαναφέρετε δεδομένα.
  - **About** (Πληροφορίες) — Εμφανίζει πληροφορίες έκδοσης σχετικά με το Security Manager.

Για να ανοίξετε τον πίνακα εργαλείων του Security Manager, κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Security Manager**.

Άνοιγμα του HP ProtectTools Security Manager

Μπορείτε να ανοίξετε το HP ProtectTools Security Manager με οποιονδήποτε από τους παρακάτω τρόπους:

- Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Security Manager**.
- Κάντε διπλό κλικ στο εικονίδιο **HP ProtectTools** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών.
- Κάντε δεξί κλικ στο εικονίδιο του **HP ProtectTools** και επιλέξτε **Open HP ProtectTools Security Manager** (Άνοιγμα του HP ProtectTools Security Manager).
- Κάντε κλικ στη μικροεφαρμογή **Security Manager ID Card** (Ταυτότητα του Security Manager) στην πλευρική εργαλειοθήκη των Windows.
- Πατήστε το συνδυασμό πλήκτρων πρόσβασης ctrl+alt+h για να ανοίξετε το μενού Quick Links (Γρήγορες συνδέσεις) του Security Manager.

Γενικές εργασίες

Οι εφαρμογές που περιλαμβάνονται σε αυτή την ομάδα σάς βοηθούν στη διαχείριση διάφορων πτυχών της ψηφιακής σας ταυτότητας.

- **Security Manager** — Δημιουργεί και διαχειρίζεται γρήγορες συνδέσεις, οι οποίες σας δίνουν τη δυνατότητα να ανοίγετε και να συνδέεστε σε τοποθεσίες web και προγράμματα πραγματοποιώντας έλεγχο ταυτότητας με τον κωδικό πρόσβασής σας στα Windows, το αποτύπωμά σας ή μια έξυπνη κάρτα.
- **Credentials** (Διαπιστευτήρια) — Σας δίνει τη δυνατότητα να αλλάξετε τον κωδικό πρόσβασής σας στα Windows, να καταχωρίσετε τα αποτυπώματά σας ή να ρυθμίσετε μια έξυπνη κάρτα με ευκολία.

Για να προσθέσετε περισσότερες εφαρμογές, κάντε κλικ στο κουμπί [+] **Discover more** (Ανακάλυψη περισσότερων) στην κάτω αριστερή γωνία του πίνακα εργαλείων. Το κουμπί αυτό μπορεί να απενεργοποιηθεί από το διαχειριστή.

Password Manager

Η σύνδεση στα Windows, τοποθεσίες web και εφαρμογές είναι πιο εύκολη και ασφαλής όταν χρησιμοποιείτε το Password Manager. Μπορείτε να το χρησιμοποιήσετε για να δημιουργήσετε ισχυρότερους κωδικούς πρόσβασης που δεν χρειάζεται να σημειώσετε ή να απομνημονεύσετε και έπειτα να συνδεθείτε εύκολα και γρήγορα μέσω αποτυπώματος, έξυπνης κάρτας ή κωδικού πρόσβασης στα Windows.

Το Password Manager παρέχει τις παρακάτω επιλογές:

- Προσθήκη, επεξεργασία ή διαγραφή ονομάτων σύνδεσης από την καρτέλα Manage (Διαχείριση).
- Χρήση του μενού Quick Links (Γρήγορες συνδέσεις) για άνοιγμα του προεπιλεγμένου προγράμματος περιήγησης και σύνδεση σε τοποθεσία web ή πρόγραμμα, μετά τη ρύθμιση.
- Μεταφορά και απόθεση για οργάνωση του μενού Quick Links (Γρήγορες συνδέσεις) σε κατηγορίες.
- Έλεγχος με μια ματιά της ύπαρξης κινδύνου ασφαλείας για κάποιον από τους κωδικούς πρόσβασης και αυτόματη δημιουργία περίπλοκου, ισχυρού κωδικού πρόσβασης που θα χρησιμοποιείται για νέες τοποθεσίες.

Πολλές από τις λειτουργίες του Password Manager διατίθενται επίσης από το εικονίδιο του Password Manager που εμφανίζεται όταν γίνεται εστίαση σε οθόνη σύνδεσης σε σελίδα web ή πρόγραμμα. Κάντε κλικ στο εικονίδιο για να εμφανιστεί ένα μενού περιβάλλοντος από το οποίο μπορείτε να επιλέξετε μεταξύ των παρακάτω επιλογών.

Για σελίδες web ή προγράμματα που δεν έχει δημιουργηθεί ακόμα όνομα σύνδεσης

Το μενού περιβάλλοντος εμφανίζει τις παρακάτω επιλογές:

- **Add [somedomain.com] to the Password Manager** (Προσθήκη [τομέας.com] στο Password Manager) — Σας επιτρέπει να προσθέσετε όνομα σύνδεσης για την τρέχουσα οθόνη σύνδεσης.
- **Open Password Manager** (Άνοιγμα του Password Manager) — Εκκινεί το Password Manager.
- **Icon settings** (Ρυθμίσεις εικονιδίου) — Σας επιτρέπει να ορίσετε τις συνθήκες στις οποίες θα εμφανίζεται το εικονίδιο του Password Manager.
- **Help** (Βοήθεια) — Εμφανίζει τη βοήθεια του λογισμικού Password Manager.

Για σελίδες web ή προγράμματα στα οποία έχει ήδη δημιουργηθεί όνομα σύνδεσης

Το μενού περιβάλλοντος εμφανίζει τις παρακάτω επιλογές:

- **Fill in logon data** (Καταχώριση δεδομένων σύνδεσης) — Συμπληρώνει τα δεδομένα σύνδεσης στα πεδία σύνδεσης και, στη συνέχεια, υποβάλλει τη σελίδα (εφόσον έχει οριστεί η επιλογή υποβολής κατά τη δημιουργία ή τελευταία επεξεργασία της σύνδεσης).
- **Edit logon** (Επεξεργασία σύνδεσης) — Σας επιτρέπει να επεξεργαστείτε τα δεδομένα σύνδεσης για τη συγκεκριμένη τοποθεσία web.
- **Add a New Account** (Προσθήκη νέου λογαριασμού) — Σας επιτρέπει να προσθέσετε ένα λογαριασμό σε σύνδεση.
- **Open Password Manager** (Άνοιγμα του Password Manager) — Εκκινεί την εφαρμογή Password Manager.
- **Help** (Βοήθεια) — Εμφανίζει τη βοήθεια του λογισμικού Password Manager.

ΣΗΜΕΙΩΣΗ Ο διαχειριστής αυτού του υπολογιστή μπορεί να έχει ρυθμίσει το Security Manager έτσι ώστε να απαιτεί περισσότερα από ένα διαπιστευτήρια κατά την επαλήθευση της ταυτότητάς σας.

Προσθήκη ονομάτων σύνδεσης

Μπορείτε εύκολα να προσθέσετε ένα όνομα σύνδεσης για τοποθεσία web ή πρόγραμμα εισάγοντας τα στοιχεία σύνδεσης μία φορά. Στη συνέχεια, το Password Manager θα εισάγει αυτόματα τα στοιχεία για σας. Μπορείτε να χρησιμοποιήσετε αυτά τα ονόματα σύνδεσης μετά την περιήγηση στην τοποθεσία web ή το πρόγραμμα ή μπορείτε να κάνετε κλικ σε ένα όνομα σύνδεσης από το μενού **Logons** (Ονόματα σύνδεσης) προκειμένου να ανοίξει το Password Manager την τοποθεσία web ή το πρόγραμμα και να πραγματοποιήσει σύνδεση.

Για να προσθέσετε ένα όνομα σύνδεσης:

1. Ανοίξτε την οθόνη σύνδεσης για μια τοποθεσία web ή πρόγραμμα.
2. Κάντε κλικ στο βέλος στο εικονίδιο του **Password Manager** και, στη συνέχεια, κάντε κλικ σε μία από τις ακόλουθες επιλογές, ανάλογα με το αν πρόκειται για οθόνη σύνδεσης σε τοποθεσία web ή πρόγραμμα:
   - Για τοποθεσία web, επιλέξτε **Add [domain name] to Password Manager** (Προσθήκη [όνομα τομέα] στο Password Manager).
   - Για πρόγραμμα, επιλέξτε **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 επισημαίνονται με ένα έντονο πορτοκαλί πλαίσιο. Μπορείτε επίσης να προβάλετε αυτό το πλαίσιο διαλόγου κάνοντας κλικ στην επιλογή **Add Logon** (Προσθήκη ονόματος σύνδεσης) από την καρτέλα **Password Manager Manage** (Διαχείριση του Password Manager). Ορισμένες επιλογές εξαρτώνται από τις συσκευές ασφαλείας που είναι συνδεδεμένες στον υπολογιστή, όπως για παράδειγμα, η χρήση του πλήκτρου πρόσβασης ctrl+alt+H, η σάρωση αποτυπώματος ή η εισαγωγή κάρτας Smart Card.
   - Για να συμπληρώσετε ένα πεδίο σύνδεσης με μία από τις ήδη διαμορφωμένες επιλογές, κάντε κλικ στα βέλη που βρίσκονται δεξιά από το πεδίο.
   - Για να προσθέσετε κι άλλα πεδία από την οθόνη στο όνομα σύνδεσης, επιλέξτε **Choose other fields** (Επιλογή άλλων πεδίων).

- Για να συμπληρωθούν τα πεδία σύνδεσης αλλά να μην γίνει υποβολή τους, απενεργοποιήστε το πλαίσιο ελέγχου **Submit logon data** (Υποβολή δεδομένων σύνδεσης).
- Για να δείτε τον κωδικό πρόσβασης για τη συγκεκριμένη σύνδεση, επιλέξτε **Show password** (Εμφάνιση κωδικού πρόσβασης).

4. Κάντε κλικ στο **OK**.

   Το σύμβολο συν αφαιρείται από το εικονίδιο του Password Manager υποδεικνύοντας ότι δημιουργήθηκε η σύνδεση.

Κάθε φορά που αποκτάτε πρόσβαση στη συγκεκριμένη τοποθεσία web ή μεταβαίνετε στο συγκεκριμένο πρόγραμμα, εμφανίζεται το εικονίδιο του Password Manager υποδεικνύοντας ότι μπορείτε να χρησιμοποιήσετε τα καταχωρισμένα διαπιστευτήρια για να συνδεθείτε.

Επεξεργασία ονομάτων σύνδεσης

Για να επεξεργαστείτε ένα όνομα σύνδεσης, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε την οθόνη σύνδεσης για μια τοποθεσία web ή πρόγραμμα.
2. Για να προβάλετε ένα πλαίσιο διαλόγου, στο οποίο μπορείτε να επεξεργαστείτε τα στοιχεία σύνδεσης, κάντε κλικ στο βέλος στο εικονίδιο του **Password Manager** και, στη συνέχεια, επιλέξτε **Edit logon** (Επεξεργασία ονόματος σύνδεσης). Τα πεδία σύνδεσης στην οθόνη και τα αντίστοιχα πεδία στο πλαίσιο διαλόγου επισημαίνονται με ένα έντονο πορτοκαλί πλαίσιο.

   Μπορείτε επίσης να προβάλετε αυτό το πλαίσιο διαλόγου κάνοντας κλικ στην επιλογή **Edit for the desired logon** (Επεξεργασία για το επιθυμητό όνομα σύνδεσης) στην καρτέλα **Password Manager Manage** (Διαχείριση του Password Manager).
3. Επεξεργαστείτε τα στοιχεία σύνδεσης.
   - Για να συμπληρώσετε ένα πεδίο σύνδεσης με μία από τις ήδη διαμορφωμένες επιλογές, κάντε κλικ στα βέλη που βρίσκονται δεξιά από το πεδίο.
   - Για να προσθέσετε κι άλλα πεδία από την οθόνη στο όνομα σύνδεσης, επιλέξτε **Choose other fields** (Επιλογή άλλων πεδίων).
   - Για να συμπληρωθούν τα πεδία σύνδεσης αλλά να μην γίνει υποβολή τους, απενεργοποιήστε το πλαίσιο ελέγχου **Submit logon data** (Υποβολή δεδομένων σύνδεσης).
   - Για να δείτε τον κωδικό πρόσβασης για τη συγκεκριμένη σύνδεση, επιλέξτε **Show password** (Εμφάνιση κωδικού πρόσβασης).
4. Κάντε κλικ στο **OK**.

Χρήση του μενού ονομάτων σύνδεσης

Το Password Manager παρέχει ένα γρήγορο και εύκολο τρόπο για το άνοιγμα τοποθεσιών web και προγραμμάτων, για τα οποία έχετε δημιουργήσει ονόματα σύνδεσης. Κάντε διπλό κλικ σε ένα όνομα σύνδεσης προγράμματος ή τοποθεσίας web από το μενού **Logons** (Ονόματα σύνδεσης) ή από την καρτέλα **Manage** (Διαχείριση) του **Password Manager** για να ανοίξετε την οθόνη σύνδεσης και, στη συνέχεια, συμπληρώστε τα δεδομένα σύνδεσης.

Όταν δημιουργείτε ένα όνομα σύνδεσης, προστίθεται αυτόματα στο μενού Logons (Ονόματα σύνδεσης) του Password Manager.

Για να προβάλετε το μενού Logons (Ονόματα σύνδεσης):

1. Πατήστε το συνδυασμό πλήκτρων πρόσβασης του **Password Manager**. Ο συνδυασμός ctrl+alt +h αποτελεί την εργοστασιακή ρύθμιση. Για να αλλάξετε το συνδυασμό πλήκτρων πρόσβασης, επιλέξτε **Password Manager** και έπειτα **Settings** (Ρυθμίσεις).
2. Πραγματοποιήστε σάρωση αποτυπώματος (σε υπολογιστές με ενσωματωμένη ή συνδεδεμένη συσκευή ανάγνωσης αποτυπωμάτων).

Οργάνωση ονομάτων σύνδεσης σε κατηγορίες

Χρησιμοποιήστε κατηγορίες για να ταξινομήσετε τα ονόματα σύνδεσης που διαθέτετε δημιουργώντας μία ή περισσότερες κατηγορίες. Στη συνέχεια, μεταφέρετε τα ονόματα σύνδεσης στις επιθυμητές κατηγορίες.

Για να προσθέσετε μια κατηγορία:

1. Στον πίνακα εργαλείων του Security Manager, επιλέξτε **Password Manager**.
2. Κάντε κλικ στην καρτέλα **Manage** (Διαχείριση) και, στη συνέχεια, επιλέξτε **Add Category** (Προσθήκη κατηγορίας).
3. Εισαγάγετε όνομα για την κατηγορία.
4. Κάντε κλικ στο **OK**.

Για να προσθέσετε ένα όνομα σύνδεσης σε κατηγορία:

1. Τοποθετήστε το δείκτη του ποντικιού στο επιθυμητό όνομα σύνδεσης.
2. Πατήστε παρατεταμένα το αριστερό κουμπί του ποντικιού.
3. Μεταφέρετε το όνομα σύνδεσης στη λίστα κατηγοριών. Καθώς μετακινείτε το ποντίκι πάνω στις κατηγορίες, αυτές θα επισημαίνονται.
4. Απελευθερώστε το κουμπί του ποντικού όταν επισημανθεί η κατηγορία που θέλετε.

Τα ονόματα σύνδεσης δεν μετακινούνται στην κατηγορία αλλά αντιγράφονται στην επιλεγμένη κατηγορία. Μπορείτε να προσθέσετε το ίδιο όνομα σύνδεσης σε περισσότερες από μία κατηγορίες και μπορείτε να προβάλετε όλα τα ονόματα σύνδεσης που διαθέτετε κάνοντας κλικ στην επιλογή **All** (Όλα).

Διαχείριση ονομάτων σύνδεσης

Το Password Manager διευκολύνει τη διαχείριση στοιχείων σύνδεσης για ονόματα χρήστη, κωδικούς πρόσβασης και πολλούς λογαριασμούς σύνδεσης, από μία κεντρική τοποθεσία.

Τα ονόματα σύνδεσης παρατίθενται στην καρτέλα Manage (Διαχείριση). Εάν έχουν δημιουργηθεί πολλά ονόματα σύνδεσης για την ίδια τοποθεσία web, κάθε όνομα σύνδεσης παρατίθεται κάτω από το όνομα της τοποθεσίας web και εισάγεται στη λίστα ονομάτων σύνδεσης.

Για να διαχειριστείτε τα ονόματα σύνδεσης:

Στον πίνακα εργαλείων του Security Manager, επιλέξτε **Password Manager** και, στη συνέχεια, κάντε κλικ στην καρτέλα **Manage** (Διαχείριση).

- **Add a logon** (Προσθήκη ονόματος σύνδεσης) — Επιλέξτε **Add Logon** (Προσθήκη ονόματος σύνδεσης) και ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.
- **Edit a logon** (Επεξεργασία ονόματος σύνδεσης) — Κάντε κλικ σε ένα όνομα σύνδεσης, επιλέξτε **Edit** (Επεξεργασία) και, στη συνέχεια, τροποποιήστε τα δεδομένα σύνδεσης.
- **Delete a logon** (Διαγραφή ονόματος σύνδεσης) — Κάντε κλικ σε ένα όνομα σύνδεσης και, στη συνέχεια, επιλέξτε **Delete** (Διαγραφή).

Για να προσθέσετε κι άλλο όνομα σύνδεσης για μια τοποθεσία web ή πρόγραμμα:

1. Ανοίξτε την οθόνη σύνδεσης για την τοποθεσία web ή το πρόγραμμα.
2. Κάντε κλικ στο εικονίδιο του **Password manager** για να προβάλετε το μενού συντομεύσεων.
3. Επιλέξτε **Add additional logon** (Προσθήκη επιπλέον ονόματος σύνδεσης) και, στη συνέχεια, ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Αξιολόγηση της ισχύος του κωδικού πρόσβασης

Η χρήση ισχυρών κωδικών πρόσβασης για τη σύνδεση σε τοποθεσίες web και προγράμματα αποτελεί μια σημαντική πτυχή για την προστασία της ταυτότητάς σας.

Το Password Manager διευκολύνει την παρακολούθηση και τη βελτίωση της ασφάλειας με μια άμεση και αυτοματοποιημένη ανάλυση της ισχύος κάθε κωδικού πρόσβασης που χρησιμοποιείται για τη σύνδεση σε τοποθεσίες web και προγράμματα.

Ρυθμίσεις εικονιδίου του Password Manager

Το Password Manager επιχειρεί να εντοπίσει οθόνες σύνδεσης για τοποθεσίες web και προγράμματα. Εάν εντοπίσει μια οθόνη σύνδεσης για την οποία δεν έχετε δημιουργήσει όνομα σύνδεσης, το Password Manager υποδεικνύει ότι πρέπει να προσθέσετε όνομα σύνδεσης για την οθόνη προβάλλοντας το εικονίδιο του Password Manager με το σύμβολο "+".

Κάντε κλικ στο βέλος του εικονιδίου και επιλέξτε **Icon Settings** (Ρυθμίσεις εικονιδίου) για να προσαρμόσετε τον τρόπο με τον οποίο το **Password Manager** διαχειρίζεται πιθανές τοποθεσίες σύνδεσης.

- **Prompt to add logons for logon screens** (Προτροπή για προσθήκη ονομάτων σύνδεσης για οθόνες σύνδεσης) — Κάντε κλικ σε αυτή την επιλογή για να ρυθμίσετε το Password Manager έτσι ώστε να σας προτρέπει να προσθέτετε όνομα σύνδεσης όταν προκύπτει ότι δεν έχει οριστεί όνομα σύνδεσης σε μια οθόνη σύνδεσης.
- **Exclude this screen** (Εξαίρεση αυτής της οθόνης) — Επιλέξτε αυτό το πλαίσιο ελέγχου για να μην λάβετε ξανά ειδοποίηση από το Password Manager να προσθέσετε όνομα σύνδεσης για τη συγκεκριμένη οθόνη σύνδεσης.

Για να αποκτήσετε πρόσβαση σε περισσότερες ρυθμίσεις του Password Manager, επιλέξτε **Password Manager** και, στη συνέχεια, κάντε κλικ στην επιλογή **Ρυθμίσεις** στον πίνακα εργαλείων του Security Manager.

Ρυθμίσεις

Μπορείτε να ορίσετε ρυθμίσεις για την προσαρμογή του HP ProtectTools Security Manager:

1. **Prompt to add logons for logon screens** (Προτροπή για προσθήκη ονομάτων σύνδεσης για οθόνες σύνδεσης) — Το εικονίδιο του Password Manager με το σύμβολο συν εμφανίζεται κάθε φορά που εντοπίζεται μια τοποθεσία web ή οθόνη σύνδεσης προγράμματος υποδεικνύοντας ότι μπορείτε να προσθέσετε όνομα σύνδεσης για τη συγκεκριμένη οθόνη στο χώρο φύλαξης κωδικών πρόσβασης. Για να απενεργοποιήσετε αυτή τη λειτουργία, στο πλαίσιο διαλόγου **Icon Settings** (Ρυθμίσεις εικονιδίου), απενεργοποιήστε το πλαίσιο ελέγχου δίπλα στην επιλογή **Prompt to add logons for logon screens** (Προτροπή για προσθήκη ονομάτων σύνδεσης για οθόνες σύνδεσης).

2. **Open Password Manager with ctrl+alt+H** (Άνοιγμα του Password Manager με ctrl+alt+H) — Το προεπιλεγμένο πλήκτρο πρόσβασης που ανοίγει το μενού Quick Links (Γρήγορες συνδέσεις) του Password Manager είναι το ctrl+alt+H. Για να αλλάξετε το πλήκτρο πρόσβασης, κάντε κλικ σε αυτή την επιλογή και εισαγάγετε ένα νέο συνδυασμό πλήκτρων. Οι συνδυασμοί μπορούν να περιλαμβάνουν ένα ή περισσότερα από τα εξής: ctrl, alt ή shift και οποιοδήποτε αλφαβητικό ή αριθμητικό πλήκτρο.

3. Κάντε κλικ στο κουμπί **Apply** (Εφαρμογή) για να αποθηκεύσετε τις αλλαγές.

Διαπιστευτήρια

Τα διαπιστευτήρια στο Security Manager χρησιμοποιούνται για να επαληθεύσουν την ταυτότητά σας. Ο τοπικός διαχειριστής του υπολογιστή μπορεί να ορίσει ποια διαπιστευτήρια θα χρησιμοποιούνται για την απόδειξη της ταυτότητάς σας κατά τη σύνδεση στο λογαριασμό Windows που διαθέτετε, τοποθεσίες web ή προγράμματα.

Τα διαθέσιμα διαπιστευτήρια μπορεί να ποικίλλουν ανάλογα με τις συσκευές ασφαλείας που είναι ενσωματωμένες ή συνδεδεμένες στον υπολογιστή. Κάθε υποστηριζόμενο διαπιστευτήριο θα διαθέτει καταχώριση στην ομάδα **Η ταυτότητά μου, Διαπιστευτήρια**.

Παρατίθενται τα διαθέσιμα διαπιστευτήρια, απαιτήσεις και η τρέχουσα κατάσταση και μπορεί να περιλαμβάνουν τα εξής:

- Αποτυπώματα
- Κωδικός πρόσβασης
- Έξυπνη κάρτα

Για να καταχωρίσετε ή να αλλάξετε ένα διαπιστευτήριο, κάντε κλικ στη σύνδεση και ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Προσωπική ταυτότητα

Η ταυτότητα σάς αναγνωρίζει μοναδικά ως κάτοχο του λογαριασμού Windows, προβάλλοντας το όνομά σας και μια φωτογραφία της επιλογής σας. Εμφανίζεται ευκρινώς στην πάνω αριστερή γωνία των σελίδων του Security Manager και ως μικροεφαρμογή στην πλευρική εργαλειοθήκη των Windows.

Ένας από τους τρόπους με τους οποίους μπορείτε να αποκτήσετε γρήγορα πρόσβαση στο Security Manager είναι να κάνετε κλικ στην ταυτότητά σας στην πλευρική εργαλειοθήκη των Windows.

Μπορείτε να αλλάξετε τη φωτογραφία και τον τρόπο εμφάνισης του ονόματός σας. Από προεπιλογή, εμφανίζονται το πλήρες όνομα χρήστη που έχετε στα Windows και η φωτογραφία που επιλέξατε κατά την εγκατάσταση των Windows.

Για να αλλάξετε το εμφανιζόμενο όνομα:

1. Κάντε κλικ στην επιλογή **Η ταυτότητά μου** στην πάνω αριστερή γωνία στον πίνακα εργαλείων του Security Manager.
2. Κάντε κλικ στο πλαίσιο που δείχνει το όνομα που έχετε καταχωρίσει για το λογαριασμό σας στα Windows. Το σύστημα θα εμφανίζει το όνομα χρήστη των Windows για αυτό το λογαριασμό.
3. Για να αλλάξετε αυτό το όνομα, πληκτρολογήστε το νέο όνομα και κάντε κλικ στο κουμπί **Αποθήκευση**.

Για να αλλάξετε την εμφανιζόμενη φωτογραφία:

1. Κάντε κλικ στην επιλογή **Η ταυτότητά μου** και έπειτα επιλέξτε **Ταυτότητα** στην πάνω αριστερή γωνία στον πίνακα εργαλείων του Security Manager.
2. Κάντε κλικ στο κουμπί **Επιλογή φωτογραφίας**, κάντε κλικ σε μια εικόνα και έπειτα κάντε κλικ στο κουμπί **Αποθήκευση**.

Ορισμός προτιμήσεων

Μπορείτε να εξατομικεύσετε ρυθμίσεις για το HP ProtectTools Security Manager. Στον πίνακα εργαλείων του Security Manager, επιλέξτε **Για προχωρημένους** και έπειτα επιλέξτε **Προτιμήσεις**. Οι διαθέσιμες ρυθμίσεις εμφανίζονται σε δύο καρτέλες: "Γενικά" και "Αποτύπωμα".

Γενικά

Στην καρτέλα "Γενικά" υπάρχουν οι παρακάτω ρυθμίσεις:

Εμφάνιση — Εμφάνιση εικονιδίου στη γραμμή εργασιών

Επιλέξτε το πλαίσιο ελέγχου για να ενεργοποιήσετε την εμφάνιση του εικονιδίου στη γραμμή εργασιών.

Αποεπιλέξτε το πλαίσιο ελέγχου για να απενεργοποιήσετε την εμφάνιση του εικονιδίου στη γραμμή εργασιών.

Αποτύπωμα

Στην καρτέλα "Αποτύπωμα" υπάρχουν οι παρακάτω ρυθμίσεις:

Γρήγορες ενέργειες — Χρησιμοποιήστε τη ρύθμιση "Γρήγορες ενέργειες" για να επιλέξετε την εργασία του Security Manager που θα πραγματοποιηθεί όταν πατήσετε ένα συγκεκριμένο πλήκτρο κατά τη σάρωση του αποτυπώματός σας.

Για να εκχωρήσετε μια γρήγορη ενέργεια σε ένα από τα αναφερόμενα πλήκτρα:

- Κάντε κλικ σε μια επιλογή **(Πλήκτρο)+Αποτύπωμα** και έπειτα επιλέξτε μία από τις διαθέσιμες εργασίες από το μενού.

Σχόλια σάρωσης αποτυπωμάτων — Εμφανίζεται μόνο όταν υπάρχει συσκευή ανάγνωσης αποτυπωμάτων. Χρησιμοποιήστε αυτή τη ρύθμιση για να προσαρμόσετε τα σχόλια που δημιουργούνται όταν σαρώνετε το αποτύπωμά σας.

- **Ενεργοποίηση ηχητικών σχολίων** — Το Security Manager σάς παρέχει ηχητικά σχόλια κατά τη σάρωση ενός αποτυπώματος αναπαράγοντας διαφορετικούς ήχους για συγκεκριμένα συμβάντα προγράμματος. Μπορείτε να εκχωρήσετε νέους ήχους σε αυτά τα συμβάντα από την καρτέλα "Ήχοι" στον Πίνακα Ελέγχου των Windows ή να απενεργοποιήσετε τα ηχητικά σχόλια καταργώντας αυτή την επιλογή.
- **Εμφάνιση σχολίων ποιότητας σάρωσης** — Από προεπιλογή, όταν η ποιότητα της σάρωσης ενός αποτυπώματος είναι ανεπαρκής για τον έλεγχο ταυτότητας, το Security Manager εμφανίζει την εικόνα ενός αποτυπώματος με ένα ερωτηματικό. Μπορείτε να απενεργοποιήσετε την εμφάνιση αυτής της εικόνας καταργώντας αυτή την επιλογή.

Δημιουργία αντιγράφων ασφαλείας και επαναφορά δεδομένων

Συνιστάται να δημιουργείτε αντίγραφα ασφαλείας των δεδομένων του Security Manager σε τακτά χρονικά διαστήματα. Η συχνότητα δημιουργίας των αντιγράφων ασφαλείας εξαρτάται από τη συχνότητα αλλαγών στα δεδομένα. Για παράδειγμα, εάν προσθέτετε νέα ονόματα σύνδεσης σε καθημερινή βάση, τότε πιθανότατα πρέπει να δημιουργείτε αντίγραφα ασφαλείας των δεδομένων καθημερινά.

Τα αντίγραφα ασφαλείας μπορούν επίσης να χρησιμοποιηθούν για μετεγκατάσταση από έναν υπολογιστή σε άλλον, μια διαδικασία που ονομάζεται επίσης εισαγωγή και εξαγωγή.

ΣΗΜΕΙΩΣΗ Με τη λειτουργία αυτή δημιουργούνται αντίγραφα ασφαλείας μόνο για τα δεδομένα.

Για να μπορέσετε να επαναφέρετε τα δεδομένα από το αρχείο του αντιγράφου ασφαλείας, θα πρέπει να έχετε εγκαταστήσει το HP ProtectTools Security Manager στον υπολογιστή όπου θα ληφθούν τα δεδομένα.

Για να δημιουργήσετε αντίγραφο ασφαλείας των δεδομένων σας:

1. Στο αριστερό τμήμα παραθύρου, επιλέξτε **Για προχωρημένους** και έπειτα **Δημιουργία αντιγράφων ασφαλείας και επαναφορά**.
2. Επιλέξτε **Αντίγραφο ασφαλείας δεδομένων**.
3. Επιλέξτε τις ενότητες που θέλετε να συμπεριλάβετε στο αντίγραφο ασφαλείας. Στις περισσότερες περιπτώσεις θα θέλετε να τις επιλέξετε όλες.
4. Πληκτρολογήστε όνομα για το αρχείο αποθήκευσης. Από προεπιλογή, το αρχείο θα αποθηκευτεί στο φάκελο "Έγγραφα". Κάντε κλικ στο κουμπί **Αναζήτηση** για να καθορίσετε άλλη τοποθεσία.
5. Πληκτρολογήστε ένα κωδικό πρόσβασης για την προστασία του αρχείου.
6. Επαληθεύστε την ταυτότητά σας.
7. Κάντε κλικ στο κουμπί **Τέλος**.

Για να επαναφέρετε τα δεδομένα σας:

1. Στο αριστερό τμήμα παραθύρου, επιλέξτε **Για προχωρημένους** και έπειτα **Δημιουργία αντιγράφων ασφαλείας και επαναφορά**.
2. Επιλέξτε **Επαναφορά δεδομένων**.
3. Επιλέξτε το αρχείο αποθήκευσης που έχει δημιουργηθεί. Μπορείτε να πληκτρολογήσετε τη διαδρομή στο παρεχόμενο πεδίο ή να κάνετε κλικ στο κουμπί **Επεξεργασία**.
4. Πληκτρολογήστε τον κωδικό πρόσβασης που χρησιμοποιείται για την προστασία του αρχείου.
5. Επιλέξτε τις ενότητες τα δεδομένα των οποίων θέλετε να επαναφέρετε. Στις περισσότερες περιπτώσεις πρόκειται για όλες τις αναφερόμενες ενότητες.
6. Κάντε κλικ στο κουμπί **Τέλος**.

Προσθήκη εφαρμογών

Μπορεί να υπάρχουν κι άλλες εφαρμογές που παρέχουν νέες λειτουργίες για αυτό το πρόγραμμα.

Κάντε κλικ στη σύνδεση **[+] Ανακάλυψη περισσότερων** του Security Manager για να αναζητήσετε περισσότερες εφαρμογές.

ΣΗΜΕΙΩΣΗ Εάν δεν υπάρχει σύνδεση **[+] Ανακάλυψη περισσότερων** στο κάτω αριστερό τμήμα του πίνακα εργαλείων, θα έχει απενεργοποιηθεί από το διαχειριστή του υπολογιστή.

Κατάσταση εφαρμογών ασφαλείας

Η σελίδα "Κατάσταση εφαρμογών" του Security Manager εμφανίζει τη γενική κατάσταση των εγκατεστημένων εφαρμογών ασφαλείας. Εμφανίζει τις εφαρμογές που έχουν εγκατασταθεί και την κατάσταση ρύθμισης της καθεμίας. Η σύνοψη εμφανίζεται αυτόματα όταν ανοίγετε τον πίνακα εργαλείων του Security Manager ή όταν επιλέγετε **Εφαρμογές ασφαλείας**.

7 Drive Encryption for HP ProtectTools (μόνο σε επιλεγμένα μοντέλα)

△ **ΠΡΟΣΟΧΗ** Αν θέλετε να εγκαταστήσετε το στοιχείο Drive Encryption, πρέπει πρώτα να αποκρυπτογραφήσετε όλους τους κρυπτογραφημένους σκληρούς δίσκους. Αν δεν το κάνετε, δεν θα μπορείτε να έχετε πρόσβαση στα δεδομένα που υπάρχουν στους κρυπτογραφημένους σκληρούς δίσκους, εκτός αν έχετε εγγραφεί στην υπηρεσία επαναφοράς του Drive Encryption. Η επανεγκατάσταση του στοιχείου Drive Encryption δεν θα σας δώσει τη δυνατότητα να έχετε πρόσβαση στους κρυπτογραφημένους σκληρούς δίσκους.

Το Drive Encryption for HP ProtectTools προσφέρει ολοκληρωμένη προστασία δεδομένων κρυπτογραφώντας το σκληρό δίσκο του υπολογιστή. Όταν έχει ενεργοποιηθεί το Drive Encryption, πρέπει να συνδεθείτε στην οθόνη σύνδεσης του Drive Encryption που εμφανίζεται πριν από την εκκίνηση του λειτουργικού συστήματος των Windows®.

Ο οδηγός ρύθμισης του HP ProtectTools παρέχει στους διαχειριστές των Windows τη δυνατότητα ενεργοποίησης του Drive Encryption, δημιουργίας αντιγράφου ασφαλείας του κλειδιού κρυπτογράφησης, προσθήκης και αφαίρεσης χρηστών και απενεργοποίησης του Drive Encryption. Για περισσότερες πληροφορίες, ανατρέξτε στη Βοήθεια του λογισμικού HP ProtectTools Security Manager.

Με το Drive Encryption μπορείτε να πραγματοποιήσετε τις παρακάτω εργασίες:

- Διαχείριση κρυπτογράφησης
  - Κρυπτογράφηση ή αποκρυπτογράφηση μεμονωμένων μονάδων

    ΣΗΜΕΙΩΣΗ Μόνο οι εσωτερικοί σκληροί δίσκοι μπορούν να κρυπτογραφηθούν.
- Επαναφορά
  - Δημιουργία αντιγράφων ασφαλείας των κλειδιών
  - Πραγματοποίηση επαναφοράς

Διαδικασίες εγκατάστασης

Άνοιγμα του Drive Encryption

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Administrative Console**.
2. Στο αριστερό τμήμα παραθύρου, επιλέξτε **Drive Encryption**.

Γενικές εργασίες

Ενεργοποίηση του Drive Encryption

Χρησιμοποιήστε τον οδηγό ρύθμισης του HP ProtectTools για να ενεργοποιήσετε το Drive Encryption.

ΣΗΜΕΙΩΣΗ Ο οδηγός αυτός χρησιμοποιείται επίσης για την προσθήκη και αφαίρεση χρηστών.

– ή –

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Administrative Console**.
2. Στο αριστερό τμήμα παραθύρου, επιλέξτε **Security** (Ασφάλεια) και έπειτα **Features** (Λειτουργίες).
3. Επιλέξτε το πλαίσιο ελέγχου **Drive Encryption** (Κρυπτογράφηση μονάδων) και, στη συνέχεια, κάντε κλικ στο κουμπί **Next** (Επόμενο).
4. Στην ενότητα **Drives to be encrypted** (Μονάδες προς κρυπτογράφηση), επιλέξτε το πλαίσιο ελέγχου για το σκληρό δίσκο που θέλετε να κρυπτογραφήσετε.
5. Τοποθετήστε τη συσκευή αποθήκευσης στην κατάλληλη υποδοχή.

   ΣΗΜΕΙΩΣΗ Για να αποθηκεύσετε το κλειδί κρυπτογράφησης, πρέπει να χρησιμοποιήσετε μια συσκευή αποθήκευσης USB με μορφή FAT32.
6. Στην ενότητα **External storage device on which to save encryption key** (Εξωτερική συσκευή αποθήκευσης για αποθήκευση του κλειδιού κρυπτογράφησης), επιλέξτε το πλαίσιο ελέγχου για τη συσκευή αποθήκευσης όπου θα αποθηκευτεί το κλειδί κρυπτογράφησης.
7. Κάντε κλικ στο κουμπί **Apply** (Εφαρμογή).

   Ξεκινά η κρυπτογράφηση της μονάδας δίσκου.

Για περισσότερες πληροφορίες, ανατρέξτε στη Βοήθεια του λογισμικού HP ProtectTools Security Manager.

Απενεργοποίηση του Drive Encryption

Χρησιμοποιήστε τον οδηγό ρύθμισης του HP ProtectTools για να απενεργοποιήσετε το Drive Encryption. Για περισσότερες πληροφορίες, ανατρέξτε στη Βοήθεια του λογισμικού HP ProtectTools Security Manager.

– ή –

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Administrative Console**.
2. Στο αριστερό τμήμα παραθύρου, επιλέξτε **Security** (Ασφάλεια) και έπειτα **Features** (Λειτουργίες).
3. Αποεπιλέξτε το πλαίσιο ελέγχου **Drive Encryption** (Κρυπτογράφηση μονάδων) και, στη συνέχεια, κάντε κλικ στο κουμπί **Apply** (Εφαρμογή).

   Ξεκινά η αποκρυπτογράφηση της μονάδας δίσκου.

Σύνδεση μετά την ενεργοποίηση του Drive Encryption

Όταν ενεργοποιείτε τον υπολογιστή μετά την ενεργοποίηση του Drive Encryption και την καταχώριση του λογαριασμού χρήστη, πρέπει να συνδεθείτε στην οθόνη σύνδεσης του Drive Encryption:

ΣΗΜΕΙΩΣΗ Εάν ο διαχειριστής των Windows έχει ενεργοποιήσει την ασφάλεια πριν από την εκκίνηση στο HP ProtectTools Security Manager, θα συνδεθείτε στον υπολογιστή αμέσως μετά την ενεργοποίησή του, χωρίς να χρειαστεί να συνδεθείτε στην οθόνη σύνδεσης του Drive Encryption.

1. Κάντε κλικ στο όνομα χρήστη και πληκτρολογήστε τον κωδικό πρόσβασης των Windows ή το PIN της κάρτας Java™ ή σαρώστε ένα δάχτυλο που έχετε καταχωρίσει.
2. Κάντε κλικ στο **OK**.

ΣΗΜΕΙΩΣΗ Εάν χρησιμοποιείτε κλειδί ανάκτησης για να συνδεθείτε στην οθόνη σύνδεσης του Drive Encryption, θα σας ζητηθεί επίσης να επιλέξετε το όνομα χρήστη των Windows και να πληκτρολογήσετε τον κωδικό πρόσβασης στην οθόνη σύνδεσης των Windows.

Προστασία δεδομένων με κρυπτογράφηση του σκληρού δίσκου

Χρησιμοποιήστε τον οδηγό ρύθμισης του HP ProtectTools για να προστατέψετε τα δεδομένα σας κρυπτογραφώντας το σκληρό σας δίσκο:

1. Στο Security Manager, επιλέξτε **Getting Started** (Έναρξη χρήσης) και έπειτα κάντε κλικ στο εικονίδιο **Security Manager Setup** (Ρύθμιση του Security Manager). Ξεκινά μια παρουσίαση που περιγράφει τις λειτουργίες του Security Manager. [Μπορείτε επίσης να ανοίξετε το Security Manager από τη σελίδα Drive Encryption (Κρυπτογράφηση μονάδων).]
2. Στο αριστερό τμήμα παραθύρου, επιλέξτε **Drive Encryption** (Κρυπτογράφηση μονάδων) και έπειτα **Encryption Management** (Διαχείριση κρυπτογράφησης).
3. Επιλέξτε **Change Encryption** (Αλλαγή κρυπτογράφησης).
4. Επιλέξτε τη μονάδα ή τις μονάδες δίσκου που θα κρυπτογραφηθούν.

ΣΗΜΕΙΩΣΗ Συνιστάται ανεπιφύλακτα να κρυπτογραφήσετε το σκληρό δίσκο.

Εμφάνιση κατάστασης κρυπτογράφησης

Οι χρήστες μπορούν να εμφανίσουν την κατάσταση κρυπτογράφησης από το HP ProtectTools Security Manager.

ΣΗΜΕΙΩΣΗ Οι αλλαγές στην κατάσταση κρυπτογράφησης των μονάδων πρέπει να γίνονται με το HP ProtectTools Administrative Console.

1. Ανοίξτε το **HP ProtectTools Security Manager**.
2. Στη ενότητα **Τα δεδομένα μου**, επιλέξτε **Κατάσταση κρυπτογράφησης**.

   Εάν είναι ενεργή η λειτουργία Drive Encryption, η κατάσταση μονάδας εμφανίζει έναν από τους παρακάτω κωδικούς κατάστασης:

   - Active (Ενεργή)
   - Inactive (Ανενεργή)
   - Not encrypted (Μη κρυπτογραφημένη)

- Encrypted (Κρυπτογραφημένη)
- Encrypting (Γίνεται κρυπτογράφηση)
- Decrypting (Γίνεται αποκρυπτογράφηση)

Εάν ο σκληρός δίσκος είναι σε διαδικασία κρυπτογράφησης ή αποκρυπτογράφησης, μια γραμμή προόδου εμφανίζει το ποσοστό ολοκλήρωσης και το χρόνο που απομένει για την ολοκλήρωση της κρυπτογράφησης ή αποκρυπτογράφησης.

Εργασίες για προχωρημένους

Διαχείριση του Drive Encryption (εργασία διαχειριστή)

Η σελίδα Encryption Management (Διαχείριση κρυπτογράφησης) δίνει στους διαχειριστές τη δυνατότητα να προβάλλουν και να αλλάζουν την κατάσταση του Drive Encryption (ενεργό ή ανενεργό) και να προβάλλουν την κατάσταση κρυπτογράφησης όλων των σκληρών δίσκων του υπολογιστή.

- Εάν η κατάσταση είναι Inactive (Ανενεργό), ο διαχειριστής των Windows δεν έχει ενεργοποιήσει ακόμα το Drive Encryption στο HP ProtectTools Security Manager και ο σκληρός δίσκος δεν προστατεύεται. Χρησιμοποιήστε τον οδηγό ρύθμισης του HP ProtectTools Security Manager για να ενεργοποιήσετε το Drive Encryption.
- Εάν η κατάσταση είναι Active (Ενεργό), το Drive Encryption έχει ενεργοποιηθεί και διαμορφωθεί. Η μονάδα δίσκου βρίσκεται σε μία από τις παρακάτω καταστάσεις:
  - Not encrypted (Μη κρυπτογραφημένη)
  - Encrypted (Κρυπτογραφημένη)
  - Encrypting (Γίνεται κρυπτογράφηση)
  - Decrypting (Γίνεται αποκρυπτογράφηση)

Κρυπτογράφηση ή αποκρυπτογράφηση μεμονωμένων μονάδων

Για να κρυπτογραφήσετε έναν ή περισσότερους σκληρούς δίσκους στον υπολογιστή ή να αποκρυπτογραφήσετε μια μονάδα δίσκου που είναι ήδη κρυπτογραφημένη, χρησιμοποιήστε τη λειτουργία Change Encryption (Αλλαγή κρυπτογράφησης):

1. Ανοίξτε το **HP ProtectTools Administrative Console**, επιλέξτε **Drive Encryption** (Κρυπτογράφηση μονάδων) και έπειτα επιλέξτε **Encryption Management** (Διαχείριση κρυπτογράφησης).
2. Επιλέξτε **Change Encryption** (Αλλαγή κρυπτογράφησης).
3. Στο πλαίσιο διαλόγου Change Encryption (Αλλαγή κρυπτογράφησης), επιλέξτε ή αποεπιλέξτε το πλαίσιο ελέγχου για κάθε σκληρό δίσκο που θέλετε να κρυπτογραφήσετε ή να αποκρυπτογραφήσετε και κάντε κλικ στο **OK**.

ΣΗΜΕΙΩΣΗ Όταν γίνεται κρυπτογράφηση ή αποκρυπτογράφηση της μονάδας, η γραμμή προόδου δείχνει το χρόνο που απομένει για την ολοκλήρωση της διαδικασίας κατά την τρέχουσα περίοδο λειτουργίας. Εάν τερματιστεί η λειτουργία του υπολογιστή ή εκκινηθεί η αναστολή λειτουργίας ή η αδρανοποίηση κατά τη διαδικασία κρυπτογράφησης και έπειτα επανεκκινηθεί ο υπολογιστής, η ένδειξη Time Remaining (Χρόνος που απομένει) επανέρχεται στην αρχή, αλλά η κρυπτογράφηση συνεχίζεται από το σημείο που είχε σταματήσει. Ο χρόνος που απομένει και η ένδειξη προόδου θα αλλάξουν πιο γρήγορα προκειμένου να εμφανίσουν την προηγούμενη πρόοδο.

Δημιουργία αντιγράφων ασφαλείας και επαναφορά (εργασία διαχειριστή)

Η σελίδα Recovery (Επαναφορά) δίνει στους διαχειριστές τη δυνατότητα να δημιουργούν αντίγραφα ασφαλείας και να επαναφέρουν τα κλειδιά κρυπτογράφησης.

Local Drive Encryption Key Backup (Αντίγραφο ασφαλείας κλειδιού κρυπτογράφησης τοπικής μονάδας) — Σας δίνει τη δυνατότητα να δημιουργήσετε αντίγραφα ασφαλείας των κλειδιών κρυπτογράφησης σε αφαιρούμενα μέσα, όταν είναι ενεργοποιημένη η λειτουργία Drive Encryption.

Δημιουργία αντιγράφων ασφαλείας κλειδιών

Μπορείτε να δημιουργήσετε αντίγραφο ασφαλείας του κλειδιού κρυπτογράφησης για μια κρυπτογραφημένη μονάδα σε μια αφαιρούμενη συσκευή αποθήκευσης:

△ **ΠΡΟΣΟΧΗ** Φροντίστε να φυλάξετε τη συσκευή αποθήκευσης που περιέχει το αντίγραφο ασφαλείας του κλειδιού σε ασφαλές μέρος, καθώς εάν ξεχάσετε τον κωδικό πρόσβασής σας ή χάσετε την κάρτα Java, η συσκευή αυτή θα είναι η μόνη σας πρόσβαση στο σκληρό σας δίσκο.

1. Ανοίξτε το **HP ProtectTools Administrative Console**, επιλέξτε **Drive Encryption** (Κρυπτογράφηση μονάδων) και έπειτα επιλέξτε **Recovery** (Επαναφορά).
2. Επιλέξτε **Backup Keys** (Αντίγραφα ασφαλείας κλειδιών).
3. Στη σελίδα Select Backup Disk (Επιλογή δίσκου αντιγράφου ασφαλείας), επιλέξτε το πλαίσιο ελέγχου για τη συσκευή όπου θέλετε να δημιουργηθεί το αντίγραφο ασφαλείας του κλειδιού κρυπτογράφησης και, στη συνέχεια, κάντε κλικ στο κουμπί **Next** (Επόμενο).
4. Διαβάστε τις πληροφορίες στην επόμενη σελίδα που εμφανίζεται και κάντε κλικ στο κουμπί **Next** (Επόμενο). Το κλειδί κρυπτογράφησης αποθηκεύεται στη συσκευή αποθήκευσης που έχετε επιλέξει.
5. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο κουμπί **Finish** (Τέλος).

Πραγματοποίηση επαναφοράς

Για να πραγματοποιήσετε επαναφορά σε περίπτωση που έχετε ξεχάσει τον κωδικό πρόσβασής σας, ακολουθήστε τα παρακάτω βήματα:

1. Ενεργοποιήστε τον υπολογιστή.
2. Τοποθετήστε την αφαιρούμενη συσκευή αποθήκευσης που περιέχει το αντίγραφο ασφαλείας του κλειδιού.
3. Όταν ανοίξει το πλαίσιο διαλόγου σύνδεσης στο Drive Encryption for HP ProtectTools, κάντε κλικ στο κουμπί **Cancel** (Άκυρο).
4. Επιλέξτε **Options** (Επιλογές) στην κάτω αριστερή γωνία της οθόνης και έπειτα επιλέξτε **Recovery** (Επαναφορά).
5. Επιλέξτε το αρχείο που περιέχει το αντίγραφο ασφαλείας του κλειδιού ή κάντε κλικ στο κουμπί **Browse** (Αναζήτηση) για να το αναζητήσετε και έπειτα κάντε κλικ στο κουμπί **Next** (Επόμενο).
6. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **OK**.

   Γίνεται εκκίνηση του υπολογιστή.

ΣΗΜΕΙΩΣΗ Συνιστάται ανεπιφύλακτα να αλλάξετε τον κωδικό πρόσβασης μετά την πραγματοποίηση επαναφοράς.

8 Privacy Manager for HP ProtectTools (μόνο σε επιλεγμένα μοντέλα)

Το Privacy Manager for HP ProtectTools σάς δίνει τη δυνατότητα να χρησιμοποιείτε μεθόδους σύνδεσης προηγμένης ασφάλειας (έλεγχος ταυτότητας) για την επαλήθευση της προέλευσης, ακεραιότητας και ασφάλειας της επικοινωνίας κατά τη χρήση e-mail, εγγράφων του Microsoft® Office ή άμεσων μηνυμάτων.

Το Privacy Manager επωφελείται από την υποδομή ασφαλείας που παρέχει το HP ProtectTools Security Manager, η οποία περιλαμβάνει τις παρακάτω μεθόδους ασφαλούς σύνδεσης:

- Έλεγχος ταυτότητας με αποτύπωμα
- Κωδικός πρόσβασης των Windows®
- Κάρτα Java™ του HP ProtectTools

Μπορείτε να χρησιμοποιήσετε οποιαδήποτε από τις παραπάνω μεθόδους ασφαλούς σύνδεσης στο Privacy Manager.

Το Privacy Manager απαιτεί τα εξής:

- HP ProtectTools Security Manager 5.00 ή νεότερη έκδοση
- Λειτουργικό σύστημα Windows® 7, Windows Vista® ή Windows XP
- Microsoft Outlook 2007 ή Microsoft Outlook 2003
- Έγκυρος λογαριασμός e-mail

ΣΗΜΕΙΩΣΗ Για να μπορείτε να έχετε πρόσβαση στις λειτουργίες ασφαλείας, πρέπει να ζητήσετε και να εγκαταστήσετε ένα πιστοποιητικό του Privacy Manager (ψηφιακό πιστοποιητικό) μέσα από το Privacy Manager. Για πληροφορίες σχετικά με το αίτημα πιστοποιητικού του Privacy Manager, δείτε την ενότητα Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 45.

Διαδικασίες εγκατάστασης

Άνοιγμα του Privacy Manager

Για να ανοίξετε το Privacy Manager:

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Security Manager**.
2. Επιλέξτε **Privacy Manager**.

– ή –

Κάντε δεξί κλικ στο εικονίδιο του **HP ProtectTools** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών, επιλέξτε **Privacy Manager** και έπειτα επιλέξτε **Configuration** (Διαμόρφωση).

– ή –

Στη γραμμή εργαλείων ενός μηνύματος e-mail του Microsoft Outlook, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) και έπειτα επιλέξτε **Certificates** (Πιστοποιητικά) ή **Trusted Contacts** (Αξιόπιστες επαφές).

– ή –

Στη γραμμή εργαλείων ενός εγγράφου του Microsoft Office, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και έπειτα επιλέξτε **Certificates** (Πιστοποιητικά) ή **Trusted Contacts** (Αξιόπιστες επαφές).

Διαχείριση πιστοποιητικών του Privacy Manager

Τα πιστοποιητικά του Privacy Manager προστατεύουν τα δεδομένα και τα μηνύματα χρησιμοποιώντας μια κρυπτογραφική τεχνολογία που ονομάζεται υποδομή δημοσίου κλειδιού (PKI). Το PKI απαιτεί από τους χρήστες να αποκτήσουν κρυπτογραφικά κλειδιά και ένα πιστοποιητικό του Privacy Manager που εκδίδεται από αρχή έκδοσης πιστοποιητικών (CA). Σε αντίθεση με τα περισσότερα προγράμματα λογισμικού κρυπτογράφησης και ελέγχου ταυτότητας που απαιτούν τον έλεγχο ταυτότητας μόνο κατά διαστήματα, το Privacy Manager απαιτεί τον έλεγχο ταυτότητας κάθε φορά που υπογράφετε ένα μήνυμα e-mail ή ένα έγγραφο του Microsoft Office χρησιμοποιώντας κρυπτογραφικό κλειδί. Το Privacy Manager καθιστά ασφαλή τη διαδικασία αποθήκευσης και αποστολής σημαντικών πληροφοριών.

Μπορείτε να πραγματοποιήσετε τις παρακάτω εργασίες:

- Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager
- Προβολή λεπτομερειών πιστοποιητικού του Privacy Manager
- Ανανέωση πιστοποιητικών του Privacy Manager
- Ορισμός προεπιλεγμένου πιστοποιητικού του Privacy Manager που θα χρησιμοποιεί το Privacy Manager όταν υπάρχουν πολλά διαθέσιμα πιστοποιητικά
- Διαγραφή και ανάκληση πιστοποιητικού του Privacy Manager (για προχωρημένους)

Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager

Για να μπορέσετε να χρησιμοποιήσετε τις λειτουργίες του Privacy Manager, πρέπει να ζητήσετε και να εγκαταστήσετε ένα πιστοποιητικό του Privacy Manager (μέσα από το Privacy Manager) χρησιμοποιώντας μια έγκυρη διεύθυνση e-mail. Η διεύθυνση e-mail πρέπει να έχει δημιουργηθεί ως

λογαριασμός του Microsoft Outlook στον ίδιο υπολογιστή από τον οποίο ζητάτε το πιστοποιητικό του Privacy Manager.

Αίτημα για πιστοποιητικό του Privacy Manager

1. Ανοίξτε το Privacy Manager και επιλέξτε **Certificates** (Πιστοποιητικά).
2. Επιλέξτε **Request a Privacy Manager certificate** (Αίτημα για πιστοποιητικό του Privacy Manager).
3. Στη σελίδα Welcome (Καλωσορίσατε), διαβάστε το κείμενο και έπειτα κάντε κλικ στο κουμπί **Next** (Επόμενο).
4. Στη σελίδα License Agreement (Άδεια χρήσης), διαβάστε την άδεια χρήσης.
5. Βεβαιωθείτε ότι έχετε επιλέξει το πλαίσιο ελέγχου δίπλα στην επιλογή **Check here to accept the terms of this license agreement** (Κάντε κλικ εδώ για να αποδεχτείτε τους όρους της άδειας χρήσης) και έπειτα κάντε κλικ στο κουμπί **Next** (Επόμενο).
6. Στη σελίδα Your Certificate Details (Λεπτομέρειες πιστοποιητικού), πληκτρολογήστε τις απαραίτητες πληροφορίες και έπειτα κάντε κλικ στο κουμπί **Next** (Επόμενο).
7. Στη σελίδα Certificate Request Accepted (Αποδοχή αιτήματος για πιστοποιητικό), κάντε κλικ στο κουμπί **Finish** (Τέλος).
8. Κάντε κλικ το **OK** για να κλείσετε το πιστοποιητικό.

Θα λάβετε ένα e-mail στο Microsoft Outlook με συνημμένο το πιστοποιητικό του Privacy Manager.

Απόκτηση προεκχωρημένου εταιρικού πιστοποιητικού του Privacy Manager

1. Στο Outlook, ανοίξτε το e-mail που λάβατε και το οποίο υποδεικνύει ότι σας έχει προεκχωρηθεί ένα εταιρικό πιστοποιητικό.
2. Επιλέξτε **Obtain** (Λήψη).
3. Θα λάβετε ένα e-mail στο Microsoft Outlook με συνημμένο το πιστοποιητικό του Privacy Manager.
4. Για να εγκαταστήσετε το πιστοποιητικό, δείτε την ενότητα Εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 46

Εγκατάσταση πιστοποιητικού του Privacy Manager

1. Όταν λάβετε το e-mail με το συνημμένο πιστοποιητικό του Privacy Manager, ανοίξτε το e-mail και κάντε κλικ στο κουμπί **Setup** (Εγκατάσταση) στην κάτω δεξιά γωνία του μηνύματος στο Outlook 2007 ή στην πάνω αριστερή γωνία στο Outlook 2003.
2. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.
3. Στη σελίδα Certificate Installed (Εγκατάσταση πιστοποιητικού), κάντε κλικ στο κουμπί **Next** (Επόμενο).
4. Στη σελίδα Certificate Backup (Αντίγραφο ασφαλείας πιστοποιητικού), πληκτρολογήστε μια τοποθεσία και ένα όνομα για το αρχείο αντιγράφου ασφαλείας ή κάντε κλικ στο κουμπί **Browse** (Αναζήτηση) για να αναζητήσετε μια τοποθεσία.

△ **ΠΡΟΣΟΧΗ** Φροντίστε να αποθηκεύσετε το αρχείο σε άλλη τοποθεσία εκτός του σκληρού δίσκου και να το φυλάξετε σε ασφαλές μέρος. Το αρχείο αυτό πρέπει να είναι αποκλειστικά για δική σας χρήση και θα σας είναι απαραίτητο εάν χρειαστεί να επαναφέρετε το πιστοποιητικό του Privacy Manager και τα σχετικά κλειδιά.

5. Πληκτρολογήστε και επιβεβαιώστε ένα κωδικό πρόσβασης και κάντε κλικ στο κουμπί **Next** (Επόμενο).

6. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

7. Εάν επιλέξετε να ξεκινήσετε τη διαδικασία πρόσκλησης αξιόπιστης επαφής, ακολουθήστε τις οδηγίες στην οθόνη ξεκινώντας με το βήμα 2 του θέματος Προσθήκη αξιόπιστων επαφών με χρήση των επαφών του Microsoft Outlook στη σελίδα 51.

   – ή –

   Εάν κάνετε κλικ στο κουμπί **Cancel** (Άκυρο), ανατρέξτε στις πληροφορίες της ενότητας Προσθήκη αξιόπιστης επαφής στη σελίδα 50 για την προσθήκη αξιόπιστης επαφής αργότερα.

Προβολή λεπτομερειών πιστοποιητικού του Privacy Manager

1. Ανοίξτε το Privacy Manager και επιλέξτε **Certificates** (Πιστοποιητικά).

2. Κάντε κλικ σε ένα πιστοποιητικό του Privacy Manager.

3. Επιλέξτε **Certificate details** (Λεπτομέρειες πιστοποιητικού).

4. Όταν ολοκληρώσετε την προβολή των λεπτομερειών, κάντε κλικ στο **OK**.

Ανανέωση πιστοποιητικού του Privacy Manager

Όταν πλησιάζει η λήξη του πιστοποιητικού του Privacy Manager, θα ειδοποιηθείτε ότι πρέπει να το ανανεώσετε:

1. Ανοίξτε το Privacy Manager και επιλέξτε **Certificates** (Πιστοποιητικά).

2. Επιλέξτε **Renew certificate** (Ανανέωση πιστοποιητικού).

3. Ακολουθήστε τις οδηγίες στην οθόνη για να αγοράσετε νέο πιστοποιητικό του Privacy Manager.

ΣΗΜΕΙΩΣΗ Η διαδικασία ανανέωσης πιστοποιητικών του Privacy Manager δεν αντικαθιστά το παλιό σας πιστοποιητικό του Privacy Manager. Θα πρέπει να αγοράσετε ένα νέο πιστοποιητικό του Privacy Manager και να το εγκαταστήσετε χρησιμοποιώντας τις ίδιες διαδικασίες που αναφέρονται στην ενότητα Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 45.

Ορισμός προεπιλεγμένου πιστοποιητικού του Privacy Manager

Από το Privacy Manager μπορείτε να δείτε μόνο πιστοποιητικά του Privacy Manager, ακόμα και εάν έχετε εγκαταστήσει στον υπολογιστή σας κι άλλα πιστοποιητικά από άλλες αρχές έκδοσης.

Εάν έχετε περισσότερα από ένα πιστοποιητικά του Privacy Manager στον υπολογιστή σας, τα οποία έχουν εγκατασταθεί μέσα από το Privacy Manager, μπορείτε να προσδιορίσετε ένα από αυτά ως προεπιλεγμένο πιστοποιητικό:

1. Ανοίξτε το Privacy Manager και επιλέξτε **Certificates** (Πιστοποιητικά).
2. Κάντε κλικ στο πιστοποιητικό του Privacy Manager που θέλετε να χρησιμοποιήσετε ως προεπιλεγμένο και έπειτα επιλέξτε **Set default** (Ορισμός προεπιλογής).
3. Κάντε κλικ στο **OK**.

ΣΗΜΕΙΩΣΗ Δεν είναι απαραίτητο να χρησιμοποιείτε το προεπιλεγμένο πιστοποιητικό του Privacy Manager. Μπορείτε να επιλέξετε οποιοδήποτε από τα πιστοποιητικά σας Privacy Manager για χρήση μέσα από τις διάφορες λειτουργίες του Privacy Manager.

Διαγραφή πιστοποιητικού του Privacy Manager

Εάν διαγράψετε ένα πιστοποιητικό του Privacy Manager, δεν θα μπορείτε να ανοίξετε τα αρχεία ή να προβάλλετε τα δεδομένα που έχετε κρυπτογραφήσει με αυτό το πιστοποιητικό. Εάν διαγράψετε κατά λάθος ένα πιστοποιητικό του Privacy Manager, μπορείτε να το επαναφέρετε χρησιμοποιώντας το αρχείο αντιγράφου ασφαλείας που δημιουργήσατε κατά την εγκατάσταση του πιστοποιητικού. Για περισσότερες πληροφορίες, δείτε την ενότητα Επαναφορά πιστοποιητικού του Privacy Manager στη σελίδα 48.

Για να διαγράψετε ένα πιστοποιητικό του Privacy Manager:

1. Ανοίξτε το Privacy Manager και επιλέξτε **Certificates** (Πιστοποιητικά).
2. Κάντε κλικ στο πιστοποιητικό του Privacy Manager που θέλετε να διαγράψετε και επιλέξτε **Advanced** (Για προχωρημένους).
3. Κάντε κλικ στο κουμπί **Delete** (Διαγραφή).
4. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).
5. Κάντε κλικ στο κουμπί **Close** (Κλείσιμο) και έπειτα στο κουμπί **Apply** (Εφαρμογή).

Επαναφορά πιστοποιητικού του Privacy Manager

Κατά την εγκατάσταση του πιστοποιητικού του Privacy Manager σας ζητείται να δημιουργήσετε ένα αντίγραφο ασφαλείας του πιστοποιητικού. Μπορείτε επίσης να δημιουργήσετε αντίγραφο ασφαλείας από τη σελίδα Migration (Μετεγκατάσταση). Αυτό το αντίγραφο ασφαλείας μπορεί να χρησιμοποιηθεί κατά τη μετεγκατάσταση από έναν υπολογιστή σε άλλον ή για την επαναφορά ενός πιστοποιητικού στον ίδιο υπολογιστή.

1. Ανοίξτε το Privacy Manager και επιλέξτε **Migration** (Μετεγκατάσταση).
2. Επιλέξτε **Restore** (Επαναφορά).
3. Στη σελίδα Migration File (Αρχείο μετεγκατάστασης), κάντε κλικ στο κουμπί **Browse** (Αναζήτηση) για να αναζητήσετε το αρχείο .dppsm που δημιουργήσατε κατά τη δημιουργία του αντιγράφου ασφαλείας και έπειτα κάντε κλικ στο κουμπί **Next** (Επόμενο).
4. Πληκτρολογήστε τον κωδικό πρόσβασης που χρησιμοποιήσατε κατά τη δημιουργία του αντιγράφου ασφαλείας και κάντε κλικ στο κουμπί **Next** (Επόμενο).

5. Κάντε κλικ στο κουμπί **Finish** (Τέλος).

6. Κάντε κλικ στο **OK**.

Για περισσότερες πληροφορίες, δείτε την ενότητα Εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 46 ή Δημιουργία αντιγράφων ασφαλείας των πιστοποιητικών του Privacy Manager και των αξιόπιστων επαφών στη σελίδα 66.

Ανάκληση πιστοποιητικού του Privacy Manager

Εάν πιστεύετε ότι το πιστοποιητικό του Privacy Manager δεν είναι ασφαλές, μπορείτε να το ανακαλέσετε:

ΣΗΜΕΙΩΣΗ Όταν ανακαλείτε ένα πιστοποιητικό του Privacy Manager, αυτό δεν διαγράφεται. Εξακολουθείτε να μπορείτε να χρησιμοποιήσετε το πιστοποιητικό για την προβολή κρυπτογραφημένων αρχείων.

1. Ανοίξτε το Privacy Manager και επιλέξτε **Certificates** (Πιστοποιητικά).

2. Επιλέξτε **Advanced** (Για προχωρημένους).

3. Κάντε κλικ στο πιστοποιητικό του Privacy Manager που θέλετε να ανακαλέσετε και επιλέξτε **Revoke** (Ανάκληση).

4. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

5. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

6. Ακολουθήστε τις οδηγίες που εμφανίζονται στην οθόνη.

Διαχείριση αξιόπιστων επαφών

Οι αξιόπιστες επαφές είναι χρήστες με τους οποίους έχετε ανταλλάξει πιστοποιητικά του Privacy Manager, τα οποία σας επιτρέπουν να επικοινωνείτε με ασφάλεια μεταξύ σας.

Το πρόγραμμα Trusted Contacts Manager (Διαχείριση αξιόπιστων επαφών) σάς επιτρέπει να εκτελείτε τις ακόλουθες εργασίες:

- Προβολή λεπτομερειών αξιόπιστης επαφής
- Διαγραφή αξιόπιστων επαφών
- Έλεγχος κατάστασης ανάκλησης για τις αξιόπιστες επαφές (για προχωρημένους)

Προσθήκη αξιόπιστων επαφών

Η προσθήκη αξιόπιστων επαφών είναι μια διαδικασία με 3 βήματα:

1. Αποστείλετε μία πρόσκληση μέσω e-mail σε ένα παραλήπτη αξιόπιστης επαφής.

2. Ο παραλήπτης αξιόπιστης επαφής απαντά στο e-mail.

3. Λαμβάνετε την απάντηση e-mail από τον παραλήπτη αξιόπιστης επαφής και κάνετε κλικ στην επιλογή **Accept** (Αποδοχή).

Μπορείτε να στείλετε προσκλήσεις e-mail αξιόπιστης επαφής σε μεμονωμένους παραλήπτες ή μπορείτε να στείλετε την πρόσκληση σε όλες τις επαφές στο βιβλίο διευθύνσεων του Microsoft Outlook.

Ανατρέξτε στις παρακάτω ενότητες για την προσθήκη αξιόπιστων επαφών.

ΣΗΜΕΙΩΣΗ Για να απαντήσουν στην πρόσκλησή σας για να γίνουν αξιόπιστες επαφές, οι παραλήπτες αξιόπιστης επαφής πρέπει να έχουν εγκαταστήσει το πρόγραμμα Privacy Manager στον υπολογιστή τους ή ένα άλλο πρόγραμμα-πελάτη. Για πληροφορίες σχετικά με την εγκατάσταση ενός άλλου προγράμματος-πελάτη, επισκεφτείτε την τοποθεσία web της DigitalPersona στη διεύθυνση http://DigitalPersona.com/PrivacyManager.

Προσθήκη αξιόπιστης επαφής

1. Ανοίξτε το Privacy Manager, κάντε κλικ στην επιλογή **Trusted Contacts Manager** (Διαχείριση αξιόπιστων επαφών) και επιλέξτε **Invite Contacts** (Πρόσκληση επαφών).

   – ή –

   Στο Microsoft Outlook, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) στη γραμμή εργαλείων και επιλέξτε **Invite Contacts** (Πρόσκληση επαφών).

2. Εάν ανοίξει το παράθυρο διαλόγου Select Certificate (Επιλογή πιστοποιητικού), κάντε κλικ στο πιστοποιητικό Privacy Manager που επιθυμείτε να χρησιμοποιήσετε και κάντε κλικ στο **OK**.

3. Όταν ανοίξει το παράθυρο διαλόγου Trusted Contact Invitation (Πρόσκληση αξιόπιστης επαφής), διαβάστε το κείμενο και, στη συνέχεια, κάντε κλικ στο **OK**.

   Δημιουργείται αυτόματα ένα e-mail.

4. Πληκτρολογήστε μία ή περισσότερες διευθύνσεις e-mail των παραληπτών που επιθυμείτε να προσθέσετε ως αξιόπιστες επαφές.

5. Επεξεργαστείτε το κείμενο και υπογράψτε με το όνομά σας (προαιρετικό).

6. Κάντε κλικ στην επιλογή **Send** (Αποστολή).

   ΣΗΜΕΙΩΣΗ Εάν δεν έχετε αποκτήσει ένα πιστοποιητικό Privacy Manager, ένα μήνυμα σας ενημερώνει ότι πρέπει να διαθέτετε ένα πιστοποιητικό Privacy Manager για να μπορείτε να αποστείλετε μια αίτηση αξιόπιστης επαφής. Κάντε κλικ στο **OK** για εκκίνηση του Certificate Request Wizard (Οδηγός αίτησης πιστοποιητικού). Για περισσότερες πληροφορίες, δείτε την ενότητα Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 45.

7. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

   ΣΗΜΕΙΩΣΗ Όταν ο παραλήπτης αξιόπιστης επαφής λάβει το e-mail, πρέπει να ανοίξει το e-mail και να κάνει κλικ στην επιλογή **Accept** (Αποδοχή) στην κάτω δεξιά γωνία του e-mail και, στη συνέχεια, να επιλέξει **OK** όταν ανοίξει το παράθυρο διαλόγου επιβεβαίωσης.

8. Όταν λάβετε μια απάντηση e-mail από ένα παραλήπτη που αποδέχεται την πρόσκληση αξιόπιστης επαφής, κάντε κλικ στην επιλογή **Accept** (Αποδοχή) στην κάτω δεξιά γωνία του e-mail.

   Θα ανοίξει ένα παράθυρο διαλόγου, το οποίο θα επιβεβαιώνει ότι ο παραλήπτης έχει προστεθεί με επιτυχία στη λίστα αξιόπιστων επαφών.

9. Κάντε κλικ στο **OK**.

Προσθήκη αξιόπιστων επαφών με χρήση των επαφών του Microsoft Outlook

1. Ανοίξτε το Privacy Manager, κάντε κλικ στην επιλογή **Trusted Contacts Manager** (Διαχείριση αξιόπιστων επαφών) και επιλέξτε **Invite Contacts** (Πρόσκληση επαφών).

   – ή –

   Στο Microsoft Outlook, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) στη γραμμή εργαλείων και επιλέξτε **Invite All My Outlook Contacts** (Πρόσκληση όλων των επαφών του Outlook).

2. Όταν ανοίξει η σελίδα Trusted Contact Invitation (Πρόσκληση αξιόπιστης επαφής), επιλέξτε τις διευθύνσεις e-mail των παραληπτών που επιθυμείτε να προσθέσετε ως αξιόπιστες επαφές και κάντε κλικ στην επιλογή **Next** (Επόμενο).

3. Όταν ανοίξει η σελίδα “Sending Invitation” (Αποστολή πρόσκλησης), κάντε κλικ στην επιλογή **Finish** (Τέλος).

   Δημιουργείται αυτόματα ένα e-mail με τις επιλεγμένες διευθύνσεις e-mail του Microsoft Outlook.

4. Επεξεργαστείτε το κείμενο και υπογράψτε με το όνομά σας (προαιρετικό).

5. Κάντε κλικ στην επιλογή **Send**(Αποστολή).

ΣΗΜΕΙΩΣΗ Εάν δεν έχετε αποκτήσει ένα πιστοποιητικό Privacy Manager, ένα μήνυμα σας ενημερώνει ότι πρέπει να διαθέτετε ένα πιστοποιητικό Privacy Manager για να μπορείτε να αποστείλετε μια αίτηση αξιόπιστης επαφής. Κάντε κλικ στο **OK** για εκκίνηση του Certificate Request Wizard (Οδηγός αίτησης πιστοποιητικού). Για περισσότερες πληροφορίες, δείτε την ενότητα Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 45.

6. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

ΣΗΜΕΙΩΣΗ Όταν ο παραλήπτης αξιόπιστης επαφής λάβει το e-mail, πρέπει να ανοίξει το e-mail και να κάνει κλικ στην επιλογή **Accept** (Αποδοχή) στην κάτω δεξιά γωνία του e-mail και, στη συνέχεια, να επιλέξει **OK** όταν ανοίξει το παράθυρο διαλόγου επιβεβαίωσης.

7. Όταν λάβετε μια απάντηση e-mail από ένα παραλήπτη που αποδέχεται την πρόσκληση αξιόπιστης επαφής, κάντε κλικ στην επιλογή **Accept** (Αποδοχή) στην κάτω δεξιά γωνία του e-mail.

   Θα ανοίξει ένα παράθυρο διαλόγου, το οποίο θα επιβεβαιώνει ότι ο παραλήπτης έχει προστεθεί με επιτυχία στη λίστα αξιόπιστων επαφών.

8. Κάντε κλικ στο **OK**.

Προβολή λεπτομερειών αξιόπιστης επαφής

1. Ανοίξτε το Privacy Manager και επιλέξτε **Trusted Contacts** (Αξιόπιστες επαφές).

2. Κάντε κλικ σε μια αξιόπιστη επαφή.

3. Επιλέξτε **Contact details** (Λεπτομέρειες επικοινωνίας).

4. Όταν ολοκληρώσετε την προβολή των λεπτομερειών, κάντε κλικ στο **OK**.

Διαγραφή μιας αξιόπιστης επαφής

1. Ανοίξτε το Privacy Manager και επιλέξτε **Trusted Contacts** (Αξιόπιστες επαφές).
2. Κάντε κλικ στην αξιόπιστη επαφή που επιθυμείτε να διαγράψετε.
3. Κάντε κλικ στο κουμπί **Delete contact** (Διαγραφή επαφής).
4. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

Έλεγχος κατάστασης ανάκλησης για μια αξιόπιστη επαφή

Για να διαπιστώσετε εάν μια αξιόπιστη επαφή έχει ανακαλέσει το πιστοποιητικό Privacy Manager:

1. Ανοίξτε το Privacy Manager και επιλέξτε **Trusted Contacts** (Αξιόπιστες επαφές).
2. Κάντε κλικ σε μια αξιόπιστη επαφή.
3. Κάντε κλικ στο κουμπί **Advanced** (Για προχωρημένους).

   Ανοίγει το πλαίσιο διαλόγου Advanced Trusted Contact Management (Διαχείριση αξιόπιστης επαφής για προχωρημένους)
4. Κάντε κλικ στην επιλογή **Check Revocation** (Έλεγχος ανάκλησης).
5. Κάντε κλικ στο κουμπί **Κλείσιμο**.

Γενικές εργασίες

Μπορείτε να χρησιμοποιήσετε το Privacy Manager με τα παρακάτω προϊόντα της Microsoft:

- Microsoft Outlook
- Microsoft Office
- Windows Live Messenger

Χρήση του Privacy Manager στο Microsoft Outlook

Όταν εγκαταστήσετε το Privacy Manager, εμφανίζεται ένα κουμπί Privacy (Απόρρητο) στη γραμμή εργαλείων του Microsoft Outlook και ένα κουμπί Send Securely (Ασφαλής αποστολή) στη γραμμή εργαλείων κάθε μηνύματος e-mail του Microsoft Outlook. Όταν κάνετε κλικ στο κάτω βέλος δίπλα στις επιλογές **Privacy** (Απόρρητο) ή **Send Securely** (Ασφαλής αποστολή), μπορείτε να επιλέξετε από τις παρακάτω επιλογές:

- Sign and Send (Υπογραφή και αποστολή) (Μόνο από το κουμπί ασφαλούς αποστολής) — Αυτή η επιλογή προσθέτει μια ψηφιακή υπογραφή στο e-mail και το αποστέλλει αφού ελέγξετε την ταυτότητά του χρησιμοποιώντας την επιλεγμένη μέθοδο σύνδεσης ασφαλείας.
- Seal for Trusted Contacts and Send (Σφράγιση για αξιόπιστες επαφές και αποστολή) (Μόνο από το κουμπί ασφαλούς αποστολής) — Αυτή η επιλογή προσθέτει μια ψηφιακή υπογραφή, κρυπτογραφεί το e-mail και το αποστέλλει αφού πραγματοποιήσετε έλεγχο ταυτότητας χρησιμοποιώντας την επιλεγμένη μέθοδο σύνδεσης ασφαλείας.
- Invite Contacts (Πρόσκληση επαφών) — Αυτή η επιλογή σάς επιτρέπει να αποστείλετε μια πρόσκληση αξιόπιστης επαφής. Για περισσότερες πληροφορίες, δείτε την ενότητα Προσθήκη αξιόπιστης επαφής στη σελίδα 50.
- Invite Outlook Contacts (Πρόσκληση επαφών από το Outlook) — Αυτή η επιλογή σάς επιτρέπει να αποστέλλετε μια πρόσκληση αξιόπιστης επαφής σε όλες τις επαφές στο βιβλίο διευθύνσεων του Microsoft Outlook. Για περισσότερες πληροφορίες, δείτε την ενότητα Προσθήκη αξιόπιστων επαφών με χρήση των επαφών του Microsoft Outlook στη σελίδα 51.
- Open the Privacy Manager software (Άνοιγμα του λογισμικού Privacy Manager) — Οι επιλογές πιστοποιητικών, επιλεγμένων επαφών και ρυθμίσεων σάς επιτρέπουν να ανοίξετε το λογισμικό του Privacy Manager για προσθήκη, προβολή ή αλλαγή των τρεχουσών ρυθμίσεων. Για περισσότερες πληροφορίες, δείτε την ενότητα Διαμόρφωση του Privacy Manager για το Microsoft Outlook στη σελίδα 54.

Διαμόρφωση του Privacy Manager για το Microsoft Outlook

1. Ανοίξτε το Privacy Manager, κάντε κλικ στην επιλογή **Settings** (Ρυθμίσεις) και στη συνέχεια, κάντε κλικ στην καρτέλα **E-mail**.

   – ή –

   Στη βασική γραμμή εργαλείων του Microsoft Outlook, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) [**Privacy** (Απόρρητο) στο Outlook 2003] και επιλέξτε **Settings** (Ρυθμίσεις).

   – ή –

   Στη γραμμή εργαλείων ενός μηνύματος e-mail Microsoft, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) και επιλέξτε **Settings** (Ρυθμίσεις).

2. Επιλέξτε τις ενέργειες που επιθυμείτε να πραγματοποιήσετε όταν αποστέλλετε ένα ασφαλές e-mail και κάντε κλικ στο **OK**.

Υπογραφή και αποστολή ενός μηνύματος e-mail

1. Στο Microsoft Outlook, επιλέξτε **New** (Νέο) ή **Reply** (Απάντηση).
2. Πληκτρολογήστε το μήνυμα e-mail.
3. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) [**Privacy** (Απόρρητο) στο Outlook 2003] και επιλέξτε **Sign and Send** (Υπογραφή και αποστολή).
4. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

Σφράγισμα και αποστολή ενός μηνύματος e-mail

Η προβολή των σφραγισμένων μηνυμάτων e-mail που υπογράφονται και σφραγίζονται (κρυπτογραφούνται) ψηφιακά, είναι δυνατή μόνο από άτομα που επιλέγετε από τη λίστα αξιόπιστων επαφών.

Για σφράγιση και αποστολή ενός μηνύματος e-mail σε μια αξιόπιστη επαφή:

1. Στο Microsoft Outlook, επιλέξτε **Δημιουργία** ή **Απάντηση**.
2. Πληκτρολογήστε το μήνυμα e-mail.
3. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Send Securely** (Ασφαλής αποστολή) [**Privacy** (Απόρρητο) στο Outlook 2003] και επιλέξτε **Seal for Trusted Contacts and Send** (Σφράγιση για αξιόπιστες επαφές και αποστολή).
4. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

Προβολή ενός σφραγισμένου μηνύματος e-mail

Όταν ανοίγετε ένα σφραγισμένο μήνυμα e-mail, εμφανίζεται η ετικέτα ασφαλείας στην επικεφαλίδα του e-mail. Η ετικέτα ασφαλείας παρέχει τις ακόλουθες πληροφορίες:

- Τα διαπιστευτήρια που χρησιμοποιήθηκαν για την εξακρίβωση της ταυτότητας του ατόμου που υπέγραψε το e-mail
- Το προϊόν που χρησιμοποιήθηκε για την εξακρίβωση των διαπιστευτηρίων του ατόμου που υπέγραψε το e-mail

Χρήση του Privacy Manager σε ένα έγγραφο του Microsoft Office 2007

ΣΗΜΕΙΩΣΗ Το Privacy Manager μπορεί να χρησιμοποιηθεί μόνο με έγγραφα του Microsoft Office 2007.

Αφού εγκαταστήσετε το πιστοποιητικό Privacy Manager, εμφανίζεται ένα κουμπί Sign and Encrypt (Υπογραφή και κρυπτογράφηση) στη δεξιά πλευρά της γραμμής εργαλείων όλων των εγγράφων του Microsoft Word, Microsoft Excel και Microsoft PowerPoint. Όταν κάνετε κλικ στο κάτω βέλος δίπλα στις επιλογές **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση), μπορείτε να ενεργοποιήσετε τις παρακάτω επιλογές:

- Sign Document (Υπογραφή εγγράφου) — Αυτή η επιλογή προσθέτει την ψηφιακή σας υπογραφή στο έγγραφο.
- Add Signature Line Before Signing (Προσθήκη γραμμής υπογραφής πριν από την υπογραφή) (Μόνο σε Microsoft Word και Microsoft Excel) — Από προεπιλογή, προστίθεται μια γραμμή υπογραφής κατά την υπογραφή ή την κρυπτογράφηση ενός εγγράφου Microsoft Word ή Microsoft Excel. Για να απενεργοποιήσετε αυτή την επιλογή, επιλέξτε **Add Signature Line** (Προσθήκη γραμμής υπογραφής) για να αφαιρέσετε το σημάδι επιλογής.
- Encrypt Document (Κρυπτογράφηση εγγράφου) — Αυτή η επιλογή προσθέτει την ψηφιακή σας υπογραφή και κρυπτογραφεί το έγγραφο.
- Remove Encryption (Αφαίρεση κρυπτογράφησης) — Αυτή η επιλογή αφαιρεί την κρυπτογράφηση από το έγγραφο.
- Open the Privacy Manager software (Άνοιγμα του λογισμικού Privacy Manager) — Οι επιλογές πιστοποιητικών, επιλεγμένων επαφών και ρυθμίσεων σάς επιτρέπουν να ανοίξετε το λογισμικό του Privacy Manager για προσθήκη, προβολή ή αλλαγή των τρεχουσών ρυθμίσεων. Για περισσότερες πληροφορίες, δείτε την ενότητα Διαχείριση πιστοποιητικών του Privacy Manager στη σελίδα 45, Διαχείριση αξιόπιστων επαφών στη σελίδα 49 ή Διαμόρφωση του Privacy Manager για το Microsoft Office στη σελίδα 55.

Διαμόρφωση του Privacy Manager για το Microsoft Office

1. Ανοίξτε το Privacy Manager, κάντε κλικ στην επιλογή **Settings** (Ρυθμίσεις) και, στη συνέχεια, κάντε κλικ στην καρτέλα **Documents** (Έγγραφα).

   – ή –

   Στη γραμμή εργαλείων ενός εγγράφου του Microsoft Office, κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και έπειτα επιλέξτε **Settings** (Ρυθμίσεις).

2. Επιλέξτε τις ενέργειες που επιθυμείτε να διαμορφώσετε και, στη συνέχεια, κάντε κλικ στο **OK**.

Υπογραφή ενός εγγράφου του Microsoft Office

1. Στο Microsoft Word, Microsoft Excel ή Microsoft PowerPoint, δημιουργήστε και αποθηκεύστε ένα έγγραφο.
2. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και, στη συνέχεια, κάντε κλικ στην επιλογή **Sign Document** (Υπογραφή εγγράφου).
3. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.
4. Όταν ανοίξει το παράθυρο διαλόγου επιβεβαίωσης, διαβάστε το κείμενο και, στη συνέχεια, κάντε κλικ στο **OK**.

Εάν αργότερα αποφασίσετε να επεξεργαστείτε το έγγραφο, ακολουθήστε τα εξής βήματα:

1. Κάντε κλικ στο κουμπί **Office** στην επάνω αριστερή γωνία της οθόνης.
2. Κάντε κλικ στην επιλογή **Prepare** (Προετοιμασία) και επιλέξτε **Mark as Final** (Σήμανση ως τελικό).
3. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι) και συνεχίστε.
4. Όταν ολοκληρώσετε την επεξεργασία σας, υπογράψτε το έγγραφο ξανά.

Προσθήκη γραμμής υπογραφής κατά την υπογραφή ενός εγγράφου Microsoft Word ή Microsoft Excel

Το Privacy Manager επιτρέπει την προσθήκη μιας γραμμής υπογραφής όταν υπογράφετε ένα έγγραφο Microsoft Word ή Microsoft Excel:

1. Στο Microsoft Word ή το Microsoft Excel δημιουργήστε και αποθηκεύστε ένα έγγραφο.
2. Κάντε κλικ στο μενού **Κεντρική**.
3. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και, στη συνέχεια, κάντε κλικ στην επιλογή **Add Signature Line Before Signing** (Προσθήκη γραμμής υπογραφής πριν από την υπογραφή).

   ΣΗΜΕΙΩΣΗ Ένα σημάδι επιλογής εμφανίζεται δίπλα από την επιλογή Add Signature Line Before Signing (Προσθήκη γραμμής υπογραφής πριν από την υπογραφή) όταν ενεργοποιηθεί η επιλογή. Από προεπιλογή, η επιλογή είναι ενεργοποιημένη.

4. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και, στη συνέχεια, κάντε κλικ στην επιλογή **Sign Document** (Υπογραφή εγγράφου).
5. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

Προσθήκη προτεινόμενων υπογραφόντων σε ένα έγγραφο Microsoft Word ή Microsoft Excel

Μπορείτε να προσθέσετε περισσότερες από μία γραμμές υπογραφής στο έγγραφό σας ορίζοντας προτεινόμενους υπογράφοντες. Ένας προτεινόμενος υπογράφοντας είναι ένας χρήστης που έχει οριστεί από τον κάτοχο ενός εγγράφου Microsoft Word ή Microsoft Excel για προσθήκη μιας γραμμής υπογραφής στο έγγραφο. Οι προτεινόμενοι υπογράφοντες μπορεί να είστε εσείς ή άλλο πρόσωπο που επιθυμείτε να υπογράψει το έγγραφό σας. Για παράδειγμα, εάν προετοιμάζετε ένα έγγραφο που πρέπει να υπογραφεί από όλα τα μέλη του τμήματός σας, μπορείτε να συμπεριλάβετε γραμμές υπογραφής για αυτούς τους χρήστες στο κάτω μέρος της τελευταίας σελίδας του εγγράφου με οδηγίες για υπογραφή έως μια συγκεκριμένη ημερομηνία.

Για προσθήκη ενός προτεινόμενου υπογράφοντα σε ένα έγγραφο Microsoft Word ή Microsoft Excel:

1. Στο Microsoft Word ή το Microsoft Excel, δημιουργήστε και αποθηκεύστε ένα έγγραφο.
2. Κάντε κλικ στο μενού **Εισαγωγή**.
3. Στην ομάδα **Κείμενο** στη γραμμή εργαλείων, κάντε κλικ στο βέλος δίπλα στην επιλογή **Γραμμή υπογραφής** και επιλέξτε **Privacy Manager Signature Provider** (Παροχή υπογραφής Privacy Manager).

   Ανοίγει το παράθυρο διαλόγου Signature Setup (Ρύθμιση υπογραφής).
4. Στο πλαίσιο κάτω από την επιλογή **Suggested signer** (Προτεινόμενος υπογράφοντας), πληκτρολογήστε το όνομα του προτεινόμενου υπογράφοντα.
5. Στο πλαίσιο κάτω από την επιλογή **Instructions to the signer** (Οδηγίες για τον υπογράφοντα), πληκτρολογήστε ένα μήνυμα για τον προτεινόμενο υπογράφοντα.

ΣΗΜΕΙΩΣΗ Αυτό το μήνυμα θα εμφανιστεί στη θέση ενός τίτλου και είτε θα διαγραφεί είτε θα αντικατασταθεί από τον τίτλο του χρήστη όταν θα υπογραφεί το έγγραφο.

6. Επιλέξτε το πλαίσιο ελέγχου **Show sign date in signature line** (Εμφάνιση ημερομηνίας υπογραφής στη γραμμή υπογραφής) για εμφάνιση της ημερομηνίας.
7. Επιλέξτε τον τίτλο **Show signer's title in signature line** (Εμφάνιση του τίτλου υπογράφοντα στη γραμμή υπογραφής) για εμφάνιση του τίτλου.

ΣΗΜΕΙΩΣΗ Επειδή ο κάτοχος του εγγράφου ορίζει προτεινόμενους υπογράφοντες στο έγγραφό του, εάν τα πλαίσια ελέγχου **Show sign date in signature line** (Εμφάνιση ημερομηνίας υπογραφής στη γραμμή υπογραφής) ή/και **Show signer's title in signature line** (Εμφάνιση του τίτλου υπογράφοντα στη γραμμή υπογραφής) δεν είναι επιλεγμένα, ο προτεινόμενος υπογράφοντας δεν θα μπορέσει να εμφανίσει την ημερομηνία ή/και τον τίτλο στη γραμμή υπογραφής ακόμη και εάν οι ρυθμίσεις του εγγράφου του προτεινόμενου υπογράφοντα είναι ρυθμισμένες για να το κάνουν.'

8. Κάντε κλικ στο **OK**.

Προσθήκη γραμμής υπογραφής ενός προτεινόμενου υπογράφοντα

Όταν οι προτεινόμενοι υπογράφοντες θα ανοίγουν το έγγραφο, θα βλέπουν τα ονόματά τους σε αγκύλες, υποδεικνύοντας ότι απαιτείται η υπογραφή τους.

Για υπογραφή του εγγράφου:

1. Κάντε διπλό κλικ στην κατάλληλη γραμμή υπογραφής.
2. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

   Η γραμμή υπογραφής θα εμφανίζεται σύμφωνα με τις ρυθμίσεις που καθορίζονται από τον κάτοχο του εγγράφου.

Κρυπτογράφηση ενός εγγράφου του Microsoft Office

Μπορείτε να κρυπτογραφήσετε ένα έγγραφο του Microsoft Office για εσάς και για τις αξιόπιστες επαφές σας. Όταν κρυπτογραφείτε ένα έγγραφο και το κλείνετε, εσείς και οι αξιόπιστες επαφές που επιλέξατε από τη λίστα πρέπει να πραγματοποιείτε έλεγχο ταυτότητας πριν από το άνοιγμα.

Για κρυπτογράφηση ενός εγγράφου του Microsoft Office:

1. Στο Microsoft Word, Microsoft Excel ή Microsoft PowerPoint, δημιουργήστε και αποθηκεύστε ένα έγγραφο.
2. Κάντε κλικ στο μενού **Κεντρική**.
3. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και, στη συνέχεια, κάντε κλικ στην επιλογή **Encrypt Document** (Κρυπτογράφηση εγγράφου).

   Ανοίγει το πλαίσιο διαλόγου Select Trusted Contacts (Επιλογή αξιόπιστων επαφών)
4. Κάντε κλικ στο όνομα μιας αξιόπιστης επαφής που θα μπορεί να ανοίξει το έγγραφο και να προβάλλει το περιεχόμενό του.

ΣΗΜΕΙΩΣΗ Για επιλογή πολλών ονομάτων αξιόπιστων επαφών, κρατήστε πατημένο το πλήκτρο ctrl και κάντε κλικ στα μεμονωμένα ονόματα.

5. Κάντε κλικ στο **OK**.

Εάν αργότερα αποφασίσετε να επεξεργαστείτε το έγγραφο, ακολουθήστε τα βήματα στην ενότητα Αφαίρεση κρυπτογράφησης από ένα έγγραφο του Microsoft Office στη σελίδα 58. Όταν αφαιρεθεί η κρυπτογράφηση, μπορείτε να επεξεργαστείτε το έγγραφο. Ακολουθήστε τα βήματα σε αυτή την ενότητα για να κρυπτογραφήσετε το έγγραφο ξανά.

Αφαίρεση κρυπτογράφησης από ένα έγγραφο του Microsoft Office

Όταν αφαιρείτε την κρυπτογράφηση από ένα έγγραφο του Microsoft Office, εσείς και οι αξιόπιστες επαφές σας δεν χρειάζεται πια να πραγματοποιείτε έλεγχο της ταυτότητάς σας για να ανοίξετε και να προβάλετε τα περιεχόμενα του εγγράφου.

Για αφαίρεση κρυπτογράφησης από ένα έγγραφο του Microsoft Office:

1. Ανοίξτε ένα κρυπτογραφημένο έγγραφο Microsoft Word, Microsoft Excel ή Microsoft PowerPoint.
2. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.
3. Κάντε κλικ στο μενού **Κεντρική**.
4. Κάντε κλικ στο κάτω βέλος δίπλα στην επιλογή **Sign and Encrypt** (Υπογραφή και κρυπτογράφηση) και, στη συνέχεια, κάντε κλικ στην επιλογή **Remove Encryption** (Αφαίρεση κρυπτογράφησης).

Αποστολή ενός κρυπτογραφημένου εγγράφου του Microsoft Office

Μπορείτε να επισυνάψετε ένα κρυπτογραφημένο έγγραφο του Microsoft Office σε ένα μήνυμα e-mail, χωρίς να υπογράψετε ή να κρυπτογραφήσετε το ίδιο το e-mail. Για να το κάνετε αυτό, δημιουργήστε και αποστείλετε ένα e-mail με ένα υπογεγραμμένο ή κρυπτογραφημένο έγγραφο όπως θα κάνατε με ένα κανονικό e-mail με επισύναψη.

Ωστόσο, για βέλτιστη ασφάλεια, συνιστάται να κρυπτογραφείτε το e-mail όταν επισυνάπτετε ένα υπογεγραμμένο ή κρυπτογραφημένο έγγραφο του Microsoft Office.

Για αποστολή ενός σφραγισμένου e-mail με ένα επισυναπτόμενο υπογεγραμμένο ή/και κρυπτογραφημένο έγγραφο του Microsoft Office, ακολουθήστε τα εξής βήματα:

1. Στο Microsoft Outlook, επιλέξτε **Δημιουργία** ή **Απάντηση**.
2. Πληκτρολογήστε το μήνυμα e-mail.

3. Επισυνάψτε το έγγραφο του Microsoft Office.

4. Ανατρέξτε στην ενότητα Σφράγισμα και αποστολή ενός μηνύματος e-mail στη σελίδα 54 για περαιτέρω οδηγίες.

Προβολή ενός υπογεγραμμένου εγγράφου του Microsoft Office

ΣΗΜΕΙΩΣΗ Δεν χρειάζεται να διαθέτετε ένα πιστοποιητικό Privacy Manager για να προβάλλετε ένα υπογεγραμμένο έγγραφο του Microsoft Office.

Όταν ανοίγετε ένα υπογεγραμμένο έγγραφο του Microsoft Office, εμφανίζεται ένα εικονίδιο ψηφιακής υπογραφής στη γραμμή κατάστασης στο κάτω μέρος του παράθυρου εγγράφου.

1. Κάντε κλικ στο εικονίδιο **Digital Signatures** (Ψηφιακές υπογραφές) για εναλλαγή της εμφάνισης του παράθυρου Signatures (Υπογραφές), το οποίο εμφανίζει τα ονόματα όλων των χρηστών που υπέγραψαν το έγγραφο και την ημερομηνία που το υπέγραψε ο κάθε χρήστης.

2. Για προβολή επιπλέον πληροφοριών σχετικά με κάθε υπογραφή, κάντε δεξί κλικ σε ένα όνομα στο πλαίσιο διαλόγου Signatures (Υπογραφές) και επιλέξτε Signature Details (Λεπτομέρειες υπογραφών).

Προβολή ενός κρυπτογραφημένου εγγράφου του Microsoft Office

Για προβολή ενός κρυπτογραφημένου εγγράφου του Microsoft Office από άλλον υπολογιστή, το Privacy Manager πρέπει να είναι εγκατεστημένο σε αυτό τον υπολογιστή. Επιπλέον, πρέπει να επαναφέρετε το πιστοποιητικό Privacy Manager που χρησιμοποιήθηκε για την κρυπτογράφηση του αρχείου.

Μια αξιόπιστη επαφή που επιθυμεί να προβάλλει ένα κρυπτογραφημένο έγγραφο του Microsoft Office πρέπει να διαθέτει ένα πιστοποιητικό Privacy Manager και το Privacy Manager πρέπει να είναι εγκατεστημένο στον υπολογιστή της. Επιπλέον, η αξιόπιστη επαφή πρέπει να έχει επιλεγεί από τον κάτοχο του κρυπτογραφημένου εγγράφου του Microsoft Office.

Χρήση του Privacy Manager στο Windows Live Messenger

Το Privacy Manager προσθέτει τις ακόλουθες λειτουργίες ασφαλούς επικοινωνίας στο Windows Live Messenger:

- **Secure chat** (Ασφαλής συνομιλία) — Τα μηνύματα μεταδίδονται με χρήση του πρωτοκόλλου "SSL/TLS (Secure Sockets Layer/Transport Layer Security) over XML", την ίδια τεχνολογία που εξασφαλίζει την ασφάλεια των συναλλαγών του ηλεκτρονικού εμπορίου.
- **Recipient identification** (Αναγνώριση αποστολέα) — Μπορείτε να εξακριβώσετε την παρουσία και την ταυτότητα ενός ατόμου προτού αποστείλετε ένα μήνυμα.
- **Signed messages** (Υπογεγραμμένα μηνύματα) — Μπορείτε να υπογράψετε ηλεκτρονικά τα μηνύματά σας. Στη συνέχεια, εάν το μήνυμα αλλοιωθεί, θα επισημανθεί ως άκυρο όταν θα το λάβει ο παραλήπτης.
- **Hide/show feature** (Λειτουργία απόκρυψης/εμφάνισης) — Μπορείτε να κρύψετε οποιοδήποτε ή όλα τα μηνύματα στο παράθυρο Privacy Manager Chat. Μπορείτε επίσης να στείλετε ένα μήνυμα, του οποίου το περιεχόμενο θα είναι κρυφό. Θα απαιτείται έλεγχος ταυτότητας προτού εμφανιστεί το μήνυμα.

- **Secure chat history** (Ιστορικό ασφαλών συνομιλιών) — Τα αρχεία καταγραφής των συνομιλιών σας κρυπτογραφούνται προτού αποθηκευτούν και απαιτείται έλεγχος ταυτότητας πριν από την προβολή τους.
- **Automatic locking/unlocking** (Αυτόματο κλείδωμα/ξεκλείδωμα) — Μπορείτε να κλειδώσετε και να ξεκλειδώσετε το παράθυρο Privacy Manager Chat ή να το ρυθμίσετε για αυτόματο κλείδωμα έπειτα από μια συγκεκριμένη χρονική περίοδο.

Εκκίνηση μιας συνομιλίας με το Privacy Manager Chat

ΣΗΜΕΙΩΣΗ Για να χρησιμοποιήσετε το Privacy Manager Chat και οι δύο συμμετέχοντες πρέπει να έχουν εγκαταστήσει το Privacy Manager και ένα πιστοποιητικό του Privacy Manager. Για λεπτομέρειες σχετικά με την εγκατάσταση ενός πιστοποιητικού Privacy Manager, δείτε την ενότητα Αίτημα και εγκατάσταση πιστοποιητικού του Privacy Manager στη σελίδα 45.

1. Για εκκίνηση του Privacy Manager Chat στο Windows Live Messenger, πραγματοποιήστε μία από τις παρακάτω διαδικασίες:

   α. Κάντε δεξί κλικ σε μια ηλεκτρονική επαφή στο Live Messenger και, στη συνέχεια, επιλέξτε **Έναρξη δραστηριότητας**.

   β. Κάντε κλικ στο κουμπί **Start Chat** (Έναρξη συνομιλίας).

   – ή –

   α. Κάντε διπλό κλικ σε μια συνδεδεμένη επαφή στο Live Messenger και, στη συνέχεια, επιλέξτε το μενού **Προβολή λίστας δραστηριοτήτων**.

   β. Κάντε κλικ στην επιλογή **Ενέργεια** και επιλέξτε **Start Chat** (Έναρξη συνομιλίας).

   – ή –

   α. Κάντε δεξί κλικ στο εικονίδιο ProtectTools στην περιοχή ειδοποιήσεων, κάντε κλικ στην επιλογή **Privacy Manager for HP ProtectTools** και επιλέξτε **Start Chat** (Έναρξη συνομιλίας).

   β. Στο Live Messenger, κάντε κλικ στην επιλογή **Ενέργειες: Έναρξη δραστηριότητας** και επιλέξτε **Privacy Manager Chat**.

   ΣΗΜΕΙΩΣΗ Κάθε χρήστης πρέπει να είναι συνδεδεμένος στο Live Messenger και οι χρήστες πρέπει να εμφανίζονται στο ηλεκτρονικό παράθυρο Live Messenger του άλλου. Κάντε κλικ για να επιλέξετε ένα συνδεδεμένο χρήστη.

   Το Privacy Manager στέλνει μια πρόσκληση στην επαφή για εκκίνηση του Privacy Manager Chat. Όταν η επαφή αποδεχτεί την πρόσκληση, ανοίγει το παράθυρο Privacy Manager Chat. Εάν η προσκεκλημένη επαφή δεν διαθέτει το Privacy Manager, θα της ζητηθεί να πραγματοποιήσει λήψη του προγράμματος.

2. Κάντε κλικ στο **Start** (Έναρξη) για να ξεκινήσετε μια ασφαλή συνομιλία.

Διαμόρφωση του Privacy Manager για το Windows Live Messenger

1. Στο Privacy Manager Chat, κάντε κλικ στο κουμπί **Settings** (Ρυθμίσεις).

   – ή –

   Στο Privacy Manager, κάντε κλικ στην επιλογή **Settings** (Ρυθμίσεις) και, στη συνέχεια, κάντε κλικ στην καρτέλα **Chat** (Συνομιλία).

   – ή –

   Στο Privacy Manager Live Messenger History Viewer, κάντε κλικ στο κουμπί **Settings** (Ρυθμίσεις).

2. Για να καθορίσετε το χρονικό διάστημα αναμονής του Privacy Manager Chat προτού κλειδώσει τη συνομιλία σας, επιλέξτε έναν αριθμό από το πλαίσιο **Lock session after _ minutes of inactivity** (Κλείδωμα της συνομιλίας μετά από _ λεπτά αδράνειας).

3. Για να καθορίσετε ένα φάκελο ιστορικού για τις συνομιλίες σας, κάντε κλικ στην επιλογή **Browse** (Αναζήτηση) για αναζήτηση ενός φακέλου και επιλέξτε **OK**.

4. Για αυτόματη κρυπτογράφηση και αποθήκευση των συνομιλιών σας κατά το κλείσιμο, επιλέξτε το πλαίσιο ελέγχου **Automatically save secure chat history** (Αυτόματη αποθήκευση ασφαλούς ιστορικού συνομιλιών).

5. Κάντε κλικ στο **OK**.

Συνομιλία στο παράθυρο Privacy Manager Chat

Μετά την εκκίνηση του Privacy Manager Chat, ανοίγει ένα παράθυρο Privacy Manager Chat στο Windows Live Messenger. Η χρήση του Privacy Manager Chat είναι παρόμοια με τη χρήση του Windows Live Messenger, εκτός από τις παρακάτω πρόσθετες λειτουργίες που είναι διαθέσιμες στο παράθυρο του Privacy Manager Chat:

- **Save** (Αποθήκευση) — Κάντε κλικ σε αυτό το κουμπί για να αποθηκεύσετε τη συνομιλία σας στον φάκελο που καθορίσατε στις ρυθμίσεις διαμόρφωσης. Μπορείτε επίσης να διαμορφώσετε το Privacy Manager Chat ώστε να αποθηκεύει αυτόματα κάθε νέα συνομιλία όταν αυτή τερματίζεται.
- **Hide all** (Απόκρυψη όλων) και **Show all** (Εμφάνιση όλων) — Κάντε κλικ στο κατάλληλο κουμπί για επέκταση ή σύμπτυξη των μηνυμάτων που εμφανίζονται στο παράθυρο Secure Communications (Ασφαλείς συνομιλίες). Μπορείτε επίσης να αποκρύψετε ή να εμφανίσετε μεμονωμένα μηνύματα κάνοντας κλικ στην επικεφαλίδα του μηνύματος.
- **Are you there?** (Είσαι εκεί;) — Κάντε κλικ σε αυτό το κουμπί για να ζητήσετε έλεγχο της ταυτότητας από την επαφή σας.
- **Lock** (Κλείδωμα) — Κάντε κλικ σε αυτό το κουμπί για κλείσιμο του παράθυρου Privacy Manager Chat και επιστροφή στο παράθυρο Chat Entry (Καταχώριση συνομιλίας). Για να εμφανίσετε το παράθυρο Secure Communications ξανά, κάντε κλικ στην επιλογή **Resume the session** (Συνέχιση της συνομιλίας) και στη συνέχεια πραγματοποιήστε έλεγχο της ταυτότητας χρησιμοποιώντας την επιλεγμένη μέθοδο σύνδεσης ασφαλείας.
- **Send** (Αποστολή) — Κάντε κλικ σε αυτό το κουμπί για να αποστείλετε ένα κρυπτογραφημένο μήνυμα στην επαφή σας.
- **Send signed** (Αποστολή με υπογραφή) — Επιλέξτε αυτό το πλαίσιο ελέγχου για να υπογράψετε ηλεκτρονικά και να κρυπτογραφήσετε τα μηνύματά σας. Στη συνέχεια, εάν το μήνυμα αλλοιωθεί,

θα επισημανθεί ως άκυρο όταν θα το λάβει ο παραλήπτης. Θα πρέπει να πιστοποιείται η ταυτότητά σας κάθε φορά που αποστέλλετε ένα υπογεγραμμένο μήνυμα.

- **Send hidden** (Αποστολή με απόκρυψη) — Επιλέξτε αυτό το πλαίσιο ελέγχου για να κρυπτογραφήσετε και να αποστείλετε ένα μήνυμα με εμφάνιση μόνο της επικεφαλίδας του μηνύματος. Η επαφή σας θα πρέπει να πιστοποιήσει την ταυτότητά της για ανάγνωση του περιεχόμενου του μηνύματος.

Προβολή ιστορικού συνομιλιών

Το Privacy Manager Chat: Το πρόγραμμα προβολής Live Messenger History Viewer εμφανίζει μόνο τα κρυπτογραφημένα αρχεία συνομιλιών του Privacy Manager Chat. Μπορείτε να αποθηκεύσετε τις συνομιλίες κάνοντας κλικ στην επιλογή **Save** (Αποθήκευση) στο παράθυρο Privacy Manager Chat ή ρυθμίζοντας την αυτόματη αποθήκευση στην καρτέλα Chat (Συνομιλία) του Privacy Manager. Στο πρόγραμμα προβολής, για κάθε συνομιλία εμφανίζεται το (κρυπτογραφημένο) εμφανιζόμενο όνομα της επαφής και η ημερομηνία και η ώρα που άρχισε και τελείωσε η συνομιλία. Από προεπιλογή, εμφανίζονται οι συνομιλίες για όλους τους λογαριασμούς e-mail που έχετε ρυθμίσει. Μπορείτε να χρησιμοποιήσετε το μενού **Display history for** (Εμφάνιση ιστορικού για) για να επιλέξετε την προβολή μόνο συγκεκριμένων λογαριασμών.

Το πρόγραμμα προβολής σάς επιτρέπει να εκτελέσετε τις ακόλουθες εργασίες:

- Εμφάνιση όλων των συνομιλιών στη σελίδα 62
- Εμφάνιση συνομιλιών για συγκεκριμένο λογαριασμό στη σελίδα 63
- Προβολή αναγνωριστικού συνομιλίας στη σελίδα 63
- Προβολή συνομιλίας στη σελίδα 63
- Αναζήτηση συνομιλιών για συγκεκριμένο κείμενο στη σελίδα 64
- Διαγραφή συνομιλίας στη σελίδα 64
- Προσθήκη ή αφαίρεση στηλών στη σελίδα 64
- Φιλτράρισμα εμφανιζόμενων συνομιλιών στη σελίδα 64

Για εκκίνηση του προγράμματος προβολής Live Messenger History Viewer:

▲ Στην περιοχή ειδοποιήσεων, στο δεξί άκρο της γραμμής εργασιών, κάντε δεξί κλικ στο εικονίδιο **HP ProtectTools** και επιλέξτε **Privacy Manager: for HP ProtectTools** (Privacy Manager: για HP ProtectTools) και, στη συνέχεια, κάντε κλικ στην επιλογή **Live Messenger History Viewer**.

– ή –

▲ Σε μια συνομιλία, κάντε κλικ στην επιλογή **History Viewer** (Πρόγραμμα προβολής ιστορικού) ή **History** (Ιστορικό).

Εμφάνιση όλων των συνομιλιών

Η εμφάνιση όλων των συνομιλιών προβάλλει το κρυπτογραφημένο εμφανιζόμενο όνομα για τις τρέχουσες επιλεγμένες συνομιλίες και όλες τις συνομιλίες στον ίδιο λογαριασμό.

Για εμφάνιση όλων των αποθηκευμένων ιστορικών συνομιλιών:

1. Στο πρόγραμμα προβολής Live Messenger History, κάντε δεξί κλικ σε οποιαδήποτε συνομιλία και, στη συνέχεια, επιλέξτε **Reveal All Sessions** (Εμφάνιση όλων των συνομιλιών).
2. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

   Τα εμφανιζόμενα ονόματα των επαφών αποκρυπτογραφούνται.
3. Κάντε διπλό κλικ σε οποιαδήποτε συνομιλία για προβολή του περιεχομένου της.

Εμφάνιση συνομιλιών για συγκεκριμένο λογαριασμό

Η εμφάνιση μιας συνομιλίας προβάλλει το κρυπτογραφημένο εμφανιζόμενο όνομα της επαφής για την τρέχουσα επιλεγμένη επαφή.

Για εμφάνιση του ιστορικού μιας συγκεκριμένης συνομιλίας:

1. Στο πρόγραμμα προβολής Live Messenger History, κάντε δεξί κλικ σε οποιαδήποτε συνομιλία και, στη συνέχεια, επιλέξτε **Reveal Session** (Εμφάνιση συνομιλίας).
2. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

   Το εμφανιζόμενο όνομα της επαφής αποκρυπτογραφείται.
3. Κάντε διπλό κλικ στη συνομιλία για προβολή του περιεχομένου της.

ΣΗΜΕΙΩΣΗ Οι πρόσθετες συνομιλίες που έχουν κρυπτογραφηθεί με το ίδιο πιστοποιητικό θα εμφανίζουν ένα εικονίδιο μη κλειδωμένου, υποδεικνύοντας ότι μπορείτε να πραγματοποιήσετε προβολή τους κάνοντας διπλό κλικ σε οποιαδήποτε από αυτές τις συνομιλίες χωρίς πρόσθετο έλεγχο ταυτότητας. Οι συνομιλίες που έχουν κρυπτογραφηθεί με διαφορετικό πιστοποιητικό θα εμφανίζουν ένα εικονίδιο κλειδώματος, υποδεικνύοντας ότι απαιτείται περαιτέρω έλεγχος ταυτότητας για αυτές τις συνομιλίες προτού εμφανίσετε τα εμφανιζόμενα ονόματα των επαφών ή τα περιεχόμενα.

Προβολή αναγνωριστικού συνομιλίας

Για προβολή ενός αναγνωριστικού συνομιλίας:

▲ Στο πρόγραμμα προβολής Live Messenger History, κάντε δεξί κλικ σε οποιαδήποτε συνομιλία που έχει εμφανιστεί και επιλέξτε **View session ID** (Προβολή αναγνωριστικού συνομιλίας).

Προβολή συνομιλίας

Η προβολή μιας συνομιλίας ανοίγει το φάκελο για προβολή. Εάν η συνομιλία δεν έχει εμφανιστεί (προβάλλοντας το κρυπτογραφημένο εμφανιζόμενο όνομα της επαφής) προηγουμένως, θα εμφανιστεί εκείνη τη στιγμή.

Για προβολή ενός ιστορικού συνομιλίας του Live Messenger:

1. Στο πρόγραμμα προβολής Live Messenger History, κάντε δεξί κλικ σε οποιαδήποτε συνομιλία και, στη συνέχεια, επιλέξτε **View** (Προβολή).
2. Εάν σας ζητηθεί, πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.

   Το περιεχόμενο της συνομιλίας έχει αποκρυπτογραφηθεί.

Αναζήτηση συνομιλιών για συγκεκριμένο κείμενο

Μπορείτε να πραγματοποιήσετε αναζήτηση κειμένου σε συνομιλίες που έχουν εμφανιστεί (αποκρυπτογραφημένες) στο παράθυρο του προγράμματος προβολής. Σε αυτές τις συνομιλίες το εμφανιζόμενο όνομα της επαφής εμφανίζεται ως απλό κείμενο.

Για αναζήτηση κειμένου σε ιστορικό συνομιλιών:

1. Στο πρόγραμμα προβολής ιστορικού Live Messenger History Viewer, κάντε κλικ στο κουμπί **Search** (Αναζήτηση).
2. Εισάγετε το κείμενο αναζήτησης, διαμορφώστε τυχόν επιθυμητές παραμέτρους και επιλέξτε **OK**.

   Οι συνομιλίες που περιέχουν το κείμενο επισημαίνονται στο παράθυρο του προγράμματος προβολής.

Διαγραφή συνομιλίας

1. Επιλέξτε ένα ιστορικό συνομιλιών.
2. Κάντε κλικ στο κουμπί **Delete** (Διαγραφή).

Προσθήκη ή αφαίρεση στηλών

Από προεπιλογή, οι 3 πιο χρησιμοποιούμενες στήλες εμφανίζονται στο πρόγραμμα προβολής ιστορικού Live Messenger History Viewer. Μπορείτε να προσθέσετε επιπλέον στήλες στην οθόνη ή μπορείτε να αφαιρέσετε στήλες από την οθόνη.

Για προσθήκη στηλών στην οθόνη:

1. Κάντε δεξί κλικ σε οποιαδήποτε επικεφαλίδα στήλης και επιλέξτε **Add/Remove Columns** (Προσθήκη/Αφαίρεση στηλών).
2. Επιλέξτε μια στήλη στο αριστερό τμήμα του παραθύρου και κάντε κλικ στην επιλογή **Add** (Προσθήκη) για να την μετακινήσετε στο δεξί τμήμα του παραθύρου.

Για αφαίρεση στηλών από την οθόνη:

1. Κάντε δεξί κλικ σε οποιαδήποτε επικεφαλίδα στήλης και επιλέξτε **Add/Remove Columns** (Προσθήκη/Αφαίρεση στηλών).
2. Επιλέξτε μια επικεφαλίδα στήλης στο δεξί τμήμα του παραθύρου και κάντε κλικ στην επιλογή **Remove** (Αφαίρεση) για να την μετακινήσετε στο αριστερό τμήμα του παραθύρου.

Φιλτράρισμα εμφανιζόμενων συνομιλιών

Στο πρόγραμμα προβολής ιστορικού Live Messenger History Viewer, εμφανίζεται μια λίστα των συνομιλιών για όλους τους λογαριασμούς σας. Μπορείτε επίσης να φιλτράρετε τις εμφανιζόμενες συνομιλίες για τα παρακάτω:

- Συγκεκριμένοι λογαριασμοί. Για λεπτομέρειες, ανατρέξτε στην ενότητα Εμφάνιση συνομιλιών για συγκεκριμένο λογαριασμό στη σελίδα 65.
- Εύρος ημερομηνιών. Για λεπτομέρειες, ανατρέξτε στην ενότητα Εμφάνιση συνομιλιών για ένα εύρος ημερομηνιών στη σελίδα 65.
- Διαφορετικοί φάκελοι. Για λεπτομέρειες, ανατρέξτε στην ενότητα Εμφάνιση συνομιλιών που είναι αποθηκευμένες σε φάκελο διαφορετικό από τον προεπιλεγμένο φάκελο στη σελίδα 65.

Εμφάνιση συνομιλιών για συγκεκριμένο λογαριασμό

- Στο πρόγραμμα προβολής ιστορικού Live Messenger History Viewer, επιλέξτε ένα λογαριασμό από το μενού **Display history for** (Εμφάνιση ιστορικού για).

Εμφάνιση συνομιλιών για ένα εύρος ημερομηνιών

1. Στο πρόγραμμα προβολής ιστορικού Live Messenger History Viewer, κάντε κλικ στο κουμπί **Advanced Filter** (Προηγμένο φίλτρο).

   Ανοίγει το πλαίσιο διαλόγου του Advanced Filter (Προηγμένο φίλτρο).

2. Επιλέξτε το πλαίσιο ελέγχου **Display only sessions within specified date range** (Εμφάνιση συνομιλιών μόνο μέσα σε συγκεκριμένο εύρος συνομιλιών).

3. Στα πλαίσια **From date** (Από) και **To date** (Προς), εισαγάγετε την ημερομηνία, το μήνα ή/και το έτος ή κάντε κλικ στο βέλος δίπλα από το ημερολόγιο για να επιλέξετε τις ημερομηνίες.

4. Κάντε κλικ στο **OK**.

Εμφάνιση συνομιλιών που είναι αποθηκευμένες σε φάκελο διαφορετικό από τον προεπιλεγμένο φάκελο

1. Στο πρόγραμμα προβολής ιστορικού Live Messenger History Viewer, κάντε κλικ στο κουμπί **Advanced Filter** (Προηγμένο φίλτρο).

2. Επιλέξτε το πλαίσιο ελέγχου **Use an alternate history files folder** (Χρήση εναλλακτικού φακέλου αρχείων ιστορικού).

3. Εισαγάγετε την τοποθεσία του φακέλου ή κάντε κλικ στην επιλογή **Browse** (Αναζήτηση) για αναζήτηση ενός φακέλου.

4. Κάντε κλικ στο **OK**.

Εργασίες για προχωρημένους

Μετεγκατάσταση πιστοποιητικών του Privacy Manager και αξιόπιστων επαφών σε διαφορετικό υπολογιστή

Μπορείτε να πραγματοποιήσετε ασφαλή μετεγκατάσταση των πιστοποιητικών του Privacy Manager και των αξιόπιστων επαφών σε διαφορετικό υπολογιστή ή να δημιουργήσετε αντίγραφα ασφαλείας των δεδομένων σας για ασφαλή διατήρηση. Για να το κάνετε αυτό, δημιουργήστε αντίγραφα ασφαλείας των δεδομένων ως αρχείο που προστατεύεται από κωδικό πρόσβασης σε μια τοποθεσία δικτύου ή σε οποιαδήποτε αφαιρούμενη συσκευή αποθήκευσης και, στη συνέχεια, επαναφέρετε το αρχείο στο νέο υπολογιστή.

Δημιουργία αντιγράφων ασφαλείας των πιστοποιητικών του Privacy Manager και των αξιόπιστων επαφών

Για να δημιουργήσετε αντίγραφα ασφαλείας των πιστοποιητικών του Privacy Manager και των αξιόπιστων επαφών σε ένα αρχείο που προστατεύεται από κωδικό πρόσβασης, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε το Privacy Manager και επιλέξτε **Migration** (Μετεγκατάσταση).
2. Κάντε κλικ στην επιλογή **Backup** (Δημιουργία αντιγράφων ασφαλείας).
3. Στη σελίδα Select Data (Επιλογή δεδομένων), επιλέξτε τις κατηγορίες δεδομένων που θα συμπεριληφθούν στο αρχείο μετεγκατάστασης και κάντε κλικ στο **Next** (Επόμενο).
4. Στη σελίδα Migration File (Αρχείο μετεγκατάστασης), πληκτρολογήστε ένα όνομα αρχείου ή κάντε κλικ στην επιλογή **Browse** (Αναζήτηση) για αναζήτηση μιας τοποθεσίας και κάντε κλικ στην επιλογή **Next** (Επόμενο).
5. Πληκτρολογήστε και επιβεβαιώστε ένα κωδικό πρόσβασης και κάντε κλικ στο κουμπί **Next** (Επόμενο).

ΣΗΜΕΙΩΣΗ Αποθηκεύστε τον κωδικό πρόσβασης σε ένα ασφαλές μέρος, καθώς θα τον χρειαστείτε κατά την επαναφορά του αρχείου μετεγκατάστασης.

6. Πραγματοποιήστε έλεγχο ταυτότητας χρησιμοποιώντας τη μέθοδο ασφαλούς σύνδεσης που έχετε επιλέξει.
7. Στη σελίδα Migration File Saved (Αποθήκευση αρχείου μετεγκατάστασης), κάντε κλικ στην επιλογή **Finish** (Τέλος).

Επαναφορά αντιγράφων ασφαλείας των πιστοποιητικών του Privacy Manager και των αξιόπιστων επαφών

Για επαναφορά των πιστοποιητικών του Privacy Manager και των αξιόπιστων επαφών σε ένα διαφορετικό υπολογιστή ως μέρος της διαδικασίας μετεγκατάστασης ή στον ίδιο υπολογιστή, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε το Privacy Manager και επιλέξτε **Migration** (Μετεγκατάσταση).
2. Επιλέξτε **Restore** (Επαναφορά).
3. Στη σελίδα Migration File (Αρχείο μετεγκατάστασης), κάντε κλικ στην επιλογή **Browse** (Αναζήτηση) για αναζήτηση του αρχείου και επιλέξτε **Next** (Επόμενο).

4. Πληκτρολογήστε τον κωδικό πρόσβασης που χρησιμοποιήσατε κατά τη δημιουργία του αρχείου αντιγράφου ασφαλείας και κάντε κλικ στο κουμπί **Next** (Επόμενο).

5. Στη σελίδα Migration File (Αρχείο μετεγκατάστασης), κάντε κλικ στην επιλογή **Finish** (Τέλος).

Κεντρική διαχείριση του Privacy Manager

Η εγκατάσταση του Privacy Manager μπορεί να αποτελεί μέρος μιας κεντρικής εγκατάστασης, που έχει προσαρμοστεί από το διαχειριστή σας. Μία ή περισσότερες από τις παρακάτω λειτουργίες μπορεί να είναι είτε ενεργοποιημένες είτε απενεργοποιημένες:

- **Certificate use policy** (Πολιτική χρήσης πιστοποιητικού) — Μπορεί να περιορίζεστε στη χρήση πιστοποιητικών του Privacy Manager που έχουν εκδοθεί από την Comodo ή μπορεί να σας επιτρέπεται η χρήση ψηφιακών πιστοποιητικών από άλλες αρχές έκδοσης.
- **Encryption policy** (Πολιτική κρυπτογράφησης) — Οι δυνατότητες κρυπτογράφησης μπορεί να είναι μεμονωμένα ενεργοποιημένες ή απενεργοποιημένες στο Microsoft Office ή στο Outlook και στο Windows Live Messenger.

9 File Sanitizer for HP ProtectTools

Το File Sanitizer είναι ένα εργαλείο που επιτρέπει τον ασφαλή τεμαχισμό των αρχείων σας (προσωπικές πληροφορίες ή αρχεία, δεδομένα ιστορικού ή δεδομένα σχετικά με το web ή άλλα στοιχεία δεδομένων) στον υπολογιστή σας και τον περιοδικό καθαρισμό του σκληρού σας δίσκου.

ΣΗΜΕΙΩΣΗ Αυτή η έκδοση του File Sanitizer υποστηρίζει μόνο το σκληρό δίσκο του συστήματος.

Τεμαχισμός

Ο τεμαχισμός είναι διαφορετικός από την τυπική διαγραφή των Windows® (επίσης γνωστή και ως απλή διαγραφή στο File Sanitizer) καθώς όταν τεμαχίζετε ένα στοιχείο με το File Sanitizer, πραγματοποιείται ανάκληση ενός αλγόριθμου που αποκρύπτει τα δεδομένα, καθιστώντας σχεδόν αδύνατη την επαναφορά του αρχικού στοιχείου. Η απλή διαγραφή των Windows μπορεί να αφήσει το αρχείο (ή το στοιχείο) άθικτο στο σκληρό δίσκο ή σε κατάσταση όπου οι κλασικές μέθοδοι μπορούν να χρησιμοποιηθούν για την επαναφορά του αρχείου (ή του στοιχείου).

Μόλις επιλέξετε ένα αρχείο τεμαχισμού (Υψηλής ασφάλειας, μεσαίας ασφάλειας ή χαμηλής ασφάλειας), επιλέγεται αυτόματα μια προκαθορισμένη λίστα στοιχείων και μια μέθοδος διαγραφής για τον τεμαχισμό. Μπορείτε επίσης να διαμορφώσετε ένα προφίλ τεμαχισμού, που σας επιτρέπει να καθορίσετε τον αριθμό των κύκλων τεμαχισμού, τα στοιχεία που θα συμπεριλαμβάνονται στον τεμαχισμό, τα αρχεία που χρειάζονται επιβεβαίωση πριν από τον τεμαχισμό και τα αρχεία που θα εξαιρεθούν από τον τεμαχισμό. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Επιλογή ή δημιουργία ενός προφίλ τεμαχισμού στη σελίδα 72.

Μπορείτε να ρυθμίσετε ένα αυτόματο πρόγραμμα τεμαχισμού και μπορείτε επίσης να τεμαχίζετε στοιχεία μη αυτόματα όποτε το επιθυμείτε. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Ρύθμιση προγράμματος τεμαχισμού στη σελίδα 71, Μη αυτόματος τεμαχισμός ενός στοιχείου στη σελίδα 76 ή Μη αυτόματος τεμαχισμός όλων των επιλεγμένων στοιχείων στη σελίδα 77.

ΣΗΜΕΙΩΣΗ Ένα αρχείο .dll μπορεί να τεμαχιστεί και να αφαιρεθεί από το σύστημα μόνο εάν έχει μετακινηθεί στον κάδο ανακύκλωσης.

Καθαρισμός ελεύθερου χώρου

Η διαγραφή ενός στοιχείου στα Windows δεν αφαιρεί εντελώς τα περιεχόμενα του στοιχείου από το σκληρό δίσκο σας. Τα Windows διαγράφουν μόνο την αναφορά στο στοιχείο. Τα περιεχόμενα του στοιχείου παραμένουν στο σκληρό δίσκο μέχρι ένα άλλο στοιχείο να αντικαταστήσει την ίδια περιοχή στο σκληρό δίσκο με νέες πληροφορίες.

Ο καθαρισμός του ελεύθερου χώρου επιτρέπει την ασφαλή εγγραφή τυχαίων δεδομένων πάνω σε διαγραμμένα στοιχεία, αποτρέποντας τους χρήστες από την προβολή των αρχικών περιεχομένων του διαγραμμένου στοιχείου.

ΣΗΜΕΙΩΣΗ Ο καθαρισμός του ελεύθερου χώρου αφορά αυτά τα στοιχεία που διαγράφετε μέσω του Κάδου ανακύκλωσης των Windows ή όταν διαγράφετε ένα στοιχείο μη αυτόματα. Ο καθαρισμός του ελεύθερου χώρου δεν προσφέρει επιπλέον ασφάλεια στα τεμαχισμένα στοιχεία.

Μπορείτε να ρυθμίσετε ένα αυτόματο πρόγραμμα καθαρισμού του ελεύθερου χώρου ή μπορείτε να ενεργοποιήσετε τον καθαρισμό του ελεύθερου χώρου μη αυτόματα χρησιμοποιώντας το εικονίδιο **HP ProtectTools** στην περιοχή ειδοποιήσεων, στο δεξί άκρο της γραμμής εργασιών. Για περισσότερες πληροφορίες, ανατρέξτε στην ενότητα Ρύθμιση ενός προγράμματος καθαρισμού του ελεύθερου χώρου στη σελίδα 72 ή Μη αυτόματη ενεργοποίηση του καθαρισμού ελεύθερου χώρου στη σελίδα 77.

Διαδικασίες εγκατάστασης

Άνοιγμα του File Sanitizer

Για άνοιγμα του File Sanitizer:

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Security Manager**.
2. Κάντε κλικ στην επιλογή **File Sanitizer**.

– ή –

- Κάντε διπλό κλικ στο εικονίδιο **File Sanitizer** που βρίσκεται στην επιφάνεια εργασίας.

– ή –

- Κάντε δεξί κλικ στο εικονίδιο του **HP ProtectTools** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών, επιλέξτε **File Sanitizer** και, στη συνέχεια, κάντε κλικ στην επιλογή **Open File Sanitizer** (Άνοιγμα του File Sanitizer).

Ρύθμιση προγράμματος τεμαχισμού

ΣΗΜΕΙΩΣΗ Για πληροφορίες σχετικά με την επιλογή ενός προκαθορισμένου προφίλ τεμαχισμού ή με τη δημιουργία ενός προφίλ τεμαχισμού, ανατρέξτε στην ενότητα Επιλογή ή δημιουργία ενός προφίλ τεμαχισμού στη σελίδα 72.

ΣΗΜΕΙΩΣΗ Για πληροφορίες σχετικά με το μη αυτόματο τεμαχισμό στοιχείων, ανατρέξτε στην ενότητα Μη αυτόματος τεμαχισμός ενός στοιχείου στη σελίδα 76 .

1. Ανοίξτε το File Sanitizer και επιλέξτε **Shred** (Τεμαχισμός).
2. Ενεργοποιήστε μια επιλογή τεμαχισμού:
   - **Windows shutdown** (Τερματισμός των Windows) — Ενεργοποιήστε αυτή την επιλογή για τεμαχισμό όλων των επιλεγμένων στοιχείων κατά τον τερματισμό των Windows.

     ΣΗΜΕΙΩΣΗ Όταν είναι ενεργοποιημένη αυτή η επιλογή, εμφανίζεται ένα πλαίσιο διαλόγου κατά τον τερματισμό, που σας ρωτά εάν επιθυμείτε να συνεχίσετε με τον τεμαχισμό επιλεγμένων στοιχείων ή εάν επιθυμείτε να παρακάμψετε τη διαδικασία. Κάντε κλικ στην επιλογή **Yes** (Ναι) για παράκαμψη της διαδικασίας τεμαχισμού ή κάντε κλικ στην επιλογή **No** (Όχι) για συνέχιση του τεμαχισμού.

   - **Web browser open** (Άνοιγμα προγράμματος περιήγησης στο Web) — Ενεργοποιήστε αυτή την επιλογή για τεμαχισμό όλων των επιλεγμένων στοιχείων που σχετίζονται με το web, όπως το ιστορικό URL του προγράμματος περιήγησης, όταν ανοίγετε ένα πρόγραμμα περιήγησης στο web.
   - **Web browser quit** (Κλείσιμο προγράμματος περιήγησης στο Web) — Ενεργοποιήστε αυτή την επιλογή για τεμαχισμό όλων των επιλεγμένων στοιχείων που σχετίζονται με το web, όπως το ιστορικό URL του προγράμματος περιήγησης, όταν κλείνετε ένα πρόγραμμα περιήγησης στο Web.

- **Key sequence** (Ακολουθία πλήκτρων) — Ενεργοποιήστε αυτή την επιλογή για έναρξη του τεμαχισμού με χρήση μιας ακολουθίας πλήκτρων.
- **Scheduler** (Χρονοδιάγραμμα) — Επιλέξτε το πλαίσιο ελέγχου **Activate Scheduler** (Ενεργοποίηση χρονοδιαγράμματος), πληκτρολογήστε τον κωδικό πρόσβασης των Windows και, στη συνέχεια, εισαγάγετε ημέρα και ώρα για τον τεμαχισμό των επιλεγμένων στοιχείων.

ΣΗΜΕΙΩΣΗ Ένα αρχείο .dll μπορεί να τεμαχιστεί και να αφαιρεθεί από το σύστημα μόνο εάν έχει μετακινηθεί στον κάδο ανακύκλωσης.

3. Κάντε κλικ στο **Apply** (Εφαρμογή) και έπειτα στο **OK**.

Ρύθμιση ενός προγράμματος καθαρισμού του ελεύθερου χώρου

ΣΗΜΕΙΩΣΗ Ο καθαρισμός του ελεύθερου χώρου αφορά τα στοιχεία που διαγράφετε μέσω του Κάδου ανακύκλωσης των Windows ή τη μη αυτόματη διαγραφή στοιχείων. Ο καθαρισμός του ελεύθερου χώρου δεν προσφέρει επιπλέον ασφάλεια στα τεμαχισμένα στοιχεία.

Για ρύθμιση ενός προγράμματος καθαρισμού του ελεύθερου χώρου:

1. Ανοίξτε το File Sanitizer και επιλέξτε **Free Space Bleaching** (Καθαρισμός ελεύθερου χώρου).
2. Επιλέξτε το πλαίσιο ελέγχου **Activate Scheduler** (Ενεργοποίηση χρονοδιαγράμματος), πληκτρολογήστε τον κωδικό πρόσβασης των Windows και, στη συνέχεια, εισαγάγετε ημέρα και ώρα για τον τεμαχισμό των επιλεγμένων στοιχείων.
3. Κάντε κλικ στο **Apply** (Εφαρμογή) και έπειτα στο **OK**.

ΣΗΜΕΙΩΣΗ Η διαδικασία καθαρισμού του ελεύθερου χώρου μπορεί να διαρκέσει μεγάλο χρονικό διάστημα. Παρόλο που ο καθαρισμός του ελεύθερου χώρου πραγματοποιείται στο παρασκήνιο, η λειτουργία του υπολογιστή σας μπορεί να επιβραδυνθεί λόγω αυξημένης χρήσης του επεξεργαστή.

Επιλογή ή δημιουργία ενός προφίλ τεμαχισμού

Μπορείτε να καθορίσετε μια μέθοδο διαγραφής και να επιλέξετε τα στοιχεία για τεμαχισμό επιλέγοντας ένα προκαθορισμένο προφίλ ή δημιουργώντας το δικό σας προφίλ.

Επιλογή ενός προκαθορισμένου προφίλ τεμαχισμού

Μόλις επιλέξετε ένα προκαθορισμένο αρχείο τεμαχισμού (Υψηλής ασφαλείας, Μεσαίας ασφαλείας ή Χαμηλής Ασφαλείας), επιλέγεται αυτόματα μια προκαθορισμένη μέθοδος διαγραφής και μια λίστα στοιχείων. Μπορείτε να κάνετε κλικ στο κουμπί **View Details** (Προβολή λεπτομερειών) για προβολή της προκαθορισμένης λίστας στοιχείων που έχουν επιλεγεί για τεμαχισμό.

Για επιλογή ενός προκαθορισμένου προφίλ τεμαχισμού:

1. Ανοίξτε το File Sanitizer και επιλέξτε **Settings** (Ρυθμίσεις).
2. Κάντε κλικ σε ένα προκαθορισμένο προφίλ τεμαχισμού.
3. Κάντε κλικ στην επιλογή **View Details** (Προβολή λεπτομερειών) για προβολή της λίστας στοιχείων που έχουν επιλεγεί για τεμαχισμό.
4. Στην περιοχή **Shred the following** (Τεμαχισμός των παρακάτω), επιλέξτε το πλαίσιο ελέγχου δίπλα στο κάθε στοιχείο που επιθυμείτε να επιβεβαιώσετε πριν από τον τεμαχισμό.
5. Κάντε κλικ στο **Apply** (Εφαρμογή) και έπειτα στο **OK**.

Διαμόρφωση ενός προφίλ τεμαχισμού

Όταν δημιουργείτε ένα προφίλ τεμαχισμού, καθορίσετε τον αριθμό των κύκλων τεμαχισμού, τα στοιχεία που θα συμπεριλαμβάνονται στον τεμαχισμό, τα αρχεία που χρειάζονται επιβεβαίωση πριν από τον τεμαχισμό και τα αρχεία που θα εξαιρεθούν από τον τεμαχισμό:

1. Ανοίξτε το File Sanitizer, επιλέξτε **Settings** (Ρυθμίσεις), κάντε κλικ στην επιλογή **Advanced Security Settings** (Προηγμένες ρυθμίσεις ασφαλείας) και επιλέξτε **View Details** (Προβολή λεπτομερειών).

2. Καθορίστε τον αριθμό των κύκλων τεμαχισμού.

ΣΗΜΕΙΩΣΗ Ο επιλεγμένος αριθμός των κύκλων τεμαχισμού θα πραγματοποιείται για κάθε στοιχείο. Για παράδειγμα, εάν επιλέξετε 3 κύκλους τεμαχισμού, ένας αλγόριθμος που αποκρύπτει τα δεδομένα εκτελείται 3 ξεχωριστές φορές. Εάν επιλέξετε τους κύκλους τεμαχισμού υψηλής ασφάλειας, ο τεμαχισμός ενδέχεται να διαρκέσει για μεγάλο χρονικό διάστημα, ωστόσο, όσο μεγαλύτερος είναι ο αριθμός των κύκλων τεμαχισμού που θα καθορίσετε, τόσο λιγότερο πιθανή είναι η ανάκτηση των δεδομένων.

3. Επιλέξτε τα στοιχεία που επιθυμείτε να τεμαχίσετε:

   α. Στην περιοχή **Available shred options** (Διαθέσιμες επιλογές τεμαχισμού), κάντε κλικ σε ένα στοιχείο και επιλέξτε **Add** (Προσθήκη).

   β. Για προσθήκη ενός προσαρμοσμένου στοιχείου, κάντε κλικ στην επιλογή **Add Custom Option** (Προσθήκη προσαρμοσμένης επιλογής) και, στη συνέχεια, αναζητήστε ή πληκτρολογήστε τη διαδρομή στο όνομα αρχείου ή το φάκελο. Κάντε κλικ στο **Open** (Άνοιγμα) και έπειτα στο **OK**. Στην περιοχή **Available shred options** (Διαθέσιμες επιλογές τεμαχισμού), κάντε κλικ στο προσαρμοσμένο στοιχείο και επιλέξτε **Add** (Προσθήκη).

ΣΗΜΕΙΩΣΗ Για αφαίρεση ενός στοιχείου από τις διαθέσιμες επιλογές τεμαχισμού, κάντε κλικ στο στοιχείο και επιλέξτε **Delete** (Διαγραφή).

4. Στην περιοχή **Shred the following** (Τεμαχισμός των παρακάτω), επιλέξτε το πλαίσιο ελέγχου δίπλα στο κάθε στοιχείο που επιθυμείτε να επιβεβαιώσετε πριν από τον τεμαχισμό

ΣΗΜΕΙΩΣΗ Για αφαίρεση ενός στοιχείου από τη λίστα τεμαχισμού, κάντε κλικ στο στοιχείο και επιλέξτε **Remove** (Αφαίρεση).

5. Για την προστασία των αρχείων ή φακέλων από αυτόματο τεμαχισμό, στην περιοχή **Do not shred the following** (Μην τεμαχίσετε τα παραπάνω), κάντε κλικ στην επιλογή **Add** (Προσθήκη) και, στη συνέχεια, αναζητήστε ή πληκτρολογήστε τη διαδρομή στο όνομα αρχείου ή το φάκελο. Κάντε κλικ στο **Open** (Άνοιγμα) και έπειτα στο **OK**.

ΣΗΜΕΙΩΣΗ Για αφαίρεση ενός στοιχείου από τη λίστα εξαιρέσεων, κάντε κλικ στο στοιχείο και επιλέξτε **Delete** (Διαγραφή).

6. Όταν ολοκληρώσετε τη διαμόρφωση του προφίλ τεμαχισμού, κάντε κλικ στην επιλογή **Apply** (Εφαρμογή) και επιλέξτε **OK**.

Διαμόρφωση ενός προφίλ απλής διαγραφής

Το προφίλ απλής διαγραφής πραγματοποιεί μια τυπική διαγραφή στοιχείων χωρίς τεμαχισμό. Όταν διαμορφώνετε ένα προφίλ απλής διαγραφής, καθορίζετε τα στοιχεία που θα συμπεριληφθούν στην απλή διαγραφή, τα στοιχεία που θα επιβεβαιωθούν προτού πραγματοποιηθεί μια απλή διαγραφή και τα στοιχεία που θα εξαιρεθούν από μια απλή διαγραφή.

ΣΗΜΕΙΩΣΗ Εάν χρησιμοποιήσετε την επιλογή απλής διαγραφής, ο καθαρισμός του ελεύθερου χώρου μπορεί να πραγματοποιείται τακτικά στα στοιχεία που έχουν διαγραφεί μη αυτόματα ή με χρήση του Κάδου ανακύκλωσης των Windows.

Για διαμόρφωση ενός προφίλ απλής διαγραφής:

1. Ανοίξτε το File Sanitizer, επιλέξτε **Settings** (Ρυθμίσεις), κάντε κλικ στην επιλογή **Simple Delete Setting** (Ρύθμιση απλής διαγραφής) και επιλέξτε **View Details** (Προβολή λεπτομερειών).
2. Επιλέξτε τα στοιχεία που επιθυμείτε να διαγράψετε:
   α. Στην περιοχή **Available delete options** (Διαθέσιμες επιλογές διαγραφής), κάντε κλικ σε ένα στοιχείο και επιλέξτε **Add** (Προσθήκη).
   β. Για προσθήκη ενός προσαρμοσμένου στοιχείου, επιλέξτε **Add Custom Option** (Προσθήκη προσαρμοσμένης επιλογής), πληκτρολογήστε ένα όνομα αρχείου ή φακέλου και κάντε κλικ στο **OK**. Κάντε κλικ στο προσαρμοσμένο στοιχείο και έπειτα κάντε κλικ στην επιλογή **Add** (Προσθήκη).

   ΣΗΜΕΙΩΣΗ Για διαγραφή ενός στοιχείου από τις διαθέσιμες επιλογές διαγραφής, κάντε κλικ στο στοιχείο και επιλέξτε **Delete** (Διαγραφή).
3. Στην περιοχή **Delete the following** (Διαγραφή των παρακάτω), επιλέξτε το πλαίσιο ελέγχου δίπλα στο κάθε στοιχείο που επιθυμείτε να επιβεβαιώσετε πριν από τη διαγραφή.

   ΣΗΜΕΙΩΣΗ Για αφαίρεση ενός στοιχείου από τη λίστα διαγραφής, κάντε κλικ στο στοιχείο και επιλέξτε **Remove** (Αφαίρεση).
4. Στην περιοχή **Do not delete the following** (Μην διαγράψετε τα παρακάτω), επιλέξτε **Add** (Προσθήκη) για επιλογή των συγκεκριμένων στοιχείων που επιθυμείτε να εξαιρέσετε από τον τεμαχισμό.

   ΣΗΜΕΙΩΣΗ Για αφαίρεση ενός στοιχείου από τη λίστα εξαιρέσεων, κάντε κλικ στο στοιχείο και επιλέξτε **Delete** (Διαγραφή).
5. Όταν ολοκληρώσετε τη διαμόρφωση του προφίλ απλής διαγραφής, κάντε κλικ στην επιλογή **Apply** (Εφαρμογή) και επιλέξτε **OK**.

Γενικές εργασίες

Μπορείτε να χρησιμοποιήσετε το File Sanitizer για να εκτελέσετε τις παρακάτω διαδικασίες:

- Use a key sequence to initiate shredding (Χρήση μιας ακολουθίας πλήκτρων για εκκίνηση του τεμαχισμού) — Αυτή η λειτουργία σάς επιτρέπει να δημιουργήσετε μια ακολουθία πλήκτρων (για παράδειγμα, ctrl+alt+s) για εκκίνηση του τεμαχισμού. Για λεπτομέρειες, ανατρέξτε στην ενότητα Χρήση μιας ακολουθίας πλήκτρων για εκκίνηση του τεμαχισμού στη σελίδα 75.
- Use the File Sanitizer icon to initiate shredding (Χρήση του εικονιδίου File Sanitizer για εκκίνηση του τεμαχισμού) — Αυτή η λειτουργία είναι παρόμοια με τη λειτουργία μεταφοράς και απόθεσης των Windows. Για λεπτομέρειες, ανατρέξτε στην ενότητα Χρήση του εικονιδίου File Sanitizer στη σελίδα 76.
- Manually shred a specific asset or all selected assets (Μη αυτόματος τεμαχισμός ενός συγκεκριμένου στοιχείου ή όλων των επιλεγμένων στοιχείων) — Αυτές οι λειτουργίες επιτρέπουν το μη αυτόματο τεμαχισμό στοιχείων χωρίς να χρειάζεται να περιμένετε την πραγματοποίηση του τακτικού προγράμματος τεμαχισμού. Για λεπτομέρειες, ανατρέξτε στην ενότητα Μη αυτόματος τεμαχισμός ενός στοιχείου στη σελίδα 76 ή Μη αυτόματος τεμαχισμός όλων των επιλεγμένων στοιχείων στη σελίδα 77.
- Manually activate free space bleaching (Μη αυτόματη ενεργοποίηση του καθαρισμού ελεύθερου χώρου) — Αυτή η λειτουργία επιτρέπει τη μη αυτόματη ενεργοποίηση του καθαρισμού ελεύθερου χώρου. Για λεπτομέρειες, ανατρέξτε στην ενότητα Μη αυτόματη ενεργοποίηση του καθαρισμού ελεύθερου χώρου στη σελίδα 77.
- Abort a shred or free space bleaching operation (Ματαίωση μιας λειτουργίας καθαρισμού ελεύθερου χώρου) — Αυτή η λειτουργία επιτρέπει τη διακοπή του τεμαχισμού ή της διαδικασίας καθαρισμού του ελεύθερου χώρου. Για λεπτομέρειες, ανατρέξτε στην ενότητα Ματαίωση μιας λειτουργίας τεμαχισμού ή καθαρισμού ελεύθερου χώρου στη σελίδα 77.
- View the log files (Προβολή των αρχείων καταγραφής δεδομένων) — Αυτή η λειτουργία επιτρέπει την προβολή των αρχείων καταγραφής δεδομένων τεμαχισμού και καθαρισμού του ελεύθερου χώρου, που περιέχουν τυχόν σφάλματα ή αποτυχίες από την τελευταία λειτουργία τεμαχισμού ή καθαρισμού του ελεύθερου χώρου. Για λεπτομέρειες, ανατρέξτε στην ενότητα Προβολή των αρχείων καταγραφής δεδομένων στη σελίδα 77.

ΣΗΜΕΙΩΣΗ Η διαδικασία τεμαχισμού ή καθαρισμού του ελεύθερου χώρου ενδέχεται να διαρκέσει για μεγάλο χρονικό διάστημα. Παρόλο που ο τεμαχισμός και ο καθαρισμός του ελεύθερου χώρου πραγματοποιούνται στο παρασκήνιο, η λειτουργία του υπολογιστή σας μπορεί να επιβραδυνθεί λόγω αυξημένης χρήσης του επεξεργαστή.

Χρήση μιας ακολουθίας πλήκτρων για εκκίνηση του τεμαχισμού

Για καθορισμό μιας ακολουθίας πλήκτρων, ακολουθήστε τα εξής βήματα:

1. Ανοίξτε το File Sanitizer και επιλέξτε **Shred** (Τεμαχισμός).
2. Επιλέξτε το πλαίσιο ελέγχου **Key sequence** (Ακολουθία πλήκτρων).
3. Πληκτρολογήστε ένα χαρακτήρα στο διαθέσιμο πλαίσιο.
4. Επιλέξτε είτε το πλαίσιο **CTRL** είτε το πλαίσιο **ALT** και, στη συνέχεια, επιλέξτε το πλαίσιο **SHIFT**.

   Για παράδειγμα, για εκκίνηση του αυτόματου τεμαχισμού χρησιμοποιήστε το πλήκτρο s και το συνδυασμό ctrl+shift, πληκτρολογήστε s στο πλαίσιο και, στη συνέχεια, επιλέξτε **CTRL** και **SHIFT**.

ΣΗΜΕΙΩΣΗ Βεβαιωθείτε ότι έχετε επιλέξει μια ακολουθία πλήκτρων διαφορετική από τις άλλες ακολουθίες πλήκτρων που έχετε διαμορφώσει.

Για εκκίνηση του τεμαχισμού με τη χρήση μιας ακολουθίας πλήκτρων:

1. Κρατήστε πατημένο το πλήκτρο shift και το πλήκτρο ctrl ή το πλήκτρο alt (ή οποιοδήποτε συνδυασμό καθορίσατε) ενώ πατάτε τον επιλεγμένο χαρακτήρα.
2. Εάν ανοίξει ένα πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

Χρήση του εικονιδίου File Sanitizer

△ **ΠΡΟΣΟΧΗ** Δεν είναι δυνατή η επαναφορά των τεμαχισμένων στοιχείων. Επιλέξτε προσεκτικά τα στοιχεία που επιθυμείτε να τεμαχίσετε μη αυτόματα.

1. Πλοηγηθείτε στο έγγραφο ή το φάκελο που επιθυμείτε να τεμαχίσετε.
2. Σύρετε το στοιχείο στο εικονίδιο File Sanitizer στην επιφάνεια εργασίας.
3. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

Μη αυτόματος τεμαχισμός ενός στοιχείου

△ **ΠΡΟΣΟΧΗ** Δεν είναι δυνατή η επαναφορά των τεμαχισμένων στοιχείων. Επιλέξτε προσεκτικά τα στοιχεία που επιθυμείτε να τεμαχίσετε μη αυτόματα.

1. Κάντε δεξί κλικ στο εικονίδιο του **HP ProtectTools** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών, επιλέξτε **File Sanitizer** και, στη συνέχεια, κάντε κλικ στην επιλογή **Shred One** (Τεμαχισμός ενός).
2. Όταν ανοίξει ένα πλαίσιο διαλόγου Browse (Αναζήτηση), πλοηγηθείτε στο στοιχείο που επιθυμείτε να τεμαχίσετε και επιλέξτε **OK**.

ΣΗΜΕΙΩΣΗ Το στοιχείο που θα επιλέξετε μπορεί να είναι ένα αρχείο ή φάκελος.

3. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

– ή –

1. Κάντε δεξί κλικ στο εικονίδιο **File Sanitizer** στην επιφάνεια εργασίας και επιλέξτε **Shred One** (Τεμαχισμός ενός).
2. Όταν ανοίξει ένα πλαίσιο διαλόγου Browse (Αναζήτηση), πλοηγηθείτε στο στοιχείο που επιθυμείτε να τεμαχίσετε και επιλέξτε **OK**.
3. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

– ή –

1. Ανοίξτε το File Sanitizer και επιλέξτε **Shred** (Τεμαχισμός).
2. Κάντε κλικ στο κουμπί **Browse** (Αναζήτηση).
3. Όταν ανοίξει ένα πλαίσιο διαλόγου Browse (Αναζήτηση), πλοηγηθείτε στο στοιχείο που επιθυμείτε να τεμαχίσετε και επιλέξτε **OK**.
4. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

Μη αυτόματος τεμαχισμός όλων των επιλεγμένων στοιχείων

1. Κάντε δεξί κλικ στο εικονίδιο του **HP ProtectTools** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών, επιλέξτε **File Sanitizer** και, στη συνέχεια, κάντε κλικ στην επιλογή **Shred Now** (Τεμαχισμός τώρα).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

– ή –

1. Κάντε δεξί κλικ στο εικονίδιο **File Sanitizer** στην επιφάνεια εργασίας και επιλέξτε **Shred Now** (Τεμαχισμός τώρα).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

– ή –

1. Ανοίξτε το File Sanitizer και επιλέξτε **Shred** (Τεμαχισμός).
2. Κάντε κλικ στο κουμπί **Shred now** (Τεμαχισμός τώρα).
3. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

Μη αυτόματη ενεργοποίηση του καθαρισμού ελεύθερου χώρου

1. Κάντε δεξί κλικ στο εικονίδιο του **HP ProtectTools** στην περιοχή ειδοποιήσεων, στη δεξιά πλευρά της γραμμής εργασιών, επιλέξτε **File Sanitizer** και, στη συνέχεια, κάντε κλικ στην επιλογή **Bleach Now** (Καθαρισμός τώρα).
2. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

– ή –

1. Ανοίξτε το File Sanitizer και επιλέξτε **Free Space Bleaching** (Καθαρισμός ελεύθερου χώρου).
2. Κάντε κλικ στην επιλογή **Bleach Now** (Καθαρισμός τώρα).
3. Όταν ανοίξει το πλαίσιο διαλόγου επιβεβαίωσης, κάντε κλικ στο **Yes** (Ναι).

Ματαίωση μιας λειτουργίας τεμαχισμού ή καθαρισμού ελεύθερου χώρου

Όταν πραγματοποιείται μια λειτουργία τεμαχισμού ή καθαρισμού ελεύθερου χώρου, εμφανίζεται ένα μήνυμα πάνω από το εικονίδιο HP ProtectTools Security Manager στην περιοχή ειδοποιήσεων. Το μήνυμα παρέχει πληροφορίες σχετικά με τη διαδικασία τεμαχισμού ή καθαρισμού ελεύθερου χώρου (ολοκλήρωση ποσοστού) και προσφέρει την επιλογή ματαίωσης της λειτουργίας.

Για ματαίωση της λειτουργίας:

▲ Κάντε κλικ στο μήνυμα και επιλέξτε **Stop** (Διακοπή) για ακύρωση της λειτουργίας.

Προβολή των αρχείων καταγραφής δεδομένων

Κάθε φορά που πραγματοποιείται μια λειτουργία τεμαχισμού ή καθαρισμού του ελεύθερου χώρου, δημιουργούνται αρχεία καταγραφής δεδομένων σφαλμάτων ή αποτυχιών. Τα αρχεία καταγραφής δεδομένων ενημερώνονται πάντα σύμφωνα με την τελευταία λειτουργία τεμαχισμού ή καθαρισμού του ελεύθερου χώρου.

ΣΗΜΕΙΩΣΗ Τα αρχεία που τεμαχίζονται ή καθαρίζονται με επιτυχία δεν εμφανίζονται στα αρχεία καταγραφής δεδομένων.

Δημιουργείται ένα αρχείο καταγραφής δεδομένων για λειτουργίες τεμαχισμού και άλλο αρχείο καταγραφής δεδομένων για λειτουργίες καθαρισμού του ελεύθερου χώρου. Και τα δύο αρχεία καταγραφής δεδομένων βρίσκονται στο σκληρό δίσκο στη διαδρομή:

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

10 Device Access Manager for HP ProtectTools (μόνο σε επιλεγμένα μοντέλα)

Οι διαχειριστές του λειτουργικού συστήματος Windows® χρησιμοποιούν το Device Access Manager for HP ProtectTools για έλεγχο της πρόσβασης στις συσκευές σε ένα σύστημα και για προστασία ενάντια σε μη εξουσιοδοτημένη χρήση:

- Δημιουργούνται προφίλ συσκευής για κάθε χρήστη για καθορισμό των συσκευών στις οποίες επιτρέπεται ή απαγορεύεται η άδεια πρόσβασης.
- Οι χρήστες μπορούν επίσης να οργανωθούν σε ομάδες, όπως η καθορισμένη ομάδα διαχειριστών συσκευής (Device Administrator) ή οι ομάδες είναι δυνατό να καθοριστούν με χρήση της επιλογής διαχείρισης υπολογιστή στην ενότητα "Εργαλεία Διαχείρισης" του Πίνακα Ελέγχου.
- Η πρόσβαση σε συσκευές μπορεί να επιτραπεί ή απαγορευτεί βάσει της ιδιότητας μέλους μιας ομάδας.
- Για κλάσεις συσκευών όπως οι μονάδες CD-ROM και οι μονάδες DVD, η πρόσβαση ανάγνωσης και η πρόσβαση εγγραφής μπορεί να επιτρέπονται ή να απαγορεύονται ξεχωριστά.

Μπορεί επίσης να δοθεί άδεια ανάγνωσης και τροποποίησης της πολιτικής ελέγχου πρόσβασης της συσκευής σε χρήστες με περιορισμένα δικαιώματα.

Διαδικασίες ρύθμισης

Άνοιγμα του Device Access Manager

Για άνοιγμα του Device Access Manager, ακολουθήστε τα παρακάτω βήματα:

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε διαδοχικά **Όλα τα προγράμματα**, **HP** και τέλος **HP ProtectTools Administrative Console**.
2. Στο αριστερό τμήμα του παραθύρου, επιλέξτε **Device Access Manager**.

Διαμόρφωση πρόσβασης συσκευής

Το Device Access Manager for HP ProtectTools διαθέτει τρεις προβολές:

- Η προβολή Simple Configuration (Απλή διαμόρφωση) χρησιμοποιείται για να επιτρέπει ή να απαγορεύει την πρόσβαση σε μέλη της ομάδας Device Administrators (Διαχειριστές συσκευής).
- Η προβολή Device Class Configuration (Διαμόρφωση κλάσης συσκευής) χρησιμοποιείται για να επιτρέπει ή να απαγορεύει την πρόσβαση σε τύπους συσκευών ή συγκεκριμένες συσκευές για συγκεκριμένους χρήστες ή ομάδες.
- Η προβολή User Access Settings (Ρυθμίσεις πρόσβασης χρήστη) χρησιμοποιείται για τον καθορισμό των χρηστών που μπορούν να προβάλλουν ή να τροποποιήσουν τις πληροφορίες στην προβολή Simple Configuration και Device Class Configuration.

Ομάδα Device administrators (Διαχειριστές συσκευής)

Μόλις πραγματοποιείται εγκατάσταση του Device Access Manager, δημιουργείται μια ομάδα Device Administrators (Διαχειριστές συσκευής).

Ο διαχειριστής του συστήματος μπορεί να εφαρμόσει μια απλή πολιτική ελέγχου πρόσβασης στη συσκευή απαγορεύοντας την πρόσβαση σε ορισμένες κλάσεις συσκευών, εκτός εάν ένας χρήστης ταξινομηθεί ως αξιόπιστος (όσον αφορά την πρόσβαση στο σύστημα). Ο προτεινόμενος τρόπος διαχωρισμού μεταξύ χρηστών "αξιόπιστων για τη συσκευή" και χρηστών "μη αξιόπιστων για τη συσκευή" είναι να γίνουν όλοι οι χρήστες που είναι αξιόπιστοι για τη συσκευή, μέλη της ομάδας Device Administrators (Διαχειριστές συσκευής). Εάν παρέχετε στα μέλη της ομάδας Device Administrators (Διαχειριστές συσκευής) πρόσβαση σε συσκευές μέσω των προβολών Simple Configuration (Απλή διαμόρφωση) ή Device Class Configuration (Διαμόρφωση κλάσεων συσκευών), θα εξασφαλίσετε ότι οι χρήστες που είναι "αξιόπιστοι για τη συσκευή" θα έχουν πλήρη πρόσβαση στο συγκεκριμένο σύνολο κλάσεων συσκευών.

ΣΗΜΕΙΩΣΗ Η προσθήκη ενός χρήστη στην ομάδα των διαχειριστών της συσκευής δεν επιτρέπει αυτόματα στο χρήστη την πρόσβαση σε συσκευές. Ωστόσο, η προβολή Simple Configuration (Απλή διαμόρφωση) μπορεί να χρησιμοποιηθεί για να επιτρέπει την πρόσβαση στις απαιτούμενες κλάσεις συσκευών για χρήστες "αξιόπιστους για τη συσκευή".

Για προσθήκη χρηστών στην ομάδα Device Administrators (Διαχειριστές συσκευής), ακολουθήστε τα εξής βήματα:

- Για Windows 7, Vista ή XP Professional, χρησιμοποιήστε το τυπικό συμπληρωματικό πρόγραμμα MMC "Τοπικοί χρήστες και ομάδες".
- Για εκδόσεις "home" των Windows 7, Vista® ή XP, από ένα λογαριασμό με δικαιώματα, πληκτρολογήστε τα παρακάτω στο παράθυρο γραμμής εντολών:

```
c:\> net localgroup “Device Administrators” username /ADD
```

Απλή διαμόρφωση

Οι διαχειριστές και οι εξουσιοδοτημένοι χρήστες μπορούν να χρησιμοποιήσουν την προβολή Simple Configuration (Απλή διαμόρφωση) για να τροποποιήσουν την πρόσβαση στις ακόλουθες τάξεις συσκευών για όλους όσους δεν είναι διαχειριστές της συσκευής:

ΣΗΜΕΙΩΣΗ Για να μπορείτε να χρησιμοποιήσετε αυτή την προβολή για ανάγνωση των πληροφοριών πρόσβασης της συσκευής, πρέπει να έχει επιτραπεί στο χρήστη ή στην ομάδα η πρόσβαση "ανάγνωσης" στην προβολή **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη). Για να μπορείτε να τροποποιήσετε αυτή την προβολή για ανάγνωση των πληροφοριών πρόσβασης της συσκευής, πρέπει να έχει επιτραπεί στο χρήστη ή στην ομάδα η πρόσβαση "αλλαγής" στην προβολή **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη).

- Όλα τα αφαιρούμενα μέσα (δισκέτες, μονάδες USB flash, κλπ.)
- Όλες οι μονάδες DVD/CD-ROM
- Όλες οι σειριακές και παράλληλες θύρες
- Όλες οι συσκευές Bluetooth®
- Όλες οι συσκευές υπερύθρων
- Όλες οι συσκευές μόντεμ
- Όλες οι συσκευές PCMCIA
- Όλες οι συσκευές 1394

Για να επιτρέπεται ή να απαγορεύεται η πρόσβαση σε μια τάξη συσκευών για όλους όσους δεν είναι διαχειριστές της συσκευής, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Simple Configuration** (Απλή διαμόρφωση).
2. Στο δεξί τμήμα του παραθύρου, για απαγόρευση πρόσβασης, επιλέξτε το πλαίσιο ελέγχου για μια κλάση συσκευών ή μια συγκεκριμένη συσκευή. Απενεργοποιήστε το πλαίσιο ελέγχου για να επιτρέπεται η πρόσβαση σε αυτή την κλάση συσκευών ή συγκεκριμένη συσκευή.

   Εάν ένα πλαίσιο ελέγχου είναι απενεργοποιημένο, οι τιμές που επηρεάζουν το σενάριο πρόσβασης έχουν αλλάξει από την προβολή Device Class Configuration (Διαμόρφωση κλάσης συσκευής). Για επαναφορά των τιμών στις απλές ρυθμίσεις, κάντε κλικ στο πλαίσιο ελέγχου για διαγραφή ή ρύθμισή του και κάντε κλικ στην επιλογή **Yes** (Ναι) για επιβεβαίωση.
3. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

   ΣΗΜΕΙΩΣΗ Εάν δεν εκτελείται υπηρεσία παρασκηνίου, θα ανοίξει ένα παράθυρο διαλόγου για να σας ρωτήσει εάν θέλετε να πραγματοποιήσετε εκκίνησή του. Κάντε κλικ στο **Yes** (Ναι).
4. Κάντε κλικ στο **OK**.

Έναρξη υπηρεσίας παρασκηνίου

Προτού να μπορούν να εφαρμοστούν τα προφίλ συσκευής, το HP ProtectTools Security Manager ανοίγει ένα παράθυρο διαλόγου για να σας ρωτήσει εάν θέλετε να πραγματοποιήσετε εκκίνηση της υπηρεσίας παρασκηνίου HP ProtectTools Device Locking/Auditing. Κάντε κλικ στο **Yes** (Ναι). Η υπηρεσία παρασκηνίου θα ξεκινήσει και από τότε θα ξεκινά αυτόματα κάθε φορά που θα πραγματοποιείται εκκίνηση του συστήματος.

ΣΗΜΕΙΩΣΗ Πρέπει να καθοριστεί ένα προφίλ συσκευής προτού εμφανιστεί το μήνυμα προτροπής της υπηρεσίας παρασκηνίου.

Οι διαχειριστές μπορούν επίσης να πραγματοποιήσουν εκκίνηση ή διακοπή αυτής της υπηρεσίας:

1. Κάντε κλικ στο κουμπί **Έναρξη** και επιλέξτε **Πίνακας Ελέγχου**.
2. Κάντε κλικ στην επιλογή **Εργαλεία Διαχείρισης** και επιλέξτε **Υπηρεσίες**.
3. Αναζητήστε την υπηρεσία **HP ProtectTools Device Locking/Auditing**.

Η διακοπή της υπηρεσίας κλειδώματος/ελέγχου συσκευών δεν θα διακόψει το κλείδωμα της συσκευής. Δύο στοιχεία ενισχύουν το κλείδωμα της συσκευής:

- Υπηρεσία κλειδώματος/ελέγχου συσκευών
- Πρόγραμμα οδήγησης DAMDrv.sys

Με την εκκίνηση της υπηρεσίας πραγματοποιείται εκκίνηση και του προγράμματος οδήγησης της συσκευής, αλλά με τη διακοπή της υπηρεσίας δεν διακόπτεται και το πρόγραμμα οδήγησης.

Για να καθορίσετε εάν εκτελείται η υπηρεσία παρασκηνίου, ανοίξτε ένα παράθυρο γραμμής εντολών και πληκτρολογήστε sc query flcdlock.

Για να καθορίσετε εάν εκτελείται η υπηρεσία παρασκηνίου, ανοίξτε ένα παράθυρο γραμμής εντολών και πληκτρολογήστε sc query damdrv.

Διαμόρφωση κλάσης συσκευής

Οι διαχειριστές και οι εξουσιοδοτημένοι χρήστες μπορούν να προβάλλουν και να τροποποιήσουν τις λίστες χρηστών και ομάδων στις οποίες επιτρέπεται ή απαγορεύεται η άδεια πρόσβασης σε κλάσεις συσκευών ή συγκεκριμένες συσκευές.

ΣΗΜΕΙΩΣΗ Για να μπορείτε να χρησιμοποιήσετε αυτή την προβολή για ανάγνωση των πληροφοριών πρόσβασης της συσκευής, πρέπει να έχει επιτραπεί στο χρήστη ή την ομάδα η πρόσβαση "ανάγνωσης" στην προβολή **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη). Για να μπορείτε να τροποποιήσετε αυτή την προβολή για ανάγνωση των πληροφοριών πρόσβασης της συσκευής, πρέπει να έχει επιτραπεί στο χρήστη ή την ομάδα η πρόσβαση "αλλαγής" στην προβολή **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη).

Η προβολή Device Class Configuration (Διαμόρφωση κλάσης συσκευής) διαθέτει τις παρακάτω ενότητες:

- **Device List** (Λίστα συσκευών) — Εμφανίζει όλες τις κλάσεις συσκευών και τις συσκευές που είναι εγκατεστημένες στο σύστημα ή που μπορεί να είχαν εγκατασταθεί στο σύστημα προηγουμένως.
  - Συνήθως εφαρμόζεται προστασία για μια κλάση συσκευών. Ένας επιλεγμένος χρήστης ή ομάδα θα μπορέσει να προσπελάσει οποιαδήποτε συσκευή στην κλάση συσκευών.
  - Προστασία μπορεί να εφαρμόζεται επίσης και σε συγκεκριμένες συσκευές.
- **User List** (Λίστα χρηστών) — Εμφανίζει όλους τους χρήστες και τις ομάδες, στους οποίους επιτρέπεται ή απαγορεύεται η πρόσβαση στην επιλεγμένη κλάση συσκευών ή στη συγκεκριμένη συσκευή.
  - Η καταχώριση στη λίστα χρηστών μπορεί να πραγματοποιηθεί για ένα συγκεκριμένο χρήστη ή για μια ομάδα, στην οποία ο χρήστης είναι μέλος.
  - Εάν μια καταχώριση χρήστη ή ομάδας στη λίστα χρηστών δεν είναι διαθέσιμη, η ρύθμιση έχει μεταβιβαστεί από την κλάση συσκευών στη λίστα συσκευών (Device List) ή από το φάκελο Class (Κλάση).
  - Ορισμένες κλάσεις συσκευών, όπως DVD και CD-ROM, μπορούν να ελέγχονται περαιτέρω επιτρέποντας ή απαγορεύοντας την πρόσβαση ξεχωριστά για τις λειτουργίες ανάγνωσης και εγγραφής.

    Όσον αφορά άλλες συσκευές και κλάσεις, τα δικαιώματα πρόσβασης ανάγνωσης και εγγραφής μπορούν να μεταβιβαστούν. Για παράδειγμα, η πρόσβαση ανάγνωσης μπορεί να μεταβιβαστεί από μια υψηλότερη κλάση, αλλά η πρόσβαση εγγραφής μπορεί να απαγορευτεί ειδικά για ένα χρήστη ή μια ομάδα.

    ΣΗΜΕΙΩΣΗ Εάν το πλαίσιο ελέγχου Read (Ανάγνωση) είναι κενό, τότε η καταχώριση ελέγχου πρόσβασης δεν επιδρά στην πρόσβαση ανάγνωσης της συσκευής. Ούτε επιτρέπει ούτε απαγορεύει την πρόσβαση στη συσκευή.

    Παράδειγμα 1 — Εάν σε ένα χρήστη ή ομάδα απαγορευτεί η πρόσβαση εγγραφής για μια συσκευή ή κλάση συσκευών:

    Στον ίδιο χρήστη, στην ίδια ομάδα ή σε ένα μέλος της ίδιας ομάδας μπορεί να επιτραπεί η πρόσβαση εγγραφής ή μόνο η πρόσβαση ανάγνωσης και εγγραφής για μια συσκευή που βρίσκεται σε χαμηλότερο επίπεδο στην ιεραρχία συσκευών.

    Παράδειγμα 2 — Εάν σε ένα χρήστη ή ομάδα επιτρέπεται η πρόσβαση εγγραφής για μια συσκευή ή κλάση συσκευών:

    Στον ίδιο χρήστη, στην ίδια ομάδα ή σε ένα μέλος της ίδιας ομάδας μπορεί να απαγορευτεί η πρόσβαση εγγραφής ή μόνο η πρόσβαση ανάγνωσης και εγγραφής για την ίδια συσκευή ή για μια συσκευή που βρίσκεται σε χαμηλότερο επίπεδο στην ιεραρχία συσκευών.

    Παράδειγμα 3 — Εάν σε ένα χρήστη ή ομάδα επιτρέπεται η πρόσβαση ανάγνωσης για μια συσκευή ή κλάση συσκευών:

    Στον ίδιο χρήστη, στην ίδια ομάδα ή σε ένα μέλος της ίδιας ομάδας μπορεί να απαγορευτεί η πρόσβαση ανάγνωσης ή μόνο η πρόσβαση ανάγνωσης και εγγραφής για την ίδια συσκευή ή για μια συσκευή που βρίσκεται σε χαμηλότερο επίπεδο στην ιεραρχία συσκευών.

    Παράδειγμα 4 — Εάν σε ένα χρήστη ή ομάδα απαγορευτεί η πρόσβαση ανάγνωσης για μια συσκευή ή κλάση συσκευών:

Στον ίδιο χρήστη, στην ίδια ομάδα, ή σε ένα μέλος της ίδιας ομάδας μπορεί να επιτραπεί η πρόσβαση ανάγνωσης ή μόνο η πρόσβαση ανάγνωσης και εγγραφής για μια συσκευή που βρίσκεται σε χαμηλότερο επίπεδο στην ιεραρχεία συσκευών.

Παράδειγμα 5 — Εάν σε ένα χρήστη ή ομάδα επιτρέπεται η πρόσβαση ανάγνωσης και εγγραφής για μια συσκευή ή κλάση συσκευών:

Στον ίδιο χρήστη, στην ίδια ομάδα ή σε ένα μέλος της ίδιας ομάδας μπορεί να απαγορευτεί η πρόσβαση εγγραφής ή μόνο η πρόσβαση ανάγνωσης και εγγραφής για την ίδια συσκευή ή για μια συσκευή που βρίσκεται σε χαμηλότερο επίπεδο στην ιεραρχία συσκευών.

Παράδειγμα 6 — Εάν σε ένα χρήστη ή ομάδα απαγορευτεί η πρόσβαση ανάγνωσης και εγγραφής για μια συσκευή ή κλάση συσκευών:

Στον ίδιο χρήστη, στην ίδια ομάδα ή σε ένα μέλος της ίδιας ομάδας μπορεί να επιτραπεί η πρόσβαση ανάγνωσης ή μόνο η πρόσβαση ανάγνωσης και εγγραφής για μια συσκευή που βρίσκεται σε χαμηλότερο επίπεδο στην ιεραρχία συσκευών.

Άρνηση πρόσβασης σε χρήστη ή ομάδα

Για να αποτρέψετε την πρόσβαση ενός χρήστη ή μιας ομάδας σε μια συσκευή ή σε μια κλάση συσκευών, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής).
2. Στη λίστα συσκευών, κάντε κλικ στην κλάση συσκευής που θέλετε να διαμορφώσετε.
   - Κλάση συσκευής
   - Όλες οι συσκευές
   - Μεμονωμένη συσκευή
3. Στην περιοχή **User/Groups** (Χρήστης/Ομάδες), επιλέξτε το χρήστη ή την ομάδα που θέλετε να μην έχει πρόσβαση.
4. Επιλέξτε **Deny** (Να απαγορεύεται) διπλά σε ένα χρήστη ή ομάδα.
5. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

ΣΗΜΕΙΩΣΗ Όταν οι ρυθμίσεις απαγόρευσης ή αποδοχής έχουν οριστεί στο ίδιο επίπεδο συσκευής για ένα χρήστη, η απαγόρευση πρόσβασης υπερισχύει.

Αποδοχή πρόσβασης για ένα χρήστη ή μια ομάδα

Για να προσφέρετε την άδεια πρόσβασης ενός χρήστη ή μιας ομάδας σε μια συσκευή ή σε μια κλάση συσκευών, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής).
2. Στη λίστα συσκευών, επιλέξτε ένα από τα παρακάτω:
   - Κλάση συσκευής
   - Όλες οι συσκευές
   - Μεμονωμένη συσκευή
3. Επιλέξτε **Add** (Προσθήκη).

   Ανοίγει το πλαίσιο διαλόγου **Select Users or Groups** (Επιλογή χρηστών και ομάδων).
4. Επιλέξτε **Advanced** (Για προχωρημένους) και επιλέξτε **Find Now** (Εύρεση τώρα) για να αναζητήσετε χρήστες ή ομάδες για προσθήκη.
5. Επιλέξτε ένα χρήστη ή μια ομάδα που επιθυμείτε να προσθέσετε στη λίστα των διαθέσιμων χρηστών και ομάδων και, στη συνέχεια, επιλέξτε **OK**.
6. Κάντε κλικ στο **OK** ξανά.
7. Κάντε κλικ στο **Allow** (Να επιτρέπεται) για να παρέχετε πρόσβαση σε αυτό τον χρήστη ή την ομάδα.
8. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Κατάργηση πρόσβασης για ένα χρήστη ή μια ομάδα

Για να καταργήσετε την άδεια πρόσβασης ενός χρήστη ή μιας ομάδας σε μια συσκευή ή σε μια κλάση συσκευών, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής).
2. Στη λίστα συσκευών, κάντε κλικ στην κλάση συσκευής που θέλετε να διαμορφώσετε.
   - Κλάση συσκευής
   - Όλες οι συσκευές
   - Μεμονωμένη συσκευή
3. Κάντε κλικ στην επιλογή **User/Groups** (Χρήστης/Ομάδες),στο χρήστη ή ομάδα που θέλετε να καταργήσετε και, στη συνέχεια, κάντε κλικ στο **Remove** (Κατάργηση).
4. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Αποδοχή πρόσβασης σε μια κλάση συσκευών για ένα χρήστη μιας ομάδας

Για να επιτρέψετε σε ένα χρήστη να προσπελάσει μια κλάση συσκευών ενώ επιθυμείτε να απαγορεύσετε την πρόσβαση σε όλα τα άλλα μέλη της ομάδας αυτού του χρήστη, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής).
2. Στη λίστα συσκευών, κάντε κλικ στην κλάση συσκευής που θέλετε να διαμορφώσετε.
   - Κλάση συσκευής
   - Όλες οι συσκευές
   - Μεμονωμένη συσκευή
3. Στην περιοχή **User/Groups** (Χρήστης/Ομάδες), επιλέξτε την ομάδα που θέλετε να μην έχει πρόσβαση και, στη συνέχεια, επιλέξτε **Deny** (Να απαγορεύεται).
4. Περιηγηθείτε στο φάκελο κάτω από αυτό της απαιτούμενης τάξης και, στη συνέχεια, προσθέστε το συγκεκριμένο χρήστη.
5. Κάντε κλικ στο **Allow** (Να επιτρέπεται) για να επιτραπεί η πρόσβαση σε αυτό το χρήστη.
6. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Πρόσβαση σε μια συγκεκριμένη συσκευή για ένα χρήστη μιας ομάδας

Οι διαχειριστές μπορούν να επιτρέψουν σε ένα χρήστη να έχει πρόσβαση σε μια συγκεκριμένη συσκευή ενώ να απαγορεύσουν την πρόσβαση σε όλα τα άλλα μέλη της ομάδας αυτού του χρήστη για όλες τις συσκευές αυτής της τάξης.

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής).
2. Στη λίστα συσκευών, κάντε κλικ στην κλάση συσκευών που θέλετε να διαμορφώσετε και έπειτα περιηγηθείτε στο φάκελο που βρίσκεται κάτω από αυτή.
3. Επιλέξτε **Add** (Προσθήκη). Ανοίγει το πλαίσιο διαλόγου **Select Users or Groups** (Επιλογή χρηστών και ομάδων).
4. Κάντε κλικ στην επιλογή **Advanced** (Για προχωρημένους) και επιλέξτε **Find Now** (Εύρεση τώρα) για αναζήτηση της ομάδας του χρήστη στην οποία θα απαγορευτεί η πρόσβαση σε όλες τις συσκευές της κλάσης.
5. Κάντε κλικ στην ομάδα και επιλέξτε **OK**.
6. Πραγματοποιήστε πλοήγηση στη συγκεκριμένη συσκευή της κλάσης συσκευών, στην οποία θα επιτραπεί η πρόσβαση στο χρήστη.
7. Επιλέξτε **Add** (Προσθήκη). Ανοίγει το πλαίσιο διαλόγου **Select Users or Groups** (Επιλογή χρηστών και ομάδων).
8. Επιλέξτε **Advanced** (Για προχωρημένους) και επιλέξτε **Find Now** (Εύρεση τώρα) για να αναζητήσετε χρήστες ή ομάδες για προσθήκη.
9. Κάντε κλικ στο χρήστη που θέλετε να έχει πρόσβαση και έπειτα κάντε κλικ στο **OK**.

10. Κάντε κλικ στο **Allow** (Να επιτρέπεται) για να επιτραπεί η πρόσβαση σε αυτό το χρήστη.

11. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Επαναφορά της διαμόρφωσης

△ **ΠΡΟΣΟΧΗ** Η επαναφορά της διαμόρφωσης απορρίπτει όλες τις αλλαγές που πραγματοποιήθηκαν στη διαμόρφωση της συσκευής και επαναφέρει όλες τις ρυθμίσεις στις εργοστασιακά προεπιλεγμένες τιμές.

Για επαναφορά των ρυθμίσεων διαμόρφωσης στις εργοστασιακές τιμές, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής).

2. Κάντε κλικ στο κουμπί **Reset** (Επαναφορά).

3. Κάντε κλικ στο **Yes** (Ναι) για επιβεβαίωση.

4. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Εργασίες για προχωρημένους

Έλεγχος πρόσβασης στις ρυθμίσεις διαμόρφωσης

Στην προβολή **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη), οι διαχειριστές καθορίζουν τις ομάδες ή τους χρήστες στους οποίους επιτρέπεται η χρήση των σελίδων Simple Configuration (Απλή διαμόρφωση) και Device Class Configuration (Διαμόρφωση κλάσης συσκευής).

ΣΗΜΕΙΩΣΗ Ένας χρήστης ή μια ομάδα πρέπει να διαθέτει "Πλήρη δικαιώματα διαχειριστή-χρήστη" προκειμένου να μπορεί να τροποποιήσει τις ρυθμίσεις στην προβολή User Access Settings (Ρυθμίσεις πρόσβασης χρήστη).

- Σε ένα χρήστη ή μία ομάδα πρέπει να επιτραπεί η πρόσβαση "View (Read-only) Configuration Settings" (Προβολή ρυθμίσεων διαμόρφωσης (μόνο για ανάγνωση)) στην προβολή User Access Settings (Ρυθμίσεις πρόσβασης χρήστη) προκειμένου να μπορεί να εμφανίζει τις πληροφορίες απλής διαμόρφωσης (Simple Configuration) και διαμόρφωσης κλάσης συσκευής (Device Class Configuration).
- Σε ένα χρήστη ή μία ομάδα πρέπει να επιτραπεί η πρόσβαση Change Configuration Settings (Αλλαγή ρυθμίσεων διαμόρφωσης) στην προβολή User Access Settings (Ρυθμίσεις πρόσβασης χρήστη) προκειμένου να μπορεί να αλλάξει τις πληροφορίες απλής διαμόρφωσης (Simple Configuration) και διαμόρφωσης κλάσης συσκευής (Device Class Configuration).

ΣΗΜΕΙΩΣΗ Ακόμη και στα μέλη της ομάδας των διαχειριστών πρέπει να επιτραπεί η πρόσβαση "ανάγνωσης" για εμφάνιση των προβολών Simple Configuration (Απλή διαμόρφωση) και Device Class Configuration (Διαμόρφωση κλάσης συσκευής) και η πρόσβαση "αλλαγής" για αλλαγή των δεδομένων χρησιμοποιώντας τις προβολές Simple Configuration και Device Class Configuration.

ΣΗΜΕΙΩΣΗ Μετά την αξιολόγηση των επιπέδων πρόσβασης για όλους τους χρήστες και τις ομάδες, εάν ένας χρήστης δεν έχει επιλεγμένη ούτε την επιλογή Allow (Να επιτρέπεται) ούτε την επιλογή Deny (Να απαγορεύεται) για ένα συγκεκριμένο επίπεδο πρόσβασης, δεν επιτρέπεται η πρόσβαση του χρήστη σε εκείνο το επίπεδο.

Αποδοχή πρόσβασης σε μια υπάρχουσα ομάδα ή χρήστη

Για αποδοχή πρόσβασης σε μια υπάρχουσα ομάδα ή χρήστη για προβολή και αλλαγή των ρυθμίσεων διαμόρφωσης, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη).
2. Επιλέξτε μια ομάδα ή χρήστη, στον οποίο θα επιτραπεί η πρόσβαση.
3. Στην καρτέλα **Permissions** (Άδειες), επιλέξτε **Allow** (Να επιτρέπεται) για κάθε τύπο άδειας που θα δοθεί στην επιλεγμένη ομάδα ή χρήστη:

ΣΗΜΕΙΩΣΗ Οι άδειες που παρέχονται είναι αθροιστικές. Για παράδειγμα, σε ένα χρήστη που έχει δοθεί η άδεια Change Configuration Settings (Αλλαγή ρυθμίσεων διαμόρφωσης), δίνεται αυτόματα η άδεια View (Read-only) Configuration Settings (Προβολή ρυθμίσεων διαμόρφωσης (μόνο για ανάγνωση)). Σε ένα χρήστη που έχει δοθεί η άδεια Full User Administrator Rights (Πλήρη δικαιώματα διαχειριστή-χρήστη), δίνονται επίσης οι άδειες Change Configuration Settings (Αλλαγή ρυθμίσεων διαμόρφωσης) και View (Read-only) Configuration Settings (Προβολή ρυθμίσεων διαμόρφωσης (μόνο για ανάγνωση)).

- Full User Administrator Rights (Πλήρη δικαιώματα διαχειριστή-χρήστη)
- Change Configuration Settings (Αλλαγή ρυθμίσεων διαμόρφωσης)
- View (Read-only) Configuration Settings (Προβολή ρυθμίσεων διαμόρφωσης (μόνο για ανάγνωση))

4. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Απαγόρευση πρόσβασης σε μια υπάρχουσα ομάδα ή χρήστη

Για απαγόρευση πρόσβασης σε μια υπάρχουσα ομάδα ή χρήστη για προβολή και αλλαγή των ρυθμίσεων διαμόρφωσης, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη).
2. Επιλέξτε μια ομάδα ή χρήστη, στον οποίο θα απαγορεύεται η πρόσβαση.
3. Στην καρτέλα **Permissions** (Άδειες), επιλέξτε **Deny** (Να απαγορεύεται) για κάθε τύπο άδειας που θα απαγορεύεται για την επιλεγμένη ομάδα ή χρήστη:
   - Full User Administrator Rights (Πλήρη δικαιώματα διαχειριστή-χρήστη)
   - Change Configuration Settings (Αλλαγή ρυθμίσεων διαμόρφωσης)
   - View (Read-only) Configuration Settings (Προβολή ρυθμίσεων διαμόρφωσης (μόνο για ανάγνωση))
4. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Προσθήκη νέας ομάδας ή χρήστη

Για αποδοχή πρόσβασης σε μια νέα ομάδα ή χρήστη για προβολή και αλλαγή των ρυθμίσεων διαμόρφωσης, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη).
2. Επιλέξτε **Add** (Προσθήκη). Ανοίγει το πλαίσιο διαλόγου **Select Users or Groups** (Επιλογή χρηστών και ομάδων).
3. Επιλέξτε **Advanced** (Για προχωρημένους) και επιλέξτε **Find Now** (Εύρεση τώρα) για να αναζητήσετε χρήστες ή ομάδες για προσθήκη.
4. Επιλέξτε μια ομάδα ή χρήστη, επιλέξτε **OK** και, στη συνέχεια, επιλέξτε **OK** ξανά.
5. Κάντε κλικ στο **Allow** (Να επιτρέπεται) για να επιτραπεί η πρόσβαση σε αυτό το χρήστη.
6. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Κατάργηση πρόσβασης ομάδας ή χρήστη

Για κατάργηση πρόσβασης μιας ομάδας ή χρήστη για προβολή και αλλαγή των ρυθμίσεων διαμόρφωσης, ακολουθήστε τα εξής βήματα:

1. Στο αριστερό τμήμα του παραθύρου του **HP ProtectTools Administrative Console**, κάντε κλικ στο **Device Access Manager** και επιλέξτε **User Access Settings** (Ρυθμίσεις πρόσβασης χρήστη).
2. Επιλέξτε μια ομάδα ή χρήστη και έπειτα κάντε κλικ στο κουμπί **Remove** (Κατάργηση).
3. Κάντε κλικ στο εικονίδιο **Save** (Αποθήκευση).

Σχετική τεκμηρίωση

Το Device Access Manager for HP ProtectTools είναι συμβατό με το προϊόν HP ProtectTools Enterprise Device Access Manager της εταιρείας. Όταν εργάζεστε με το προϊόν της εταιρείας, το Device Access Manager for HP ProtectTools επιτρέπει πρόσβαση μόνο για ανάγνωση στις λειτουργίες του.

Περισσότερες πληροφορίες σχετικά με το Device Access Manager for HP ProtectTools είναι διαθέσιμες στο Web στη διεύθυνση http://www.hp.com/hps/security/products.

11 LoJack Pro για HP ProtectTools

Το Computrace LoJack Pro, που υποστηρίζεται από το λογισμικό Absolute Software (πωλείται ξεχωριστά), απευθύνεται στο αυξανόμενο πρόβλημα των υπολογιστών που έχουν χαθεί ή κλαπεί.

Η ενεργοποίηση αυτού του λογισμικού ενεργοποιεί και τον παράγοντα Computrace, ο οποίος παραμένει ενεργός στον υπολογιστή σας ακόμη και εάν ο σκληρός δίσκος έχει αναδιαμορφωθεί ή αντικατασταθεί.

Το LoJack Pro επιτρέπει την απομακρυσμένη παρακολούθηση, διαχείριση και εντοπισμό του υπολογιστή σας. Εάν ο υπολογιστής σας χαθεί ή κλαπεί, η ομάδα Absolute's Recovery θα βοηθήσει στην επανάκτησή του.*

ΣΗΜΕΙΩΣΗ *Αυτή η λειτουργία εξαρτάται από τη γεωγραφική τοποθεσία. Ανατρέξτε στο συμφωνητικό συνδρομής του λογισμικού Absolute Software για περισσότερες λεπτομέρειες.

12 Αντιμετώπιση προβλημάτων

HP ProtectTools Security Manager

Σύντομη περιγραφή	Λεπτομέρειες	Λύση
Οι έξυπνες κάρτες και τα USB token δεν είναι διαθέσιμα στο Security Manager εάν εγκατασταθούν μετά την εγκατάσταση του Security Manager.	Προκειμένου να χρησιμοποιήσετε έξυπνες κάρτες ή USB token στο Security Manager, το λογισμικό υποστήριξης (προγράμματα οδήγησης, παροχείς PKCS#11 κλπ.) πρέπει να έχει εγκατασταθεί πριν από την εγκατάσταση του Security Manager. Εάν έχετε ήδη εγκαταστήσει το Security Manager ακολουθήστε τα παρακάτω βήματα μετά την εγκατάσταση του λογισμικού υποστήριξης της έξυπνης κάρτας ή του token:	Συνδεθείτε στο Password Manager. Στο HP ProtectTools Security Manager, επιλέξτε **Password Manager**, κάντε κλικ στην επιλογή **Credentials** (Διαπιστευτήρια) και επιλέξτε **Smart Card** (Έξυπνη κάρτα) Εάν σας ζητηθεί, επανεκκινήστε τον υπολογιστή.
Ορισμένες σελίδες εφαρμογών στο web δημιουργούν σφάλματα που εμποδίζουν το χρήστη από την εκτέλεση ή ολοκλήρωση εργασιών.	Ορισμένες εφαρμογές με βάση το web παύουν να λειτουργούν και αναφέρουν σφάλματα λόγω του μοτίβου λειτουργίας του Single Sign On. Για παράδειγμα, στον Internet Explorer εμφανίζεται ένα **!** μέσα σε κίτρινο τρίγωνο, το οποίο υποδεικνύει ότι προέκυψε σφάλμα.	Η λειτουργία Single Sign On του Security Manager δεν υποστηρίζει όλες τις διασυνδέσεις web των λογισμικών. Απενεργοποιήστε την υποστήριξη Single Sign On για τη συγκεκριμένη σελίδα web απενεργοποιώντας την υποστήριξη Single Sign On. Δείτε την πλήρη τεκμηρίωση του Single Sign On, η οποία είναι διαθέσιμη στα αρχεία βοήθειας του λογισμικού Security Manager. Εάν δεν είναι δυνατή η απενεργοποίηση της λειτουργίας Single Sign On για μια δεδομένη εφαρμογή, επικοινωνήστε με την τεχνική υποστήριξη της HP και ζητήστε υποστήριξη τρίτου επιπέδου από τον υπεύθυνο επικοινωνίας της υπηρεσίας HP.
Η επιλογή **Browse for Virtual Token** (Αναζήτηση εικονικού διακριτικού) δεν εμφανίζεται κατά τη διαδικασία σύνδεσης.	Ο χρήστης δεν μπορεί να αλλάξει την τοποθεσία ενός καταχωρισμένου εικονικού token στο Password Manager επειδή η επιλογή αναζήτησης έχει αφαιρεθεί για μείωση των κινδύνων ασφαλείας.	Η επιλογή αναζήτησης καταργήθηκε επειδή επέτρεπε σε μη χρήστες να διαγράψουν και να μετονομάσουν αρχεία και να αναλάβουν τον έλεγχο των Windows.
Οι διαχειριστές τομέων δεν μπορούν να αλλάξουν τον κωδικό πρόσβασης στα Windows παρότι είναι εξουσιοδοτημένοι.	Αυτό συμβαίνει όταν ένας διαχειριστής τομέα συνδεθεί σε ένα τομέα και καταχωρίσει την ταυτότητα τομέα με το Password Manager χρησιμοποιώντας ένα λογαριασμό με δικαιώματα διαχειριστή στον τομέα και τον τοπικό υπολογιστή. Όταν ο διαχειριστής τομέα προσπαθήσει να αλλάξει τον κωδικό πρόσβασης των Windows από το Password Manager, ο διαχειριστής	Το Password Manager δεν μπορεί να αλλάξει ένα κωδικό πρόσβασης λογαριασμού χρήστη τομέα από την επιλογή **Change Windows password** (Αλλαγή κωδικού πρόσβασης για τα Windows). Το Security Manager μπορεί να αλλάξει μόνο τους κωδικούς πρόσβασης των λογαριασμών των τοπικών υπολογιστών. Ο χρήστης τομέα μπορεί να αλλάξει τον κωδικό πρόσβασής του από την επιλογή **Αλλαγή κωδικού πρόσβασης** στην **Ασφάλεια των Windows**, αλλά, καθώς ο χρήστης τομέα δεν διαθέτει

Σύντομη περιγραφή	Λεπτομέρειες	Λύση
	λαμβάνει ένα σφάλμα αποτυχίας σύνδεσης: **User account restriction** (Περιορισμός λογαριασμού χρήστη).	ένα φυσικό λογαριασμό στον τοπικό υπολογιστή, το Password Manager μπορεί να αλλάξει μόνο τον κωδικό πρόσβασης που χρησιμοποιείται για τη σύνδεση.
Το Password Manager αντιμετωπίζει προβλήματα συμβατότητας με τον κωδικό πρόσβασης GINA του Corel WordPerfect 12.	Εάν ένα χρήστης συνδεθεί στο Password Manager, δημιουργήσει ένα έγγραφο στο WordPerfect και το αποθηκεύσει με προστασία του κωδικού πρόσβασης, το Password Manager δεν μπορεί να εντοπίσει ή να αναγνωρίσει, είτε μη αυτόματα είτε αυτόματα, τον κωδικό πρόσβασης GINA.	Η HP ερευνά κάποιον τρόπο παράκαμψης του προβλήματος για τις μελλοντικές βελτιώσεις προϊόντων.
Το Password Manager δεν αναγνωρίζει το κουμπί **Connect** (Σύνδεση) στην οθόνη.	Εάν τα διαπιστευτήρια Single Sign On για σύνδεση απομακρυσμένου υπολογιστή έχουν οριστεί στην επιλογή **Connect** (Σύνδεση), όταν γίνεται επανεκκίνηση του Single Sign On, εισαγάγει πάντοτε **Save As** (Αποθήκευση ως) αντί για **Connect** (Σύνδεση).	Η HP ερευνά κάποιον τρόπο παράκαμψης του προβλήματος για τις μελλοντικές βελτιώσεις προϊόντων.
Ο χρήστης δεν μπορεί να συνδεθεί στο Password Manager μετά τη μετάβαση από αναστολή λειτουργίας σε αδρανοποίηση στα Windows XP Service Pack 1 μόνο.	Αφού πραγματοποιηθεί η μετάβαση του συστήματος σε αδρανοποίηση και αναστολή λειτουργίας, ο διαχειριστής ή ο χρήστης δεν μπορεί να συνδεθεί στο Password Manager και η οθόνη σύνδεσης των Windows συνεχίζει να εμφανίζεται ανεξάρτητα από το διαπιστευτήριο σύνδεσης (κωδικός πρόσβασης, δακτυλικό αποτύπωμα ή κάρτα Java) που επιλέξατε.	Ενημερώστε τα Windows με το Service Pack 2 μέσω του Windows Update. Ανατρέξτε στο άρθρο 813301 στη γνωσιακή βάση της Microsoft στη διεύθυνση http://www.microsoft.com για περισσότερες πληροφορίες σχετικά με την αιτία του προβλήματος. Για να πραγματοποιηθεί η σύνδεση, ο χρήστης πρέπει να επιλέξει το Password Manager και να συνδεθεί. Μετά τη σύνδεση στο Password Manager, ζητείται από το χρήστη να συνδεθεί στα Windows (ο χρήστης μπορεί να χρειαστεί να ενεργοποιήσει την επιλογή σύνδεσης των Windows) για να ολοκληρώσει τη διαδικασία σύνδεσης. Εάν ο χρήστης συνδεθεί πρώτα στα Windows, τότε ο χρήστης πρέπει να συνδεθεί μη αυτόματα στο Password Manager.
Η διαδικασία ασφαλείας **Restore Identity** (Ανάκτηση ταυτότητας) χάνει το συσχετισμό με το εικονικό διακριτικό.	Όταν ο χρήστης θα επαναφέρει την ταυτότητα, το Password Manager ενδέχεται να χάσει τη συσχέτιση με την τοποθεσία του εικονικού token στην οθόνη σύνδεσης. Ακόμη και εάν το Password Manager έχει κατοχυρώσει το εικονικό token, ο χρήστης πρέπει να κατοχυρώσει το token ξανά για να επαναφέρει τη συσχέτιση.	Σε αυτή τη φάση αυτό έχει σχεδιαστεί έτσι. Όταν πραγματοποιείται κατάργηση της εγκατάστασης του Security Manager χωρίς τη διατήρηση των ταυτοτήτων, το τμήμα συστήματος (διακομιστή) του token καταστρέφεται, έτσι το token δεν μπορεί να χρησιμοποιηθεί πια για σύνδεση, ακόμη και εάν το τμήμα πελάτη του token επαναφέρεται μέσω της επαναφοράς ταυτότητας. Η HP ερευνά μακροπρόθεσμες επιλογές για να λυθεί το πρόβλημα.

Device Access Manager for HP ProtectTools

Στους χρήστες έχει απαγορευτεί η πρόσβαση σε συσκευές στο Device Access Manager, αλλά οι συσκευές είναι ακόμη προσπελάσιμες.

- **Επεξήγηση** — Χρησιμοποιήθηκε η απλή διαμόρφωση (Simple Configuration) ή/και η διαμόρφωση κλάσης συσκευής (Device Class Configuration) στο Device Access Manager για την απαγόρευση πρόσβασης των χρηστών σε συσκευές. Παρότι τους απαγορεύτηκε η πρόσβαση, οι χρήστες μπορούν ακόμη να προσπελάσουν τις συσκευές.
- **Λύση:**
  - Βεβαιωθείτε ότι έχει πραγματοποιηθεί εκκίνηση της υπηρεσίας HP ProtectTools Device Locking.
  - Ως χρήστης με δικαιώματα διαχειριστή, κάντε κλικ στον **Πίνακα Ελέγχου** και επιλέξτε **Σύστημα και Συντήρηση**. Στο παράθυρο "Εργαλεία Διαχείρισης", επιλέξτε **Υπηρεσίες** και αναζητήστε την υπηρεσία **HP ProtectTools Device Locking/Auditing**. Βεβαιωθείτε ότι έχει πραγματοποιηθεί εκκίνηση της υπηρεσίας και ότι ο τύπος εκκίνησης είναι **Automatic** (Αυτόματο).

Ένας χρήστης διαθέτει μη αναμενόμενη πρόσβαση σε μια συσκευή ή σε ένα χρήστη απαγορεύεται μη αναμενόμενα η πρόσβαση σε μια συσκευή.

- **Επεξήγηση** — Το Device Access Manager χρησιμοποιήθηκε για να απαγορεύει την πρόσβαση σε χρήστες σε ορισμένες συσκευές και για να επιτρέπει την πρόσβαση σε χρήστες σε ορισμένες συσκευές. Όταν ο χρήστης χρησιμοποιεί το σύστημα, μπορεί να προσπελάσει συσκευές που πιστεύει ότι το Device Access Manager έχει απαγορεύσει και του απαγορεύεται η πρόσβαση σε συσκευές που πιστεύει ότι το Device Access Manager πρέπει να επιτρέπει.
- **Λύση:**
  - Χρησιμοποιήστε τη διαμόρφωση κλήσης συσκευής (Device Class Configuration) στο Device Access Manager για να ερευνήσετε τις ρυθμίσεις συσκευής του χρήστη.
  - Κάντε κλικ στην επιλογή **Security Manager**, επιλέξτε **Device Access Manager** και, στη συνέχεια κάντε κλικ στην επιλογή **Device Class Configuration** (Διαμόρφωση κλάσης συσκευής). Επεκτείνετε τα επίπεδα στο δέντρο κλάσης συσκευών και ελέγξτε τις ρυθμίσεις που ισχύουν για αυτό το χρήστη. Αναζητήστε τυχόν άδειες Deny (Να απαγορεύεται) που μπορεί να έχουν οριστεί για το χρήστη ή για οποιαδήποτε ομάδα των Windows, στην οποία μπορεί να αποτελούν μέλος, π.χ., Χρήστες, Διαχειριστές.

Να επιτρέπεται ή να απαγορεύεται—ποιο υπερισχύει;

- **Επεξήγηση** — Στη διαμόρφωση τάξης συσκευής (Device Class Configuration), έχει οριστεί η παρακάτω διαμόρφωση:
  - Η άδεια Allow (Να επιτρέπεται) έχει δοθεί σε μια ομάδα των Windows (π.χ., BUILTIN \Διαχειριστές) και η άδεια Deny (Να απαγορεύεται) έχει δοθεί σε άλλη ομάδα των Windows (e.g., BUILTIN\Χρήστες) στο ίδιο επίπεδο στην ιεραρχία κλάσης συσκευών (π.χ, Μονάδες DVD/CD-ROM).
  - Εάν ένας χρήστης είναι μέλος και στις δύο αυτές ομάδες (π.χ., Διαχειριστής), ποια υπερισχύει;
- **Λύση:**
  - Στο χρήστη απαγορεύεται η πρόσβαση στη συσκευή. Το Deny (Να απαγορεύεται) υπερισχύει έναντι του Allow (Να επιτρέπεται).
  - Η πρόσβαση απαγορεύεται εξαιτίας του τρόπου με τον οποίο διαχειρίζονται τα Windows την αποτελεσματική άδεια για τη συσκευή. Σε μια ομάδα απαγορεύεται η πρόσβαση και σε μια ομάδα επιτρέπεται, αλλά ο χρήστης αποτελεί μέλος και στις δύο ομάδες. Απαγορεύεται η πρόσβαση στο χρήστη επειδή η απαγόρευση πρόσβασης υπερισχύει έναντι της αποδοχής πρόσβασης.
  - Ένας τρόπος επίλυσης είναι απαγορέψετε την πρόσβαση της ομάδας χρηστών στο επίπεδο μονάδων DVD/CD-ROM και να επιτρέψετε την πρόσβαση της ομάδας διαχειριστών στο επίπεδο κάτω από το επίπεδο των μονάδων DVD/CD-ROM.
  - Ένας εναλλακτικός τρόπος επίλυσης είναι να δημιουργήσετε ειδικές ομάδες των Windows, που στη μία θα επιτρέπεται η πρόσβαση στο DVD/CD και στην άλλη θα απαγορεύεται η πρόσβαση στο DVD/CD. Στη συνέχεια, θα προσθέσετε ειδικούς χρήστες στην κατάλληλη ομάδα.

Η προβολή Simple Configuration (Απλή διαμόρφωση) έχει χρησιμοποιηθεί για τη διαμόρφωση μιας πολιτικής ελέγχου πρόσβασης συσκευής, αλλά οι χρήστες με δικαιώματα διαχειριστή δεν μπορούν να προσπελάσουν τις συσκευές.

- **Επεξήγηση** — Η απλή διαμόρφωση (Simple Configuration) απαγορεύει την πρόσβαση σε χρήστες και επισκέπτες και επιτρέπει την πρόσβαση στους διαχειριστές της συσκευής.
- **Λύση:** Προσθέστε το χρήστη με δικαιώματα διαχειριστή στην ομάδα διαχειριστών της συσκευής.

Διάφορα

Επηρεαζόμενα από το λογισμικό — Σύντομη περιγραφή	Λεπτομέρειες	Λύση
Security Manager — Λήψη προειδοποιητικού μηνύματος: **The security application can not be installed until the HP Protect Tools Security Manager is installed.** (Δεν είναι δυνατή η εγκατάσταση της εφαρμογής ασφαλείας έως ότου να εγκατασταθεί το HP Protect Tools Security Manager).	Όλες οι εφαρμογές ασφαλείας όπως η ασφάλεια κάρτας Java Card Security και οι συσκευές βιομετρικής ανάγνωσης αποτελούν επεκτάσιμες προσθήκες για τη διασύνδεση του Security Manager. Το Security Manager πρέπει να εγκατασταθεί προτού φορτωθεί μια προέκταση ασφαλείας εγκεκριμένη από την HP.	Το λογισμικό Security Manager θα πρέπει να έχει εγκατασταθεί πριν από την εγκατάσταση οποιασδήποτε προσθήκης ασφαλείας.
HP ProtectTools Security Manager — Περιοδικά προκύπτει σφάλμα όταν κλείνει η διασύνδεση Security Manager.	Περιοδικά (1 στις 12 φορές), δημιουργείται σφάλμα από το κουμπί στο επάνω δεξί μέρος της οθόνης για το κλείσιμο του Security Manager πριν να ολοκληρωθεί η φόρτωση όλων των εφαρμογών προσθηκών.	Αυτό σχετίζεται με μια εξάρτηση του χρονισμού από το χρόνο φόρτωσης των υπηρεσιών προσθηκών κατά το κλείσιμο και επανεκκίνηση του Security Manager. Καθώς το PTHOST.exe αποτελεί το κέλυφος που περιλαμβάνει τις άλλες εφαρμογές (προσθήκες) εξαρτάται από την ικανότητα της προσθήκης να ολοκληρώσει το χρόνο φόρτωσής της (υπηρεσίες). Η βασική αιτία είναι ότι κλείνει το κέλυφος πριν προλάβει η προσθήκη να ολοκληρώσει τη φόρτωση. Επιτρέψτε στο Security Manager να ολοκληρώσει το μήνυμα φόρτωσης υπηρεσιών (εμφανίζεται στο επάνω μέρος του παραθύρου του Security Manager) και όλες τις προσθήκες που περιλαμβάνονται στην αριστερή στήλη. Για να αποφύγετε τυχόν σφάλμα, αφήστε ένα εύλογο χρονικό διάστημα για τη φόρτωση των προσθηκών.
HP ProtectTools— Κίνδυνος ασφαλείας λόγω πρόσβασης χωρίς περιορισμούς ή μη ελεγχόμενων δικαιωμάτων διαχειριστή.	Είναι πιθανοί πολλοί κίνδυνοι από την πρόσβαση χωρίς περιορισμό στον υπολογιστή client, συμπεριλαμβανομένων των παρακάτω: • Διαγραφή της μονάδας PSD • Κακόβουλη τροποποίηση των ρυθμίσεων χρήστη • Απενεργοποίηση πολιτικών και λειτουργιών ασφαλείας	Οι διαχειριστές συνιστάται να ακολουθούν τις "βέλτιστες πρακτικές" σε ό,τι αφορά τον περιορισμό των προνομίων των τελικών χρηστών και της πρόσβασης των χρηστών. Οι χρήστες που δεν είναι εξουσιοδοτημένοι δεν πρέπει να έχουν διαχειριστικά προνόμια.

Γλωσσάρι

ακολουθία πλήκτρων Ένας συνδυασμός συγκεκριμένων πλήκτρων που, όταν πατηθούν, ξεκινάει μια αυτόματη μόνιμη διαγραφή —π.χ. ctrl+alt+s.

αξιόπιστη επαφή Ένα άτομο που έχει αποδεχτεί μια πρόσκληση αξιόπιστης επαφής (Trusted Contact).

αξιόπιστη επικοινωνία άμεσων μηνυμάτων Μια περίοδος λειτουργίας επικοινωνίας κατά τη διάρκεια της οποίας αξιόπιστα μηνύματα αποστέλλονται από αξιόπιστο αποστολέα προς αξιόπιστη επαφή.

αξιόπιστο μήνυμα Μια περίοδος λειτουργίας επικοινωνίας κατά τη διάρκεια της οποίας αξιόπιστα μηνύματα αποστέλλονται από αξιόπιστο αποστολέα προς αξιόπιστη επαφή.

αξιόπιστος αποστολέας Μια αξιόπιστη επαφή που αποστέλλει υπογεγραμμένα ή/και κρυπτογραφημένα μηνύματα ηλεκτρονικού ταχυδρομείου και έγγραφα του Microsoft Office.

απλή διαγραφή Διαγραφή της αναφοράς των Windows προς ένα πόρο. Το περιεχόμενο του πόρου παραμένει στο σκληρό δίσκο μέχρι τα κρυφά δεδομένα να αντικατασταθούν από την εκκαθάριση του ελεύθερου χώρου.

αποκάλυψη Μια εργασία που επιτρέπει στο χρήστη να αποκρυπτογραφήσει μία ή περισσότερες περιόδους λειτουργίας του ιστορικού συνομιλιών, εμφανίζοντας ονόματα επαφών σε μορφή απλού κειμένου και καθιστώντας την περίοδο λειτουργίας διαθέσιμη για προβολή.

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

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

αρχείο επείγουσας ανάκτησης Προστατευόμενη περιοχή αποθήκευσης που επιτρέπει την επανακρυπτογράφηση των βασικών κλειδιών χρήστη από ένα κλειδί κατόχου πλατφόρμας σε άλλο.

αρχή πιστοποίησης Υπηρεσία που εκδίδει τα πιστοποιητικά που απαιτούνται για τη λειτουργία της υποδομής δημόσιου κλειδιού.

ασφάλεια σύνδεσης των Windows Προστατεύει τους λογαριασμούς σας στα Windows απαιτώντας τη χρήση συγκεκριμένων διαπιστευτηρίων για την παροχή πρόσβασης.

αυτόματη μόνιμη διαγραφή Ο προγραμματισμένος τεμαχισμός που ορίζει ο χρήστης στο File Sanitizer.

βιομετρικό Κατηγορία διαπιστευτηρίων ταυτότητας που χρησιμοποιεί ένα σωματικό στοιχείο, όπως το δακτυλικό αποτύπωμα, για την αναγνώριση του χρήστη.

γραμμή υπογραφής Ένα σύμβολο κράτησης θέσης για την οπτική εμφάνιση ψηφιακής υπογραφής. Όταν το έγγραφο υπογραφεί, εμφανίζονται το όνομα του υπογράφοντα και η μέθοδος επιβεβαίωσης. Επίσης, μπορούν να συμπεριληφθούν η ημερομηνία υπογραφής και ο τίτλος του υπογράφοντα.

δημιουργία αντιγράφων ασφαλείας Χρήση της υπηρεσίας δημιουργίας αντιγράφων ασφαλείας για την αποθήκευση ενός αντιγράφου των σημαντικών πληροφοριών προγράμματος σε μια τοποθεσία εκτός του

προγράμματος. Στη συνέχεια, μπορεί να χρησιμοποιηθεί για την επαναφορά των πληροφοριών σε μεταγενέστερη ημερομηνία στον ίδιο υπολογιστή ή σε διαφορετικό.

διακριτικό Ανατρέξτε στη μέθοδο ασφαλούς σύνδεσης.

διακριτικό USB Συσκευή ασφαλείας που αποθηκεύει πληροφορίες αναγνώρισης σχετικά με ένα χρήστη. Όπως συμβαίνει με μια κάρτα Java ή συσκευή βιομετρικής ανάγνωσης, χρησιμοποιείται για τον έλεγχο ταυτότητας του κατόχου του υπολογιστή.

διαπιστευτήρια Μέθοδος με την οποία ένας χρήστης αποδεικνύει ότι έχει την έγκριση για να εκτελέσει μια συγκεκριμένη εργασία κατά τη διαδικασία ελέγχου ταυτότητας.

διαχειριστής *Δείτε* Διαχειριστής των Windows.

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

εικονικό διακριτικό Λειτουργία ασφαλείας που λειτουργεί όπως μια κάρτα Java και μια συσκευή ανάγνωσης καρτών. Το διακριτικό αποθηκεύεται στο σκληρό δίσκο του υπολογιστή ή στο μητρώο των Windows. Όταν συνδέεστε σε ένα εικονικό διακριτικό, σας ζητείται ένα PIN χρήστη για να ολοκληρώσετε τον έλεγχο ταυτότητας.

εκκαθάριση ελεύθερου χώρου Η ασφαλής εγγραφή τυχαίων δεδομένων επάνω σε διαγραμμένους πόρους για να διαστρεβλωθούν τα περιεχόμενα του διαγραμμένου πόρου.

έλεγχος ταυτότητας Διαδικασία επαλήθευσης αν ένας χρήστης είναι εξουσιοδοτημένος να εκτελεί μια εργασία, όπως πρόσβαση σε υπολογιστή, τροποποίηση ρυθμίσεων σε συγκεκριμένο πρόγραμμα ή προβολή δεδομένων που έχουν ασφάλεια.

έλεγχος ταυτότητας κατά την εκκίνηση Λειτουργία ασφάλειας που απαιτεί κάποιο είδος ελέγχου ταυτότητας όπως κάρτα Java, κύκλωμα ασφαλείας ή κωδικό πρόσβασης κατά την ενεργοποίηση του υπολογιστή.

ενεργοποίηση Η εργασία πρέπει να ολοκληρωθεί προτού να είναι προσπελάσιμες οι λειτουργίες του Drive Encryption. Το Drive Encryption ενεργοποιείται χρησιμοποιώντας τον οδηγό HP ProtectTools Setup Wizard. Μόνο ένας διαχειριστής μπορεί να ενεργοποιήσει το Drive Encryption. Η διαδικασία ενεργοποίησης αποτελείται από την ενεργοποίηση του λογισμικού, την κρυπτογράφηση της μονάδας, τη δημιουργία λογαριασμού χρήστη και τη δημιουργία του κλειδιού κρυπτογράφησης της αρχικής δημιουργίας αντιγράφων ασφαλείας σε μια αφαιρούμενη συσκευή αποθήκευσης.

εξουσιοδοτημένος χρήστης Ένας χρήστης στον οποίο έχει δοθεί άδεια στην προβολή User Access Settings (Ρυθμίσεις πρόσβασης χρήστη) για προβολή ή τροποποίηση των προβολών Simple Configuration (Απλή διαμόρφωση) ή Device Class Configuration (Διαμόρφωση κλάσης συσκευής).

έξυπνη κάρτα Μικρό κομμάτι υλικού, παρόμοιο σε μέγεθος και σχήμα με πιστωτική κάρτα, όπου αποθηκεύονται πληροφορίες αναγνώρισης του ιδιοκτήτη. Χρησιμοποιείται για τον έλεγχο ταυτότητας του κατόχου ενός υπολογιστή.

επαναφορά Μια διαδικασία που αντιγράφει τις πληροφορίες του προγράμματος από ένα προηγούμενα αποθηκευμένο αντίγραφο ασφαλείας σε αυτό το πρόγραμμα.

επανεκκίνηση Διαδικασία νέας εκκίνησης του υπολογιστή.

ιστορικό συνομιλίας Ένα κρυπτογραφημένο αρχείο που περιέχει μια καταχώριση και των δύο πλευρών της συνομιλίας σε μια περίοδο λειτουργίας συνομιλίας.

κάρτα Java Αφαιρούμενη κάρτα που τοποθετείται στον υπολογιστή. Περιέχει πληροφορίες αναγνώρισης για σύνδεση. Η σύνδεση με μια κάρτα Java στην οθόνη σύνδεσης του Drive Encryption απαιτεί να τοποθετήσετε την κάρτα Java και να πληκτρολογήσετε το όνομα χρήστη και το PIN της κάρτας Java.

κλάση συσκευής Όλες οι συσκευές ενός συγκεκριμένου τύπου, όπως οι μονάδες.

κονσόλα Η κεντρική τοποθεσία όπου μπορείτε να προσπελάσετε και να διαχειριστείτε τις λειτουργίες και τις ρυθμίσεις του προγράμματος.

κουμπί Send Security (Αποστολή με ασφάλεια) Ένα κουμπί του λογισμικού που εμφανίζεται στη γραμμή εργαλείων των μηνυμάτων ηλεκτρονικού ταχυδρομείου του Microsoft Outlook. Αν κάνετε κλικ σε αυτό το κουμπί, μπορείτε να υπογράψετε ή/και να κρυπτογραφήσετε ένα μήνυμα ηλεκτρονικού ταχυδρομείου του Microsoft Outlook.

κουμπί Sign and Encrypt (Υπογραφή και κρυπτογράφηση) Ένα κουμπί του λογισμικού που εμφανίζεται στη γραμμή εργαλείων των εφαρμογών του Microsoft Office. Αν κάνετε κλικ στο κουμπί μπορείτε να υπογράψετε, να κρυπτογραφήσετε ή να καταργήσετε την κρυπτογράφηση σε ένα έγγραφο του Microsoft Office.

κρυπτογράφηση Η πρακτική της κρυπτογράφησης και αποκρυπτογράφησης δεδομένων προκειμένου να αποκωδικοποιούνται μόνο από συγκεκριμένα άτομα.

κρυπτογράφηση Διαδικασία όπως η χρήση αλγόριθμου, που χρησιμοποιείται στην κρυπτογραφία για τη μετατροπή απλού κειμένου σε κωδικοποιημένο κείμενο προκειμένου να προλαμβάνει την ανάγνωση αυτών των δεδομένων από μη εξουσιοδοτημένους παραλήπτες. Υπάρχουν πολλοί τύποι κρυπτογράφησης δεδομένων και αποτελούν τη βάση για την ασφάλεια δικτύων. Οι συνήθεις τύποι περιλαμβάνουν το πρότυπο κρυπτογράφησης δεδομένων και την κρυπτογράφηση δημόσιων κλειδιών.

κύκλος μόνιμης διαγραφής Ο αριθμός των φορών που ο αλγόριθμος μόνιμης διαγραφής εκτελείται σε κάθε πόρο. Όσο μεγαλύτερος είναι ο αριθμός των κύκλων μόνιμης διαγραφής που επιλέγετε, τόσο πιο ασφαλής είναι ο υπολογιστής.

κωδικός πρόσβασης ανάκλησης Ένας κωδικός πρόσβασης που δημιουργείται όταν ένας χρήστης ζητήσει ψηφιακό πιστοποιητικό. Ο κωδικός πρόσβασης είναι απαραίτητος όταν ο χρήστης θέλει να ανακαλέσει το ψηφιακό πιστοποιητικό του. Αυτό διασφαλίζει ότι μόνο ο χρήστης μπορεί να ανακαλέσει το πιστοποιητικό.

λειτουργία συσκευής SATA Λειτουργία μεταφοράς δεδομένων μεταξύ υπολογιστή και συσκευών μαζικής αποθήκευσης, όπως σκληροί δίσκοι και μονάδες οπτικών δίσκων.

λίστα αξιόπιστων επαφών Μια λίστα με τις αξιόπιστες επαφές.

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

λογαριασμός χρήστη των Windows Προφίλ για άτομο που έχει την έγκριση να συνδεθεί με ένα δίκτυο ή σε συγκεκριμένο υπολογιστή.

μέθοδος ασφαλούς σύνδεσης Η μέθοδος που χρησιμοποιείται για σύνδεση στον υπολογιστή.

μετεγκατάσταση Μια εργασία που επιτρέπει τη διαχείριση, την επαναφορά και τη μεταφορά πιστοποιητικών του Privacy Manager και αξιόπιστων επαφών.

μη αυτόματη μόνιμη διαγραφή Άμεση μόνιμη διαγραφή πόρου ή επιλεγμένων πόρων, που παρακάμπτει τον προγραμματισμό αυτόματης μόνιμης διαγραφής.

μόνιμη διαγραφή Η εκτέλεση ενός αλγόριθμου που αποκρύπτει τα δεδομένα τα οποία περιέχονται σε ένα πόρο.

οθόνη σύνδεσης στο Drive Encryption Μια οθόνη σύνδεσης που εμφανίζεται πριν από την έναρξη των Windows. Οι χρήστες πρέπει να εισαγάγουν το όνομα χρήστη και τον κωδικό πρόσβασης που έχουν στα Windows ή το PIN του Java Card. Στις περισσότερες περιπτώσεις, η καταχώριση των σωστών πληροφοριών στην οθόνη σύνδεσης του Drive Encryption επιτρέπει την απευθείας πρόσβαση στα Windows χωρίς να χρειάζεται ξανά σύνδεση στην οθόνη σύνδεσης των Windows.

ομάδα Μια ομάδα χρηστών που διαθέτει το ίδιο επίπεδο πρόσβασης ή απαγόρευσης σε μια κλάση συσκευών ή σε μια συγκεκριμένη συσκευή.

παραλήπτης πρόσκλησης για αξιόπιστη επαφή Ένα άτομο που λαμβάνει μια πρόσκληση για να γίνει αξιόπιστη επαφή.

παροχέας υπηρεσιών κρυπτογράφησης (CSP) Πάροχος ή βιβλιοθήκη αλγόριθμων κρυπτογράφησης που μπορούν να χρησιμοποιηθούν σε μια καθορισμένη διεπαφή προκειμένου να εκτελούν συγκεκριμένες λειτουργίες κρυπτογράφησης.

πίνακας εργαλείων Η κεντρική τοποθεσία όπου μπορείτε να προσπελάσετε και να διαχειριστείτε τις λειτουργίες και τις ρυθμίσεις του προγράμματος.

πιστοποιητικό του Privacy Manager Ένα ψηφιακό πιστοποιητικό που απαιτεί έλεγχο της ταυτότητας κάθε φορά που το χρησιμοποιείτε για λειτουργίες κρυπτογράφησης, όπως υπογραφή και κρυπτογράφηση μηνυμάτων ηλεκτρονικού ταχυδρομείου και εγγράφων του Microsoft Office.

πολιτική ελέγχου πρόσβασης της συσκευής Μια λίστα συσκευών στις οποίες επιτρέπεται ή απαγορεύεται η πρόσβαση του χρήστη.

πόρος Ένα στοιχείο δεδομένων που αποτελείται από προσωπικές πληροφορίες ή αρχεία, δεδομένα ιστορικού ή που έχουν σχέση με το web και άλλα, τα οποία βρίσκονται στο σκληρό δίσκο.

Πρόγραμμα προβολής ιστορικού Live Messenger History Viewer Ένα στοιχείο του Privacy Manager Chat που σας επιτρέπει να αναζητάτε και να προβάλετε κρυπτογραφημένες περιόδους λειτουργίας του ιστορικού συνομιλιών.

πρόσκληση για αξιόπιστη επαφή Ένα μήνυμα ηλεκτρονικού ταχυδρομείου που αποστέλλεται σε ένα άτομο, ζητώντας του να γίνει αξιόπιστη επαφή.

προτεινόμενος υπογράφων Ένας χρήστης ο οποίος έχει καθοριστεί από τον κάτοχο εγγράφου το Microsoft Word ή του Microsoft Excel για να προσθέσει μια γραμμή υπογραφής στο έγγραφο.

προφίλ μόνιμης διαγραφής Μια καθορισμένη μέθοδος διαγραφής και λίστα πόρων.

σύνδεση Ένα στοιχείο στο Security Manager που αποτελείται από ένα όνομα χρήστη και ένα κωδικό πρόσβασης (και πιθανόν και άλλες επιλεγμένες πληροφορίες), οι οποίες μπορούν να χρησιμοποιηθούν για τη σύνδεση σε τοποθεσίες web ή προγράμματα.

σύστημα κρυπτογράφησης αρχείων (EFS) Σύστημα για την κρυπτογράφηση όλων των αρχείων και υποφακέλων στον επιλεγμένο φάκελο.

σφραγίδα για αξιόπιστες επαφές Μια εργασία που προσθέτει ψηφιακή υπογραφή, κρυπτογραφεί το μήνυμα ηλεκτρονικού ταχυδρομείου και το αποστέλλει αφού κάνετε έλεγχο ταυτότητας χρησιμοποιώντας την επιλεγμένη μέθοδο σύνδεσης ασφαλείας.

ταυτότητα Στο HP ProtectTools Security Manager, μια ομάδα διαπιστευτηρίων και ρυθμίσεων που αντιμετωπίζονται ως λογαριασμός ή προφίλ συγκεκριμένου χρήστη.

ταυτότητα Μια μικροεφαρμογή στην πλευρική εργαλειοθήκη των Windows που χρησιμοποιείται για την οπτική αναγνώριση της επιφάνειας εργασίας σας με το όνομα χρήστη σας και την επιλεγμένη εικόνα. Κάντε κλικ στην ταυτότητα για άνοιγμα του HP ProtectTools Administrative Console.

τομέας Ομάδα υπολογιστών που ανήκει σε ένα δίκτυο και έχουν κοινόχρηστη βάση δεδομένων καταλόγου. Οι τομείς έχουν μοναδικά ονόματα και ο καθένας έχει ένα σύνολο κοινών κανόνων και διαδικασιών.

υπηρεσία παρασκηνίου Η υπηρεσία παρασκηνίου HP ProtectTools Device Locking/Auditing, η οποία πρέπει να εκτελείται για πολιτικές ελέγχου πρόσβασης στη συσκευή, οι οποίες θα εφαρμοστούν. Η προβολή της είναι δυνατή από την εφαρμογή "Υπηρεσίες" στην επιλογή "Εργαλεία Διαχείρισης" του Πίνακα Ελέγχου. Εάν δεν λειτουργεί, το HP ProtectTools Security Manager θα προσπαθήσει να την ξεκινήσει όταν εφαρμοστούν οι πολιτικές ελέγχου πρόσβασης της συσκευής.

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

ψηφιακή υπογραφή Δεδομένα που αποστέλλονται με ένα αρχείο που επιβεβαιώνουν τον αποστολέα του υλικού και ότι το αρχείο δεν έχει τροποποιηθεί μετά από την υπογραφή του.

ψηφιακό πιστοποιητικό Ηλεκτρονικά διαπιστευτήρια που επιβεβαιώνουν την ταυτότητα ατόμου ή εταιρείας συνδέοντας την ταυτότητα του κατόχου του ψηφιακού πιστοποιητικού με ένα ζεύγος ηλεκτρονικών κλειδιών που χρησιμοποιούνται για την υπογραφή ψηφιακών πληροφοριών.

ATM Πρόκειται για το Automatic Technology Manager, που επιτρέπει στους διαχειριστές δικτύου να διαχειρίζονται συστήματα από απόσταση σε επίπεδο BIOS.

Drive Encryption Προστατεύει τα δεδομένα σας κρυπτογραφώντας τους σκληρούς δίσκους και καθιστώντας αδύνατη την ανάγνωση των πληροφοριών από άτομα που δεν έχουν την κατάλληλη εξουσιοδότηση.

DriveLock Λειτουργία ασφαλείας που συνδέει τη μονάδα σκληρού δίσκου με ένα χρήστη και απαιτεί από το χρήστη να πληκτρολογήσει σωστά τον κωδικό πρόσβασης του DriveLock κατά την εκκίνηση του υπολογιστή.

HP SpareKey Αντίγραφο ασφαλείας κλειδιού κρυπτογράφησης μονάδας.

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

PSD Προσωπική ασφαλής μονάδα δίσκου που παρέχει προστατευμένο χώρο αποθήκευσης για ευαίσθητες πληροφορίες.

Single Sign On (Μοναδική σύνδεση) Λειτουργία στην οποία αποθηκεύονται τα στοιχεία ελέγχου ταυτότητας και η οποία σας επιτρέπει να χρησιμοποιήσετε τη λειτουργία Security Manager για να έχετε πρόσβαση σε εφαρμογές Internet και Windows που απαιτούν έλεγχο κωδικού χρήστη.

TXT Τεχνολογία Trusted Execution.

Ευρετήριο

S

W