Αρχική Σελίδα Προστασία | Πρόσβαση Δεδομένων Dell

Η αρχική σελίδα **Προστασία | Πρόσβαση Δεδομένων Dell** είναι η αφετηρία για την πρόσβαση σε δυνατότητες αυτής της εφαρμογής. Από αυτό το παράθυρο, μπορείτε να αποκτήσετε πρόσβαση στα ακόλουθα:

System Access Wizard
Επιλογές Πρόσβασης
Self-Encrypting Drive
Επιλογές για Προχωρημένους

Στην κάτω δεξιά γωνία του παραθύρου υπάρχει ο σύνδεσμος **για προχωρημένους** τον οποίο μπορείτε να πατήσετε για να εισέλθετε στις επιλογές για προχωρημένους.

Από τις επιλογές για προχωρημένους, μπορείτε να κάνετε κλικ στο σύνδεσμο **αρχική** στην κάτω δεξιά γωνία του παραθύρου για να επιστρέψετε στην αρχική σελίδα.

Οδηγός Πρόσβασης Συστήματος

Το πρόγραμμα System Access Wizard εκκινείται αυτόματα την πρώτη φορά που εκκινείται η εφαρμογή **Προστασία | Πρόσβαση Δεδομένων Dell**. Αυτό το πρόγραμμα θα σας καθοδηγήσει στη διαδικασία εγκατάστασης όλων των θεμάτων ασφαλείας στο σύστημά σας, συμπεριλαμβανομένου του τρόπου (π.χ., μόνο κωδικός πρόσβασης ή δακτυλικό αποτύπωμα και κωδικός πρόσβασης) και του χρόνου (από τα Windows, pre-Windows ή και τα δύο) σύνδεσης στο σύστημα. Επιπλέον, εάν το σύστημά σας διαθέτει μονάδα self-encrypting drive, μπορείτε να τη διαμορφώσετε μέσω αυτού του προγράμματος.

Λειτουργίες Διαχειριστή

Οι χρήστες που έχουν ρυθμιστεί με προνόμια διαχειριστή των Windows στο σύστημα έχουν τα δικαιώματα να πραγματοποιούν τις ακόλουθες λειτουργίες στην **Πρόσβαση | Προστασία Δεδομένων Dell**, τις οποίες οι κοινοί χρήστες δεν μπορούν:

- Ορισμός / αλλαγή κωδικού πρόσβασης στο σύστημα (Pre-Windows)
- Ορισμός / αλλαγή κωδικού πρόσβασης σκληρού δίσκου
- Ορισμός / αλλαγή κωδικού πρόσβασης διαχειριστή
- Ορισμός / αλλαγή κωδικού πρόσβασης ιδιοκτήτη TPM
- Ορισμός / αλλαγή κωδικού πρόσβασης διαχειριστή ControlVault
- Επαναφορά συστήματος
- Αρχειοθέτηση και επαναφορά διαπιστευτηρίων
- Ορισμός / αλλαγή PIN διαχειριστή smartcard
- Απαλοιφή / επαναφορά μιας smartcard
- Ενεργοποίηση / απενεργοποίηση ασφαλούς σύνδεσης Dell στα Windows
- Θέσπιση πολιτικής σύνδεσης στα Windows
- Διαχείριση αυτο-κρυπτογραφούμενων μονάδων (self-encrypting drives), συμπεριλαμβανομένων των εξής:
    - Ενεργοποίηση / απενεργοποίηση κλειδώματος self-encrypting drive
    - Ενεργοποίηση / απενεργοποίηση Συγχρονισμού Κωδικού Πρόσβασης των Windows (WPS)
    - Ενεργοποίηση / απενεργοποίηση Single Sign On (SSO)
    - Εκτέλεση κρυπτογραφικής διαγραφής

Απομακρυσμένη Διαχείριση

Η επιχείρησή σας μπορεί να εγκαταστήσει ένα περιβάλλον στο οποίο γίνεται κεντροποιημένη διαχείριση των λειτουργιών ασφαλείας της εφαρμογής **Προστασία | Πρόσβαση Δεδομένων Dell** σε περισσότερες από μια πλατφόρμες (δηλ. απομακρυσμένη διαχείριση). Σε αυτή την περίπτωση, η υποδομή ασφαλείας των Windows, όπως ο Κατάλογος Αρχείων, μπορεί να χρησιμοποιηθεί για την ασφαλή διαχείριση συγκεκριμένων λειτουργιών της εφαρμογής **Προστασία | Πρόσβαση Δεδομένων Dell**.

Όταν η διαχείριση ενός υπολογιστή είναι απομακρυσμένη (π.χ. την "κατέχει" απομακρυσμένος διαχειριστής), η τοπική διαχείριση της λειτουργίας **Προστασία | Πρόσβαση Δεδομένων Dell** είναι απενεργοποιημένη και δεν θα υπάρχει τοπική πρόσβαση στο παράθυρο διαχείρισης της εφαρμογής. Η διαχείριση των ακόλουθων λειτουργιών μπορεί να γίνεται εξ αποστάσεως:

- Trusted Platform Module (TPM)
- ControlVault
- Σύνδεση Pre-Windows
- Επαναφορά Συστήματος
- Κωδικοί πρόσβασης BIOS
- Πολιτική Σύνδεσης στα Windows
- Self-Encrypting Drives
- Καταχώριση Δακτυλικών Αποτυπωμάτων και Smartcard

Για να ζητήσετε περισσότερες πληροφορίες σχετικά με τη χρήση του EMBASSY® Remote Administration Server (ERAS) της Wave Systems για απομακρυσμένη διαχείριση, επικοινωνήστε με τον πωλητή της Dell ή πηγαίνετε στην ιστοσελίδα dell.com.

Επιλογές Πρόσβασης

Από το παράθυρο Επιλογές Πρόσβασης, μπορείτε να ορίσετε τον τρόπο πρόσβασης στο σύστημά σας.

Εάν έχετε ρυθμίσει επιλογές για **Προστασία | Πρόσβαση Δεδομένων Dell**, αυτές θα εμφανιστούν στην αρχική σελίδα με τις διαθέσιμες επιλογές (π.χ., αλλαγή κωδικού πρόσβασης για Pre-Windows σύνδεση). Οι διαθέσιμες επιλογές αποτελούν συντομεύσεις οι οποίες, όταν κάνετε κλικ επάνω τους, σας μεταφέρουν στο κατάλληλο παράθυρο για εκτέλεση μιας συγκεκριμένης εργασίας (π.χ. αλλαγή του pre-Windows κωδικού πρόσβασής σας ή καταχώρηση ενός άλλου δακτυλικού αποτυπώματος).

Γενικά
Πρώτα, μπορείτε να καθορίσετε το πότε θα συνδέεστε (Windows, pre-Windows ή και τα δύο) και το πώς (π.χ. δακτυλικό αποτύπωμα και κωδικός πρόσβασης) θα συνδέεστε. Μπορείτε να επιλέξετε μία ή δύο επιλογές για τον τρόπο σύνδεσης, οι οποίες περιλαμβάνουν συνδυασμούς δακτυλικού αποτυπώματος, smartcard και κωδικού πρόσβασης. Οι επιλογές που παρατίθενται βασίζονται στις πολιτικές σύνδεσης που ισχύουν στο περιβάλλον σας και σε αυτά που υποστηρίζονται στην πλατφόρμα.

Δακτυλικό αποτύπωμα
Εάν το σύστημά σας περιέχει συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων, μπορείτε να καταχωρίσετε ή να ενημερώσετε δακτυλικά αποτυπώματα για χρήση κατά τη σύνδεση στο σύστημά σας. Αφού καταχωρίσετε δακτυλικά αποτυπώματα, μπορείτε να περάσετε το(τα) καταχωρημένο(α) δάκτυλο(α) στη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων του συστήματός σας για να αποκτήσετε πρόσβαση στο σύστημά σας σε Windows, pre-Windows ή και τα δύο (ανάλογα με το τι ορίσατε στις Γενικές Επιλογές Πρόσβασης). Ανατρέξτε στην ενότητα Καταχώριση Δακτυλικών Αποτυπωμάτων Χρήστη για περισσότερες πληροφορίες.

Σύνδεση Pre-Windows
Εάν ορίσατε ότι οι χρήστες πρέπει να συνδέονται σε pre-Windows, πρέπει να ορίσετε ένα Κωδικό Πρόσβασης στο Σύστημα (ορισμένες φορές αναφέρεται ως κωδικός πρόσβασης pre-Windows) για πρόσβαση pre-Windows. Μόλις τον ορίσετε, ο διαχειριστής μπορεί να αλλάξει τον κωδικό πρόσβασης οποιαδήποτε στιγμή.

Μπορείτε επίσης να απενεργοποιήσετε τη σύνδεση pre-Windows από αυτή την οθόνη. Για να το κάνετε αυτό, θα πρέπει να εισαγάγετε τον τρέχοντα Κωδικό Πρόσβασης στο Σύστημα, να επαληθεύσετε ότι ο κωδικός πρόσβασης είναι σωστός και στη συνέχεια να κάνετε κλικ στο κουμπί **Απενεργοποίηση**.

Smartcard
Εάν έχετε ορίσει ότι οι χρήστες πρέπει να χρησιμοποιούν smartcard για να συνδεθούν, πρέπει να καταχωρίσετε μία ή περισσότερες κλασσικές (με επαφές) ή contactless smartcard κάρτες. Κάντε κλικ στο σύνδεσμο **Καταχώριση μιας άλλης smartcard** για να εκκινήσετε το πρόγραμμα καταχώρισης smartcard. Καταχώριση σημαίνει εγκατάσταση της smartcard σας για χρήση κατά τη σύνδεση.

Αφού καταχωρίσετε μια smartcard, μπορείτε να αλλάξετε ή να ορίσετε ένα PIN για τη συγκεκριμένη κάρτα χρησιμοποιώντας το σύνδεσμο **Αλλαγή ή ορισμός του PIN της smartcard μου**.

Σύνδεση Pre-Windows

Όταν έχει ρυθμιστεί σύνδεση pre-Windows, πρέπει να παρέχετε έλεγχο ταυτότητας (κωδικός πρόσβασης, δακτυλικό αποτύπωμα ή smartcard) κατά την ενεργοποίηση του συστήματος ή πριν τη φόρτωση των Windows. Η λειτουργία σύνδεσης pre-Windows παρέχει πρόσθετη ασφάλεια στο σύστημα, εμποδίζοντας τους μη εξουσιοδοτημένους χρήστες να παρακάμψουν την ασφάλεια των Windows και να αποκτήσουν πρόσβαση στον υπολογιστή (π.χ., όταν έχει κλαπεί).

Από το παράθυρο Σύνδεση Pre-Windows, οι διαχειριστές μπορούν να ρυθμίσουν τη σύνδεση pre-Windows ή να δημιουργήσουν ή να αλλάξουν έναν κωδικό πρόσβασης pre-Windows (Σύστημα). Εάν αυτός ο κωδικός έχει ήδη ρυθμιστεί, μπορείτε να απενεργοποιήσετε τη σύνδεση pre-Windows από αυτό το παράθυρο. Η ρύθμιση σύνδεσης pre-Windows εκκινεί ένα πρόγραμμα το οποίο πραγματοποιεί τα ακόλουθα:

- Κωδικός Πρόσβασης στο Σύστημα: Ρυθμίζει έναν Κωδικό Πρόσβασης στο Σύστημα (αναφέρεται επίσης ως κωδικός πρόσβασης pre-Windows) για πρόσβαση pre-Windows. Αυτός ο κωδικός πρόσβασης χρησιμοποιείται επίσης ως εφεδρικός σε περιπτώσεις όπου ένας χρήστης έχει πρόσθετους συντελεστές ελέγχου ταυτότητας (π.χ., για να αποκτήσει πρόσβαση στο σύστημα εάν παρουσιαστεί πρόβλημα με τον αισθητήρα δακτυλικών αποτυπωμάτων).
- Δακτυλικό αποτύπωμα ή Smartcard: Ρυθμίζει ένα δακτυλικό αποτύπωμα ή μια smartcard για χρήση κατά τη σύνδεση pre-Windows και ορίζει εάν αυτός ο συντελεστής ελέγχου ταυτότητας θα χρησιμοποιείται αντί ή επιπλέον του κωδικού πρόσβασης pre-Windows.
- Single Sign On: Από προεπιλογή, ο έλεγχος ταυτότητάς σας pre-Windows (κωδικός πρόσβασης, δακτυλικό αποτύπωμα ή smartcard) θα χρησιμοποιείται και για την αυτόματη είσοδό σας στα Windows (αυτό ονομάζεται "Single Sign On"). Για να απενεργοποιήσετε αυτή τη λειτουργία, επιλέξτε το πλαίσιο ελέγχου "Θέλω να συνδέομαι πάλι στα Windows".
- Εάν έχει ρυθμιστεί κωδικός πρόσβασης Σκληρού Δίσκου στο BIOS επιπλέον του κωδικού πρόσβασης pre-Windows, έχετε επίσης την επιλογή να αλλάξετε ή να απενεργοποιήσετε τον κωδικό πρόσβασης σκληρού δίσκου.

ΣΗΜΕΙΩΣΗ: Δεν μπορούν να χρησιμοποιηθούν όλες οι συσκευές ανάγνωσης δακτυλικών αποτυπωμάτων για έλεγχο ταυτότητας pre-Windows. Εάν η συσκευή ανάγνωσης που έχετε δεν είναι συμβατή, μπορείτε να καταχωρίσετε δακτυλικά αποτυπώματα μόνο για σύνδεση στα Windows. Για να διαπιστώσετε εάν μια συγκεκριμένη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων είναι συμβατή, επικοινωνήστε με το διαχειριστή του συστήματός σας ή πηγαίνετε στην ιστοσελίδα support.dell.com για να δείτε έναν κατάλογο των υποστηριζόμενων συσκευών ανάγνωσης δακτυλικών αποτυπωμάτων.

Απενεργοποίηση Σύνδεσης Pre-Windows
Μπορείτε επίσης να απενεργοποιήσετε τη σύνδεση pre-Windows από αυτό το παράθυρο. Για να το κάνετε αυτό, θα πρέπει να εισαγάγετε τον τρέχοντα κωδικό πρόσβασης pre-Windows (Σύστημα), να επαληθεύσετε ότι ο κωδικός πρόσβασης είναι σωστός και στη συνέχεια να κάνετε κλικ στο κουμπί **Απενεργοποίηση**. Έχετε υπόψη σας ότι όταν απενεργοποιείτε τη σύνδεση pre-Windows, τα δακτυλικά αποτυπώματα ή οι κάρτες smartcard που έχουν καταχωρηθεί παραμένουν καταχωρημένες.

Καταχώρηση Δακτυλικών Αποτυπωμάτων

Οι χρήστες μπορούν να καταχωρήσουν ή να ενημερώσουν δακτυλικά αποτυπώματα τα οποία μπορούν να χρησιμοποιηθούν για έλεγχο ταυτότητας στο σύστημα για σύνδεση pre-Windows ή Windows. Στην καρτέλα Δακτυλικό αποτύπωμα, οι εικόνες των χεριών εμφανίζουν τα δάκτυλα που έχουν καταχωρηθεί, εάν υπάρχουν καταχωρημένα δάκτυλα. Κάνοντας κλικ στο σύνδεσμο **Καταχώριση ενός άλλου** εκκινείται το πρόγραμμα καταχώρισης δακτυλικών αποτυπωμάτων, το οποίο σας καθοδηγεί στη διαδικασία καταχώρισης. "Καταχώριση" σημαίνει αποθήκευση ενός δακτυλικού αποτυπώματος για χρήση κατά τη σύνδεση. Για να καταχωρίσετε δακτυλικά αποτυπώματα θα πρέπει να διαθέτετε μια έγκυρη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων ορθά εγκατεστημένη και διαμορφωμένη.

ΣΗΜΕΙΩΣΗ: Δεν μπορούν να χρησιμοποιηθούν όλες οι συσκευές ανάγνωσης δακτυλικών αποτυπωμάτων για σύνδεση pre-Windows. Ένα μήνυμα σφάλματος θα εμφανιστεί εάν επιχειρήσετε να πραγματοποιήσετε καταχώριση για pre-Windows με μια μη συμβατή συσκευή ανάγνωσης. Για να διαπιστώσετε εάν η συσκευή είναι συμβατή, επικοινωνήστε με το διαχειριστή του συστήματός σας ή πηγαίνετε στην ιστοσελίδα support.dell.com για να δείτε έναν κατάλογο των υποστηριζόμενων συσκευών ανάγνωσης δακτυλικών αποτυπωμάτων.

Όταν καταχωρείτε δακτυλικά αποτυπώματα, θα σας ζητηθεί να εισαγάγετε τον κωδικό πρόσβασής σας στα Windows για να επαληθεύσετε την ταυτότητά σας. Εάν το απαιτεί η πολιτική σας, θα σας ζητηθεί να εισαγάγετε επίσης τον Pre-Windows (Σύστημα) . Ο κωδικός πρόσβασης Pre-Windows μπορεί να χρησιμοποιηθεί για πρόσβαση στο σύστημα εάν παρουσιαστεί πρόβλημα με τη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων.

ΣΗΜΕΙΩΣΕΙΣ:

- Συνιστάται η καταχώριση τουλάχιστον δύο δακτυλικών αποτυπωμάτων κατά τη διαδικασία καταχώρισης.
- Πρέπει να διασφαλίζετε ότι τα δακτυλικά αποτυπώματα έχουν καταχωρηθεί σωστά πριν ενεργοποιήσετε τις δυνατότητες ελέγχου ταυτότητας δακτυλικών αποτυπωμάτων.
- Εάν αλλάξετε συσκευές ανάγνωσης δακτυλικών αποτυπωμάτων σε ένα σύστημα, πρέπει να επανακαταχωρίσετε δακτυλικά αποτυπώματα με τη νέα συσκευή ανάγνωσης. Δεν συνιστάται η εναλλαγή μεταξύ δύο διαφορετικών συσκευών δακτυλικών αποτυπωμάτων.
- Εάν δείτε επαναλαμβανόμενα μηνύματα "απώλεια εστίασης αισθητήρα" κατά την καταχώριση δακτυλικών αποτυπωμάτων, αυτό ίσως σημαίνει ότι ο υπολογιστής δεν αναγνωρίζει τη συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων. Εάν η συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων είναι εξωτερική, η αποσύνδεση και επανασύνδεση της συσκευής ανάγνωσης δακτυλικών αποτυπωμάτων συνήθως λύνει αυτό το πρόβλημα.

Διαγραφή Καταχωρημένων Δακτυλικών Αποτυπωμάτων
Μπορείτε να καταργήσετε καταχωρημένα δακτυλικά αποτυπώματα κάνοντας κλικ στο σύνδεσμο **Κατάργηση δακτυλικού αποτυπώματος** ή κάνοντας κλικ (για να το απο-επιλέξετε) επάνω σε ένα καταχωρημένο δάκτυλο στο πρόγραμμα καταχώρισης δακτυλικών αποτυπωμάτων.

Για να καταργήσετε ένα συγκεκριμένο χρήστη ο οποίος έχει καταχωρημένα δακτυλικά αποτυπώματα για έλεγχο ταυτότητας pre-Windows, ο διαχειριστής μπορεί να απο-επιλέξει όλα τα δακτυλικά αποτυπώματα που έχουν καταχωρηθεί για τον εν λόγω χρήστη.

ΣΗΜΕΙΩΣΗ: Εάν εμφανιστούν μηνύματα σφάλματος κατά τη διαδικασία καταχώρισης δακτυλικών αποτυπωμάτων, μπορείτε να ανατρέξετε στην ιστοσελίδα wave.com/support/Dell για πρόσθετες λεπτομέρειες.

Καταχώριση καρτών Smart Card

Η **Προστασία | Πρόσβαση Δεδομένων Dell** σας παρέχει την επιλογή χρήσης μιας κλασσικής (με επαφές) ή contactless smartcard για σύνδεση στο λογαριασμό σας στα Windows ή για έλεγχο ταυτότητας σε pre-Windows. Στην καρτέλα Smartcard, κάντε κλικ στο σύνδεσμο **Καταχώριση μιας άλλης smartcard** για να εκκινήσετε το πρόγραμμα καταχώρισης Smartcard, το οποίο σας καθοδηγεί στη διαδικασία καταχώρισης. "Καταχώριση" σημαίνει εγκατάσταση της smartcard σας για χρήση κατά τη σύνδεση.

Για να πραγματοποιήσετε καταχώριση θα πρέπει να διαθέτετε μια έγκυρη συσκευή ελέγχου ταυτότητας smartcard ορθά εγκατεστημένη και διαμορφωμένη.

ΣΗΜΕΙΩΣΗ: Για να διαπιστώσετε εάν μια συγκεκριμένη συσκευή είναι συμβατή, επικοινωνήστε με το διαχειριστή του συστήματός σας ή πηγαίνετε στην ιστοσελίδα support.dell.com για να δείτε έναν κατάλογο όλων των υποστηριζόμενων καρτών smartcard.

Καταχώριση
Όταν καταχωρείτε μια smartcard, θα σας ζητηθεί να εισαγάγετε τον κωδικό πρόσβασής σας στα Windows για να επαληθεύσετε την ταυτότητά σας. Εάν το απαιτεί η πολιτική σας, θα σας ζητηθεί να εισαγάγετε επίσης τον Pre-Windows (Σύστημα) . Ο κωδικός πρόσβασης Pre-Windows μπορεί να χρησιμοποιηθεί για πρόσβαση στο σύστημα εάν παρουσιαστεί πρόβλημα με τη συσκευή ανάγνωσης smartcard.

Κατά τη διάρκεια της καταχώρισης, θα σας ζητηθεί το PIN της smartcard, εάν έχετε ορίσει κάποιο. Εάν η πολιτική σας απαιτεί PIN και δεν έχετε ορίσει κάποιο, θα σας ζητηθεί να δημιουργήσετε ένα.

ΣΗΜΕΙΩΣΕΙΣ:

- Μόλις ένας χρήστης καταχωρηθεί για χρήση smartcard σε pre-Windows, δεν είναι δυνατή η κατάργηση αυτού του χρήστη.
- Οι κοινοί χρήστες μπορούν να αλλάξουν το PIN χρήστη σε μια smartcard, ενώ ο διαχειριστής μπορεί να αλλάξει τόσο το PIN διαχειριστή όσο και το PIN χρήστη.
- Ο διαχειριστής μπορεί επίσης να επαναφέρει μια smartcard. Μετά την επαναφορά της, η smartcard δεν μπορεί να χρησιμοποιηθεί για έλεγχο ταυτότητας κατά τη σύνδεση σε Windows ή pre-Windows πριν καταχωρηθεί και πάλι.

ΣΗΜΕΙΩΣΗ:Για έλεγχο ταυτότητας πιστοποιητικού TPM, οι διαχειριστές μπορούν να καταχωρίζουν πιστοποιητικά TPM μέσω της διαδικασίας καταχώρισης smartcard των Microsoft Windows. Οι διαχειριστές θα πρέπει να επιλέγουν το "Wave TCG-Enabled CSP" ως πάροχο υπηρεσιών κρυπτογράφησης (CSP) αντί ενός CSP Smartcard για συμβατότητα με την εφαρμογή αυτή. Επιπλέον, η ασφαλής σύνδεση Dell πρέπει να ενεργοποιηθεί με την κατάλληλη Πολιτική Τύπου Ελέγχου Ταυτότητας για τον πελάτη.

ΣΗΜΕΙΩΣΗ: Εάν εμφανιστεί ένα μήνυμα σφάλματος το οποίο δηλώνει ότι η Υπηρεσία Smartcard δεν λειτουργεί, μπορείτε να προβείτε σε έναρξη / επανέναρξη αυτής της υπηρεσίας πραγματοποιώντας τα εξής:

- Πλοηγηθείτε στο παράθυρο Εργαλεία Διαχείρισης από τον Πίνακα Ελέγχου, επιλέξτε Υπηρεσία, στη συνέχεια κάντε δεξί κλικ στο Smartcard και επιλέξτε Έναρξη ή Επανέναρξη.
- Εάν επιθυμείτε αναλυτικότερες πληροφορίες για ένα συγκεκριμένο μήνυμα σφάλματος, πηγαίνετε στην ιστοσελίδα wave.com/support/Dell.

Επισκόπηση Self-Encrypting Drive

Η **Προστασία | Πρόσβαση Δεδομένων Dell** διαχειρίζεται τις βασιζόμενες στον υλικό εξοπλισμό λειτουργίες ασφαλείας των μονάδων self-encrypting drive , οι οποίες διαθέτουν κρυπτογράφηση δεδομένων ενσωματωμένη στο υλικό της μονάδας. Αυτή η λειτουργία χρησιμοποιείται για να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε κρυπτογραφημένα δεδομένα (όταν είναι ενεργοποιημένο το κλείδωμα μονάδας).

Η πρόσβαση στο παράθυρο Self-Encrypting Drive γίνεται κάνοντας κλικ στην κάτω καρτέλα **Self-Encrypting Drive**. Η καρτέλα αυτή εμφανίζεται μόνο όταν υπάρχουν στο σύστημά σας μία ή περισσότερες μονάδες self-encrypting drive (SED).

Κάντε κλικ στο σύνδεσμο **Εγκατάσταση** για να ξεκινήσει το πρόγραμμα εγκατάστασης Self-Encrypting Drive. Στο πρόγραμμα αυτό, θα δημιουργήσετε έναν κωδικό πρόσβασης Διαχειριστή Μονάδας, θα δημιουργήσετε αντίγραφο ασφαλείας αυτού του κωδικού και θα εφαρμόσετε τις ρυθμίσεις κρυπτογράφησης που θα πραγματοποιήσετε στη μονάδα. Μόνο διαχειριστές συστήματος μπορούν να έχουν πρόσβαση στο πρόγραμμα εγκατάστασης Self-Encrypting Drive.

Σημαντικό! Μετά την εγκατάσταση της μονάδας, η προστασία δεδομένων και το κλείδωμα μονάδας "ενεργοποιούνται". Όταν μια μονάδα είναι κλειδωμένη, ισχύει η ακόλουθη συμπεριφορά:

- Η μονάδα εισέρχεται στην *κλειδωμένη* κατάσταση όποτε απενεργοποιείτε την τροφοδοσία στη μονάδα.
- Δεν θα γίνει εκκίνηση της μονάδας μέχρι ο χρήστης να εισάγει το σωστό όνομα χρήστη και κωδικό πρόσβασης (ή δακτυλικό αποτύπωμα) στην οθόνη σύνδεσης Pre-Windows. Πριν ενεργοποιηθεί το κλείδωμα μονάδας, κάθε χρήστης του υπολογιστή μπορεί να έχει πρόσβαση στα δεδομένα της μονάδας.
- Η μονάδα είναι ασφαλής ακόμα και εάν συνδεθεί σε έναν άλλο υπολογιστή ως δευτερεύουσα μονάδα δίσκου. Για την πρόσβαση στα δεδομένα της μονάδας απαιτείται έλεγχος ταυτότητας.

Μετά την εγκατάσταση της μονάδας, το παράθυρο Self-Encrypting Drive θα εμφανίσει τη μονάδα (ή τις μονάδες) και ένα σύνδεσμο μέσω του οποίου οι χρήστες μπορούν να αλλάξουν τον κωδικό πρόσβασής τους στη μονάδα. Εάν είστε διαχειριστής μονάδας, από αυτό το παράθυρο μπορείτε επίσης να προσθέσετε ή να καταργήσετε χρήστες μονάδας. Εάν υπάρχει εξωτερική μονάδα η οποία έχει εγκατασταθεί, θα εμφανιστεί στο παράθυρο αυτό και μπορείτε να την ξεκλειδώσετε.

ΣΗΜΕΙΩΣΗ: Για να κλειδώσετε μια δευτερεύουσα, , εξωτερική μονάδα, η τροφοδοσία στη μονάδα πρέπει να γίνει ανεξάρτητα από την τροφοδοσία του υπολογιστή.

Ο διαχειριστής μονάδας μπορεί να διαχειριστεί τις ρυθμίσεις της μονάδας στο **Για προχωρημένους>Συσκευές**. Για περισσότερες πληροφορίες, βλ. Διαχείριση Συσκευών-Μονάδες Self-Encrypting Drive.

Εγκατάσταση Μονάδας

Το πρόγραμμα εγκατάστασης Self-Encrypting Drive θα σας καθοδηγήσει στη διαδικασία εγκατάστασης της μονάδας (ή των μονάδων) σας. Είναι σημαντικό να έχετε υπόψη σας τα ακόλουθα ζητήματα όταν πραγματοποιείτε αυτή τη διαδικασία.

Διαχειριστής Μονάδας
Ο πρώτος χρήστης με δικαιώματα διαχειριστή συστήματος ο οποίος ρυθμίζει την πρόσβαση στη μονάδα (και ορίζει τον κωδικό πρόσβασης του Διαχειριστή Μονάδας) γίνεται ο Διαχειριστής Μονάδας. Αυτός είναι ο μοναδικός χρήστης που έχει δικαιώματα να κάνει αλλαγές στην πρόσβαση στη μονάδα. Για να διασφαλίσετε ότι ο πρώτος χρήστης ρυθμίζεται εκούσια ως

διαχειριστής συστήματος, πρέπει να επιλέξετε το πλαίσιο ελέγχου "Κατανοώ" για να συνεχίσετε σε αυτό το βήμα.

Κωδικός Πρόσβασης Διαχειριστή Μονάδας
Το πρόγραμμα σας παροτρύνει να δημιουργήσετε έναν κωδικό πρόσβασης Διαχειριστή Μονάδας και να επανεισαγάγετε αυτόν τον κωδικό για να τον επιβεβαιώσετε. Πρέπει να εισαγάγετε τον κωδικό πρόσβασής σας στα Windows για να επιβεβαιώσετε την ταυτότητά σας πριν μπορέσετε να δημιουργήσετε τον κωδικό πρόσβασης Διαχειριστή Μονάδας. Ο τρέχον χρήστης των Windows πρέπει να έχει δικαιώματα διαχειριστή για να δημιουργήσει αυτόν τον κωδικό πρόσβασης.

Αντίγραφο Ασφαλείας Διαπιστευτηρίων Μονάδας
Πληκτρολογήστε μια τοποθεσία ή κάντε κλικ στο κουμπί **Αναζήτηση** για να επιλέξετε μια τοποθεσία στην οποία θα αποθηκεύσετε ένα αντίγραφο ασφαλείας των διαπιστευτηρίων σας ως διαχειριστής μονάδας.

ΣΗΜΑΝΤΙΚΟ**!**

- Συνιστάται θερμά η δημιουργία αντιγράφου ασφαλείας αυτών των διαπιστευτηρίων και η αποθήκευση αυτού του αντιγράφου σε μια μονάδα δίσκου διαφορετική από τον κύριο σκληρό δίσκο σας (π.χ., αφαιρούμενο μέσο). Διαφορετικά, εάν χάσετε την πρόσβαση στη μονάδα δίσκου σας δεν θα μπορείτε να έχετε πρόσβαση στο αντίγραφο ασφαλείας που δημιουργήσατε.
- Αφού ολοκληρώσετε την εγκατάσταση της μονάδας, οιχρήστες θα πρέπει να εισάγουν το σωστό όνομα χρήστη και κωδικό πρόσβασης (ή δακτυλικό αποτύπωμα) πριν τη φόρτωση των Windows προκειμένου να εισέλθουν στο σύστημα την επόμενη φορά που το σύστημα θα ενεργοποιηθεί.

Προσθήκη Χρήστη Μονάδας
Ο διαχειριστής μονάδας μπορεί να προσθέσει άλλους χρήστες στη μονάδα, οι οποίοι είναι έγκυροι χρήστες των Windows. Κατά την προσθήκη χρηστών στη μονάδα, ο διαχειριστής έχει την επιλογή να ζητήσει από το χρήστη να προβεί σε επαναφορά του κωδικού πρόσβασής του μόλις συνδεθεί για πρώτη φορά. Θα ζητηθεί από το χρήστη να επαναφέρει τον κωδικό πρόσβασής του στην οθόνη ελέγχου ταυτότητας pre-Windows πριν ξεκλειδώσει η μονάδα.

Ρυθμίσεις για προχωρημένους

- *Single Sign On* - Από προεπιλογή, ο κωδικός πρόσβασής σας Self-Encrypting Drive, τον οποίο εισάγετε πριν τη φόρτωση των Windows για τον έλεγχο ταυτότητάς σας στη μονάδα, θα χρησιμοποιείται και για την αυτόματη είσοδό σας στα Windows (αυτό ονομάζεται "Single Sign On"). Για να απενεργοποιήσετε αυτή τη λειτουργία, επιλέξτε το πλαίσιο ελέγχου "Θέλω να συνδέομαι πάλι όταν γίνεται έναρξη των Windows" όταν διαμορφώνετε τις ρυθμίσεις μονάδας.
- *Σύνδεση με Δακτυλικό Αποτύπωμα* - Στις υποστηριζόμενες πλατφόρμες, μπορείτε να ορίσετε να γίνεται έλεγχος της ταυτότητάς σας στη μονάδα self-encrypting drive χρησιμοποιώντας ένα δακτυλικό αποτύπωμα αντί για έναν κωδικό πρόσβασης.
- *Υποστήριξη Αναστολής/Αναμονής (S3)* (εάν υποστηρίζεται στην πλατφόρμα) - Εάν αυτή η δυνατότητα είναι ενεργοποιημένη, η μονάδα self-encrypting drive μπορεί να τεθεί με ασφάλεια σε κατάσταση Αναστολής/Αναμονής (αναφέρεται επίσης ως κατάσταση S3) και θα απαιτεί έλεγχο ταυτότητας pre-Windows όταν επανέλθει από την κατάσταση Αναστολής/Αναμονής.

ΣΗΜΕΙΩΣΕΙΣ:

- Όταν η Υποστήριξη S3 είναι ενεργοποιημένη, οι κωδικοί πρόσβασης κρυπτογράφησης μονάδας δίσκου υπόκειται σε οποιονδήποτε περιορισμό κωδικού πρόσβασης του BIOS που μπορεί να υπάρχει. Συμβουλευτείτε τον κατασκευαστή του υλικού του συστήματος για περισσότερες πληροφορίες σχετικά με οποιονδήποτε περιορισμό κωδικού πρόσβασης του BIOS που μπορεί να υπάρχει για το σύστημα.

- Δεν υποστηρίζουν όλες οι μονάδες self-encrypting drive την κατάσταση S3. Κατά την εγκατάσταση της μονάδας, θα ενημερωθείτε για το εάν η μονάδα υποστηρίζει ή όχι την κατάσταση Αναμονής/Αναστολής. Για μονάδες που δεν υποστηρίζουν αυτή την κατάσταση, τα αιτήματα S3 των Windows θα μετατρέπονται αυτόματα σε αιτήματα αδρανοποίησης, εάν έχει ενεργοποιηθεί η λειτουργία αδρανοποίησης (συνιστάται θερμά να ενεργοποιήσετε τη λειτουργία αδρανοποίησης στον υπολογιστή σας).
- Την πρώτη φορά που θα συνδεθείτε μετά τη ρύθμιση της επιλογής Single Sign On (SSO), η διαδικασία θα σταματήσει προσωρινά στην παρότρυνση σύνδεσης στα Windows. Θα σας ζητηθεί να εισαγάγετε τη δική σας μορφή ελέγχου ταυτότητας στα Windows, η οποία θα αποθηκευτεί με ασφάλεια για μελλοντικές προσπάθειες σύνδεσης στα Windows. Την επόμενη φορά που θα γίνει εκκίνηση του συστήματος, η λειτουργία SSO θα σας συνδέσει αυτόματα στα Windows. Η ίδια διαδικασία απαιτείται επίσης όταν αλλάξει ο έλεγχος ταυτότητας ενός χρήστη στα Windows (κωδικός πρόσβασης, δακτυλικό αποτύπωμα, PIN Smartcard). Εάν ο υπολογιστής βρίσκεται σε τομέα και αυτός ο τομέας διαθέτει πολιτική η οποία απαιτεί το πάτημα των πλήκτρων ctrl+alt+del για σύνδεση στα Windows, θα τηρηθεί η συγκεκριμένη πολιτική.

ΠΡΟΣΟΧΗ! Εάν απεγκαταστήσετε την εφαρμογή **Προστασία | Πρόσβαση Δεδομένων Dell**, πρέπει πρώτα να απενεργοποιήσετε την προστασία δεδομένων στη μονάδα self-encrypting drive και να ξεκλειδώσετε τη μονάδα.

Λειτουργίες Χρήστη SED

Οι διαχειριστές μονάδων self-encrypting drive πραγματοποιούν κάθε εργασία διαχείρισης σχετικά με την ασφάλεια και τους χρήστες των μονάδων. Οι χρήστες των μονάδων που δεν είναι διαχειριστές των μονάδων μπορούν να πραγματοποιούν μόνο τις ακόλουθες εργασίες:

- Αλλαγή του δικού τους κωδικού πρόσβασης
- Ξεκλείδωμα μονάδας

Η πρόσβαση σε αυτές τις εργασίες γίνεται από την καρτέλα **Self-Encrypting Drive** στην **Προστασία | Πρόσβαση Δεδομένων Dell**.

Αλλαγή κωδικού πρόσβασης
Επιτρέπει στους καταχωρισμένους χρήστες να δημιουργήσουν το νέο τους κωδικό πρόσβασης ελέγχου ταυτότητας μονάδας. Πρέπει να εισαγάγετε τον τρέχοντα κωδικό πρόσβασης Self-Encrypting Drive πριν ο κωδικός πρόσβασης μονάδας οριστεί στη νέα τιμή.

ΣΗΜΕΙΩΣΕΙΣ:

- Η εφαρμογή ενισχύει το μήκος του κωδικού πρόσβασης και τις πολιτικές περιπλοκότητας του κωδικού πρόσβασης στα Windows, εάν είναι ενεργοποιημένες. Εάν οι πολιτικές κωδικού πρόσβασης στα Windows δεν είναι ενεργοποιημένες, το μέγιστο μήκος για τον κωδικό πρόσβασης μιας μονάδας Self-Encrypting Drive είναι 32 χαρακτήρες. Έχετε υπόψη σας ότι το μέγιστο μήκος είναι 127 χαρακτήρες εάν η λειτουργία S3 (Αναστολή/Αναμονή) δεν είναι ενεργοποιημένη.
- Ο κωδικός πρόσβασης ενός χρήστη για τη μονάδα Self-Encrypting Drive είναι διαφορετικός από τον κωδικό πρόσβασης στα Windows. Όταν έχει γίνει αλλαγή ή επαναφορά του κωδικού πρόσβασης ενός χρήστη για τα Windows, αυτό δεν επηρεάζει τον κωδικό πρόσβασης του χρήστη για τη μονάδα, εκτός εάν έχει ενεργοποιηθεί ο Συγχρονισμός Κωδικού Πρόσβασης στα Windows. Για λεπτομέρειες, ανατρέξτε στην ενότητα Συσκευές: Μονάδες Self-Encrypting Drive.
- Σε μερικά μη αγγλικά πληκτρολόγια, υπάρχει ένα σύνολο απαγορευμένων χαρακτήρων, οι οποίοι δεν μπορούν να χρησιμοποιηθούν για τον κωδικό πρόσβασης σε μονάδα self-encrypting drive. Εάν ο κωδικός πρόσβασης των Windows περιλαμβάνει κάποιον από τους απαγορευμένους χαρακτήρες και ο Συγχρονισμός Κωδικού Πρόσβασης στα Windows είναι ενεργοποιημένος, ο συγχρονισμός θα αποτύχει και θα προκύψει ένα μήνυμα σφάλματος.

Ξεκλείδωμα Μονάδας
Το Ξεκλείδωμα Μονάδας επιτρέπει σε έναν καταχωρισμένο χρήστη της μονάδας να ξεκλειδώσει μια κλειδωμένη μονάδα . Εάν το κλείδωμα μονάδας είναι ενεργοποιημένο, η μονάδα εισέρχεται στην κλειδωμένη κατάσταση όποτε απενεργοποιείτε την τροφοδοσία του υπολογιστή. Όταν η τροφοδοσία του συστήματος ενεργοποιηθεί ξανά, πρέπει να πραγματοποιήσετε έλεγχο ταυτότητας στη μονάδα εισάγοντας τον κωδικό πρόσβασής σας στην οθόνη ελέγχου ταυτότητας pre-Windows.

ΣΗΜΕΙΩΣΕΙΣ:

- Η είσοδος στη λειτουργία εξοικονόμησης ενέργειας (δηλ. Αναστολή/Αναμονή ή Αδρανοποίηση) ίσως να μην είναι εφικτή όταν πολλοί λογαριασμοί χρήστη self-encrypting drive είναι ταυτόχρονα ενεργοί στον υπολογιστή.
- Στην οθόνη ελέγχου ταυτότητας pre-Windows, τα "Χρήστης 1", "Χρήστης 2" κλπ. υποκαθιστούν τα ονόματα χρήστη μονάδων σε εκδόσεις της εφαρμογής στις οποίες έχει γίνει τοπική προσαρμογή για τις παρακάτω γλώσσες: Κινεζικά, Ιαπωνικά, Κορεατικά και Ρώσικα.

Επιλογές για Προχωρημένους

Οι επιλογές για Προχωρημένους στην **Προστασία | Πρόσβαση Δεδομένων Dell** επιτρέπουν σε ένα χρήστη με προνόμια διαχειριστή να διαχειρίζεται τα ακόλουθα θέματα της εφαρμογής:

Συντήρηση
Κωδικοί Πρόσβασης
Συσκευές

ΣΗΜΕΙΩΣΗ: Μόνο χρήστες με προνόμια διαχειριστή μπορούν να κάνουν τροποποιήσεις στις επιλογές για Προχωρημένους.Οι κοινοί χρήστες μπορούν να βλέπουν αυτές τις ρυθμίσεις,αλλά δεν μπορούν να κάνουν αλλαγές.

Συντήρηση

Το παράθυρο Συντήρηση μπορεί να χρησιμοποιηθεί από διαχειριστές για ρύθμιση των προτιμήσεων σύνδεσης στα Windows, για επαναφορά ενός συστήματος για προετοιμασία του για άλλο σκοπό, καθώς και για αρχειοθέτηση ή επαναφορά διαπιστευτηρίων αποθηκευμένων στο υλικό ασφαλείας του συστήματος. Για λεπτομέρειες, ανατρέξτε στα ακόλουθα θέματα:

Προτιμήσεις Πρόσβασης
Επαναφορά Συστήματος
Αρχειοθέτηση & Επαναφορά Διαπιστευτηρίων

Προτιμήσεις Πρόσβασης

Το παράθυρο Προτιμήσεις Πρόσβασης επιτρέπει στους διαχειριστές να ορίζουν προτιμήσεις για σύνδεση Windows για όλους τους χρήστες του συστήματος.

ΕνεργοποίησηΑσφαλής Σύνδεση Dell
Η επιλογή αντικατάστασης της τυπικής οθόνης ctrl-alt-delete των Windows σας επιτρέπει να χρησιμοποιείτε διάφορους συντελεστές ελέγχου ταυτότητας αντί του (ή επιπλέον του) κωδικού πρόσβασης των Windows για πρόσβαση στα Windows. Μπορείτε να επιλέξετε να προσθέσετε ένα δακτυλικό αποτύπωμα ως δεύτερο συντελεστή ελέγχου ταυτότητας για να ενισχύσετε την ασφάλεια της διαδικασίας σύνδεσης στα Windows. Επιπλέον συντελεστές ελέγχου ταυτότητας μπορούν επίσης να προστεθούν για σύνδεση στα Windows, συμπεριλαμβανομένης μιας smartcard ή ενός πιστοποιητικού TPM.

ΣΗΜΕΙΩΣΕΙΣ:

- Η ενεργοποίηση της Ασφαλούς σύνδεσης Dell επηρεάζει όλους τους χρήστες στο σύστημα.
- Συνιστάται αυτή η επιλογή να ενεργοποιηθεί ΑΦΟΥ οι χρήστες καταχωρίσουν τα δακτυλικά αποτυπώματά τους ή τη smartcard.
- Την πρώτη φορά που συνδέεστε μετά τη ρύθμιση αυτής της επιλογής, θα σας ζητηθεί έλεγχος ταυτότητας στα Windows σύμφωνα με τη συνήθη πολιτική και θα πρέπει να χρησιμοποιήσετε το νέο συντελεστή (ή συντελεστές) ελέγχου ταυτότητας κατά την επόμενη εκκίνηση.

Απενεργοποίηση Ασφαλούς σύνδεσης Dell
Αυτή η επιλογή απενεργοποιεί όλες τις λειτουργίες **Προστασία | Πρόσβαση Δεδομένων Dell** για σύνδεση στα Windows. Όταν την επιλέξετε, θα επιστρέψετε στη συνήθη πολιτική σύνδεσης στα Windows.

ΣΗΜΕΙΩΣΕΙΣ:

- Εάν λάβετε ένα σφάλμα σχετικά με την Ασφαλή σύνδεση στα Windows όταν επιχειρήσετε να συνδεθείτε, απενεργοποιήσετε και ενεργοποιήστε ξανά την επιλογή Ασφαλής σύνδεση Dell.
- Εάν επιθυμείτε αναλυτικότερες πληροφορίες για ένα συγκεκριμένο μήνυμα σφάλματος, πηγαίνετε στην ιστοσελίδα wave.com/support/Dell.

Επαναφορά Συστήματος

Η λειτουργία Επαναφορά Συστήματος χρησιμοποιείται για την απαλοιφή των δεδομένων όλων των χρηστών από όλο τον υλικό εξοπλισμό ασφαλείας στην πλατφόρμα· μπορεί, για παράδειγμα, να χρησιμοποιηθεί όταν αλλάζει ο σκοπός ενός υπολογιστή. Αυτή η επιλογή απαλείφει όλους τους κωδικούς πρόσβασης στο σύστημα, εκτός από τους κωδικούς πρόσβασης των χρηστών των Windows, καθώς και όλα τα δεδομένα στις συσκευές υλικού (δηλ., ControlVault, TPM και συσκευές ανάγνωσης δακτυλικών αποτυπωμάτων). Στις μονάδες self-encrypting drive, αυτή η λειτουργία απενεργοποιεί επίσης την προστασία δεδομένων, ώστε η μονάδα να είναι προσβάσιμη.

Πρέπει πρώτα να επιβεβαιώσετε ότι κατανοείτε το γεγονός ότι προβαίνετε σε επαναφορά του συστήματος και στη συνέχεια να κάνετε κλικ στο **Επόμενο**. Για να πραγματοποιήσετε επαναφορά του συστήματος, θα σας ζητηθεί να εισαγάγετε τον κωδικό πρόσβασης για κάθε συσκευή ασφαλείας, εάν έχετε ορίσει τέτοιους κωδικούς:

- Ιδιοκτήτης TPM
- Διαχειριστής ControlVault
- Διαχειριστής BIOS
- Σύστημα BIOS (pre-Windows)
- Σκληρός Δίσκος (BIOS)
- Διαχειριστής Self-Encrypting Drive

ΣΗΜΕΙΩΣΗ: Για τις μονάδες self-encrypting drive, απαιτείται μόνο ο κωδικός πρόσβασης του διαχειριστή της μονάδας, όχι οι κωδικοί πρόσβασης όλων των χρηστών της μονάδας.

Σημαντικό! Ο μόνος τρόπος ανάκτησης οποιονδήποτε δεδομένων που έχουν διαγραφεί κατά την επαναφορά του συστήματος είναι να τα ανακτήσετε από ένα αρχείο που είχατε προηγουμένως αποθηκεύσει. Εάν δεν διαθέτετε τέτοιο αρχείο, τα δεδομένα δεν μπορούν να ανακτηθούν. Σε μια μονάδα self-encrypting drive διαγράφονται μόνο τα δεδομένα εγκατάστασης, ενώ δεν διαγράφεται κανένα από τα προσωπικά δεδομένα που υπάρχουν στη μονάδα.

Αρχειοθέτηση & Επαναφορά Διαπιστευτηρίων

Η λειτουργία Αρχειοθέτηση και Επαναφορά Διαπιστευτηρίων χρησιμοποιείται για τη δημιουργία αντιγράφων ασφαλείας και την επαναφορά όλων των διαπιστευτηρίων χρήστη (πληροφορίες σύνδεσης και κρυπτογράφησης) που είναι αποθηκευμένα στο ControlVault και το Trusted Platform Module (TPM). Ένα αντίγραφο ασφαλείας αυτών των δεδομένων είναι σημαντικό κατά την επανα-τροφοδότηση ενός υπολογιστή ή για την αποκατάσταση δεδομένων σε περίπτωση αστοχίας υλικού. Στην περίπτωση αυτή, μπορείτε απλώς να επαναφέρετε όλα τα διαπιστευτήριά σας στο νέο σας υπολογιστή από ένα αποθηκευμένο αρχείο αρχειοθέτησης.

Μπορείτε να επιλέξετε να αρχειοθετήσετε ή να επαναφέρετε διαπιστευτήρια για ένα μόνο χρήστη ή για όλους τους χρήστες στο σύστημα.

Τα διαπιστευτήρια χρήστη αποτελούνται από δεδομένα που χρησιμοποιούνται σε pre-Windows, όπως καταχωρημένα δακτυλικά αποτυπώματα και δεδομένα smartcard, καθώς και κλειδιά αποθηκευμένα στο TPM. Το TPM θα δημιουργήσει κλειδιά όπως ζητείται από ασφαλείς εφαρμογές, για παράδειγμα, η δημιουργία ενός ψηφιακού πιστοποιητικού θα δημιουργήσει κλειδιά στο TPM.

ΣΗΜΕΙΩΣΗ: Για να διαπιστώσετε εάν τα κλειδιά TPM μπορούν να αρχειοθετηθούν από την **Προστασία | Πρόσβαση Δεδομένων Dell**, συμβουλευτείτε την τεκμηρίωση για την ασφαλή εφαρμογή. Γενικά, υποστηρίζονται εφαρμογές που χρησιμοποιούν το “Wave TCG-Enabled CSP” για τη δημιουργία κλειδιών.

Αρχειοθέτηση Διαπιστευτηρίων
Για να αρχειοθετήσετε διαπιστευτήρια, πρέπει να πραγματοποιήσετε τα εξής:

- Διευκρινίστε εάν αρχειοθετείτε διαπιστευτήρια για τον εαυτό σας ή για όλους τους χρήστες στο σύστημα.
- Παρέχετε έλεγχο ταυτότητας στο υλικό ασφαλείας πληκτρολογώντας τον κωδικό πρόσβασης σύστημα (pre-Windows), τον κωδικό πρόσβασης του διαχειριστή ControlVault και τον κωδικό πρόσβασης του ιδιοκτήτη TPM.
- Δημιουργήστε έναν κωδικό πρόσβασης στο αντίγραφο ασφαλείας διαπιστευτηρίων.
- Καθορίστε μια τοποθεσία αρχείου, χρησιμοποιώντας το κουμπί **Αναζήτηση** . Η τοποθεσία αρχείου πρέπει να είναι αφαιρούμενο μέσο, όπως μια μονάδα USB flash ή μια μονάδα δικτύου, για προστασία από βλάβη του σκληρού δίσκου.

Σημαντικές Σημειώσεις:
- Σημειώστε την τοποθεσία αρχείου, καθώς ο χρήστης θα χρειαστεί αυτές τις πληροφορίες για να επαναφέρει τις πληροφορίες διαπιστευτηρίων.
- Σημειώστε τον κωδικό πρόσβασης στο αντίγραφο ασφαλείας των διαπιστευτηρίων για να εξασφαλίσετε τη δυνατότητα επαναφοράς των δεδομένων. Αυτό είναι σημαντικό, καθώς δεν είναι δυνατή η ανάκτηση του κωδικού πρόσβασης.
- Εάν δεν γνωρίζετε τον κωδικό πρόσβασης του ιδιοκτήτη TPM, επικοινωνήστε με το διαχειριστή του συστήματος ή ανατρέξτε στις οδηγίες εγκατάστασης του TPM στον υπολογιστή.

Επαναφορά Διαπιστευτηρίων
Για να επαναφέρετε διαπιστευτήρια, πρέπει να πραγματοποιήσετε τα εξής:

- Διευκρινίστε εάν επαναφέρετε διαπιστευτήρια για τον εαυτό σας ή για όλους τους χρήστες στο σύστημα.
- Μεταβείτε στην τοποθεσία αρχείου και επιλέξτε το αρχείο αρχειοθέτησης.
- Εισαγάγετε τον κωδικό πρόσβασης στο αντίγραφο ασφαλείας των διαπιστευτηρίων που δημιουργήσατε κατά τη δημιουργία του αρχείου.

- Παρέχετε έλεγχο ταυτότητας στο υλικό ασφαλείας πληκτρολογώντας τον κωδικό πρόσβασης στο σύστημα (pre-Windows), τον κωδικό πρόσβασης του διαχειριστή ControlVault και τον κωδικό πρόσβασης του ιδιοκτήτη TPM.

ΣΗΜΕΙΩΣΕΙΣ:

- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι η επαναφορά διαπιστευτηρίων απέτυχε και προσπαθήσατε αρκετές φορές να πραγματοποιήσετε επαναφορά, επιχειρήστε να επαναφέρετε ένα διαφορετικό αρχείο αρχειοθέτησης. Εάν αυτό δεν πετύχει, δημιουργήστε ένα άλλο αρχείο διαπιστευτηρίων και προσπαθήστε να πραγματοποιήσετε επαναφορά από το νέο αρχείο.
- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι δεν ήταν δυνατή η ανάκτηση των κλειδιών TPM, δημιουργήστε ένα αρχείο διαπιστευτηρίων και στη συνέχεια διαγράψτε το TPM στο BIOS. Για διαγράψτε το TPM, επανεκκινήστε τον υπολογιστή σας, πιέστε το πλήκτρο **F2** κατά την επανέναρξη για να εισέλθετε στις ρυθμίσεις BIOS, και στη συνέχεια πλοηγηθείτε στο Ασφάλεια>TPM Ασφάλεια. Κατόπιν εδραιώστε ξανά την ιδιοκτησία του TPM και προσπαθήστε να επαναφέρετε πάλι τα διαπιστευτήρια.
- Εάν επιθυμείτε αναλυτικότερες πληροφορίες για ένα συγκεκριμένο μήνυμα σφάλματος, πηγαίνετε στην ιστοσελίδα wave.com/support/Dell.

Διαχείριση Κωδικών Πρόσβασης

Από το παράθυρο Διαχείριση Κωδικών Πρόσβασης, ένας διαχειριστής μπορεί να δημιουργήσει ή να αλλάξει όλους τους κωδικούς ασφαλείας στο σύστημά σας:

- Σύστημα (αναφέρεται επίσης ως Pre-Windows)*
- Διαχειριστής*
- Σκληρός Δίσκος*
- ControlVault
- Ιδιοκτήτης TPM
- Κύριος κωδικός TPM
- TPM Password Vault
- Self-Encrypting Drive

ΣΗΜΕΙΩΣΕΙΣ:

- Εμφανίζονται μόνο οι κωδικοί πρόσβασης που ισχύουν για την τρέχουσα διαμόρφωση της πλατφόρμας, επομένως αυτό το παράθυρο αλλάζει ανάλογα με τη διαμόρφωση και την κατάσταση του συστήματος.
- Οι κωδικοί πρόσβασης με ένα * δίπλα τους είναι κωδικοί πρόσβασης στο BIOS και μπορούν επίσης να αλλάξουν μέσω του BIOS του συστήματος.
- Δεν είναι δυνατή η δημιουργία ή η αλλαγή κωδικών πρόσβασης επιπέδου BIOS εάν ο διαχειριστής του BIOS έχει αρνηθεί αλλαγές στους κωδικούς πρόσβασης.
- Κάνοντας κλικ στο σύνδεσμο **εγκατάσταση** για ένα self-encrypting drive, εκκινείται το πρόγραμμα εγκατάστασης Self-Encrypting Drive, ενώ κάνοντας κλικ στο **διαχείριση** ο χρήστης μπορεί να αλλάξει έναν ή περισσότερους κωδικούς Self-Encrypting Drive.
- Κάνοντας κλικ στο σύνδεσμο **διαχείριση** για το TPM Password Vault εμφανίζεται ένα παράθυρο στο οποίο μπορείτε να δείτε ή να αλλάξετε τους κωδικούς πρόσβασης που προστατεύουν τα κλειδιά TPM. Όταν δημιουργηθεί ένα κλειδί TPM που απαιτεί κωδικό πρόσβασης, ο κωδικός πρόσβασης δημιουργείται τυχαία και αποθηκεύεται στο vault. Δεν μπορείτε να διαχειριστείτε το TPM Password Vault μέχρι να δημιουργήσετε έναν κύριο κωδικό πρόσβασης TPM.

Κανόνες ΠεριπλοκότηταςΚωδικού Πρόσβασηςτων Windows

Η **Προστασία | Πρόσβαση Δεδομένων Dell** εξασφαλίζει ότι ο παρακάτω κωδικός πρόσβασης συμορφώνεται με τους κανόνες περιπλοκότητας κωδικού πρόσβασης των Windows για τον υπολογιστή:

- Κωδικός πρόσβασης ιδιοκτήτηTPM

Για να καθορίσετε την πολιτική περιπλοκότητας κωδικού πρόσβασης των Windows για έναν υπολογιστή, ακολουθήστε αυτά τα βήματα:

1. Εισέλθετε στον Πίνακα Ελέγχου.
2. Κάντε διπλό κλικ στην επιλογή Εργαλεία Διαχείρισης.
3. Κάντε διπλό κλικ στην επιλογή Τοπική Πολιτική Ασφαλείας.
4. Αναπτύξτε το μενού Πολιτικές Λογαριασμού και επιλέξτε Πολιτική Κωδικού Πρόσβασης.

Συσκευές

Το παράθυρο Συσκευές χρησιμοποιείται από διαχειριστές για τη διαχείριση όλων των συσκευών ασφαλείας που έχουν εγκατασταθεί στο σύστημά τους. Για κάθε συσκευή, μπορείτε να προβάλλετε την κατάσταση και πρόσθετες αναλυτικές πληροφορίες, όπως έκδοση υλικολογισμικού (firmware). Κάντε κλικ στο **εμφάνιση** για να προβάλλετε τις πληροφορίες για κάθε συσκευή ή στο **απόκρυψη** για να συμπτύξετε αυτή την ενότητα. Οι συσκευές που μπορείτε να διαχειριστείτε είναι οι ακόλουθες, ανάλογα με το ποιες περιέχει η πλατφόρμα σας:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
Πληροφορίες Συσκευών Ελέγχου Ταυτότητας

Trusted Platform Module (TPM)

Το τσιπ ασφαλείας TPM πρέπει να είναι ενεργοποιημένο και η ιδιοκτησία του TPM πρέπει να έχει καθοριστεί για να χρησιμοποιηθούν τα προηγμένα χαρακτηριστικά ασφαλείας της εφαρμογής **Προστασία | Πρόσβαση Δεδομένων Dell** και του TPM.

Το παράθυρο Trusted Platform Module στη **Διαχείριση Αρχείων** εμφανίζεται μόνο όταν ένα TPM εντοπιστεί στο σύστημά σας.

Διαχείριση TPM

Αυτές οι λειτουργίες επιτρέπουν στο διαχειριστή του συστήματος να διαχειρίζεται το TPM.

Κατάσταση
Εμφανίζει την *ενεργή* ή *ανενεργή* κατάσταση του TPM. Η "Ενεργή" κατάσταση σημαίνει ότι το TPM έχει ενεργοποιηθεί στο BIOS και είναι έτοιμο για εγκατάσταση (δηλ., μπορεί να γίνει κτήση της ιδιοκτησίας του). Δεν είναι δυνατή η διαχείριση του TPM και η πρόσβαση στα χαρακτηριστικά ασφαλείας του εάν το TPM δεν είναι ενεργό (ενεργοποιημένο).

Εάν το TPM εντοπιστεί στο σύστημα αλλά δεν είναι ενεργό (ενεργοποιημένο), μπορείτε να το ενεργοποιήσετε κάνοντας κλικ στο σύνδεσμο **ενεργοποίηση** σε αυτό το παράθυρο, χωρίς να εισέλθετε στο BIOS του συστήματος. Αφού ενεργοποιήσετε το TPM χρησιμοποιώντας αυτή τη δυνατότητα, πρέπει να γίνει επανεκκίνηση του υπολογιστή. Κατά τη διάρκεια της επανεκκίνησης, εμφανίζεται σε ορισμένες περιπτώσεις ένα μήνυμα το οποίο ζητάει από το χρήστη να δεχθεί τις αλλαγές.

ΣΗΜΕΙΩΣΗ: Η δυνατότητα ενεργοποίησης του TPM από αυτή την εφαρμογή ενδέχεται να μην υποστηρίζεται σε όλες τις πλατφόρμες. Εάν δεν υποστηρίζεται, πρέπει να το ενεργοποιήσετε στο BIOS του συστήματος. Για να το κάνετε αυτό, επανεκκινήστε το σύστημά σας, πιέστε το πλήκτρο **F2** πριν τη φόρτωση των Windows για να εισέλθετε στις ρυθμίσεις BIOS , και στη συνέχεια πλοηγηθείτε στο Ασφάλεια>TPM Ασφάλεια και ενεργοποιήστε το TPM.

Μπορείτε επίσης να *απενεργοποιήσετε* το TPM από εδώ κάνοντας κλικ στο σύνδεσμο **απενεργοποίηση**. Η απενεργοποίηση του TPM το καθιστά μη διαθέσιμο για τις προηγμένες λειτουργίες ασφαλείας. Ωστόσο, η απενεργοποίηση δεν αλλάζει κάποια από τις ρυθμίσεις TPM ούτε διαγράφει ούτε αλλάζει πληροφορίες ή κλειδιά που έχουν αποθηκευτεί στο TPM.

Με ιδιοκτήτη
Εμφανίζει την κατάσταση της ιδιοκτησίας (π.χ. "με ιδιοκτήτη") και σας επιτρέπει να καθορίσετε ή να αλλάξετε τον ιδιοκτήτη του TPM. Η ιδιοκτησία του TPM πρέπει να καταχωρηθεί προκειμένου να είναι διαθέσιμα τα χαρακτηριστικά ασφαλείας του. Για να είναι δυνατός ο καθορισμός της ιδιοκτησίας, το TPM πρέπει να είναι ενεργό (ενεργοποιημένο).

Η διαδικασία καθορισμού της ιδιοκτησίας περιλαμβάνει τη δημιουργία κωδικού πρόσβασης του ιδιοκτήτη του TPM από το χρήστη (με προνόμια διαχειριστή). Μόλις οριστεί αυτός ο κωδικός πρόσβασης, ορίζεται η ιδιοκτησία και το TPM είναι έτοιμο για χρήση.

ΣΗΜΕΙΩΣΗ: Ο κωδικός πρόσβασης ΙδιοκτήτηTPM πρέπει να συμμορφώνεται με τους Κανόνες περιπλοκότητας κωδικού πρόσβασης των Windows για το σύστημά σας.

Σημαντικό! Είναι σημαντικό να μη χάσετε ή ξεχάσετε τον κωδικό πρόσβασης ιδιοκτήτη TPM, καθώς είναι απαραίτητος για την πρόσβαση στις προηγμένες λειτουργίες ασφαλείας για το TPM στην **Προστασία | Πρόσβαση Δεδομένων Dell**.

Κλειδωμένο
Εμφανίζει την *κλειδωμένη* ή *ξεκλείδωτη* κατάσταση για το TPM. Το "Κλείδωμα" είναι ένα χαρακτηριστικό ασφαλείας του TPM. Το TPM θα εισέλθει στην κλειδωμένη κατάσταση μετά από έναν καθορισμένο αριθμό εσφαλμένων πληκτρολογήσεων του κωδικού πρόσβασης ιδιοκτήτη TPM. Ο ιδιοκτήτης TPM μπορεί να ξεκλειδώσει το TPM από εδώ· απαιτείται η πληκτρολόγηση του κωδικού πρόσβασης ιδιοκτήτη TPM.

ΣΗΜΕΙΩΣΕΙΣ:

- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι δεν ήταν δυνατός ο ορισμός ιδιοκτησίας του TPM, απαλείψτε το TPM στο BIOS του συστήματος και επιχειρήστε να ορίσετε ξανά την ιδιοκτησία. Για να απαλείψετε το TPM, επανεκκινήστε τον υπολογιστή σας, πιέστε το πλήκτρο **F2** κατά την επανέναρξη για να εισέλθετε στις ρυθμίσεις BIOS, και στη συνέχεια πλοηγηθείτε στο Ασφάλεια>TPM Ασφάλεια.
- Εάν εμφανιστεί ένα σφάλμα το οποίο δηλώνει ότι δεν ήταν δυνατή η αλλαγή του κωδικού πρόσβασης ιδιοκτήτη TPM, αρχειοθετήστε τα δεδομένα TPM (αρχειοθέτηση διαπιστευτηρίων), απαλείψτε το TPM στο BIOS, ορίστε ξανά την ιδιοκτησία του TPM και επαναφέρετε τα δεδομένα TPM (επαναφορά διαπιστευτηρίων).
- Εάν επιθυμείτε αναλυτικότερες πληροφορίες για ένα συγκεκριμένο μήνυμα σφάλματος, πηγαίνετε στην ιστοσελίδα wave.com/support/Dell.

Dell ControlVault®

Το ControlVault® (CV) της Dell είναι μια ασφαλής υλική αποθήκη για διαπιστευτήρια χρήστη που χρησιμοποιείται κατά τη σύνδεση pre-Windows (π.χ., κωδικοί πρόσβασης χρηστών ή δεδομένα καταχωρημένων δακτυλικών αποτυπωμάτων). Το παράθυρο ControlVault στη **Διαχείριση Αρχείων** εμφανίζεται μόνο όταν ένα ControlVault εντοπιστεί στο σύστημά σας.

Διαχείριση ControlVault

Αυτές οι λειτουργίες επιτρέπουν στον διαχειριστή του συστήματος να διαχειρίζεται το ControlVault του συστήματος.

Κατάσταση
Εμφανίζει την *ενεργή* ή *ανενεργή* κατάσταση του ControlVault. Η "Ανενεργή" κατάσταση σημαίνει ότι το ControlVault δεν είναι διαθέσιμο για αποθήκευση στο σύστημά σας. Συμβουλευτείτε την τεκμηρίωση της Dell για να διαπιστώσετε εάν το σύστημα περιέχει ControlVault.

Κωδικός πρόσβασης
Δηλώνει εάν έχει οριστεί ο κωδικός πρόσβασης Διαχειριστή ControlVault και σας επιτρέπει να ορίσετε έναν κωδικό πρόσβασης ή να αλλάξετε τον κωδικό πρόσβασης (εάν έχει ήδη οριστεί κάποιος). Μόνο διαχειριστές συστήματος μπορούν να ορίζουν ή να αλλάζουν αυτόν τον κωδικό. Ένας κωδικός πρόσβασης Διαχειριστή ControlVault πρέπει να έχει οριστεί προκειμένου να πραγματοποιήσετε τα ακόλουθα:

- Εκτέλεση αρχειοθέτησης ή επαναφοράς διαπιστευτηρίων.
- Απαλοιφή δεδομένων χρήστη (για όλους τους χρήστες).

ΣΗΜΕΙΩΣΗ: Εάν επιχειρηθεί αρχειοθέτηση ή επαναφορά όταν δεν έχει οριστεί κωδικός πρόσβασης Διαχειριστή ControlVault, ο διαχειριστής παροτρύνεται να δημιουργήσει έναν (εάν ο συγκεκριμένος χρήστης είναι διαχειριστής).

Καταχωρημένοι Χρήστες
Δηλώνει εάν υπάρχουν χρήστες με καταχωρημένα διαπιστευτήρια σύνδεσης (π.χ., κωδικοί πρόσβασης, δακτυλικά αποτυπώματα ή δεδομένα smartcard) που είναι επί του παρόντος αποθηκευμένα στο ControlVault.

Απαλοιφή Δεδομένων Χρήστη
Τα δεδομένα στο ControlVault ίσως χρειαστεί να διαγραφούν κάποια στιγμή, για παράδειγμα, εάν οι χρήστες αντιμετωπίζουν προβλήματα κατά τη χρήση ή την καταχώρηση διαπιστευτηρίων pre-Windows για έλεγχο ταυτότητας. Όλα τα δεδομένα που είναι αποθηκευμένα στο ControlVault μπορούν να διαγραφούν, για ένα χρήστη ή για όλους τους χρήστες, από αυτό το παράθυρο.

Για να διαγραφούν τα δεδομένα όλων των χρηστών στην πλατφόρμα πρέπει να εισαχθεί ο κωδικός πρόσβασης Διαχειριστή ControlVault. Θα σας ζητηθεί επίσης ο κωδικός πρόσβασης στο σύστημα (pre-Windows) εάν έχουν καταχωρηθεί διαπιστευτήρια pre-Windows. Όταν απαλείφετε τα δεδομένα όλων των χρηστώμ, ο κωδικός πρόσβασης Διαχειριστή ControlVault και ο κωδικός πρόσβασης στο σύστημα επαναφέρονται. Σημειώστε ότι αυτός είναι ο μόνος τρόπος για να απαλείψετε τον κωδικό πρόσβασης Διαχειριστή ControlVault.

ΣΗΜΕΙΩΣΗ: Αφού απαλείψετε τα δεδομένα όλων των χρηστών, θα σας ζητηθεί να επανεκκινήσετε τον υπολογιστή σας. Η επανεκκίνηση είναι σημαντική για την ορθή λειτουργία του συστήματός σας.

Δεν χρειάζεται να έχει οριστεί κωδικός πρόσβασης Διαχειριστή ControlVault για την απαλοιφή των διαπιστευτηρίων ενός μόνο χρήστη. Όταν κάνετε κλικ στο **απαλοιφή δεδομένων χρήστη**, θα σας ζητηθεί να επιλέξετε το χρήστη του οποίου τα διαπιστευτήρια στο ControlVault θέλετε να

απαλείψετε. Αφού επιλέξετε ένα χρήστη, θα σας ζητηθεί ο κωδικός πρόσβασης στο σύστημα (μόνο εάν έχουν καταχωρηθεί διαπιστευτήρια pre-Windows).

ΣΗΜΕΙΩΣΕΙΣ:

- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι δεν είναι δυνατή η δημιουργία του κωδικού πρόσβασης Διαχειριστή ControlVault, θα πρέπει να αρχειοθετήσετε τα διαπιστευτήριά σας, να απαλείψετε τα δεδομένα όλων των χρηστών από το ControlVault, να επανεκκινήσετε τον υπολογιστή και να επιχειρήσετε να δημιουργήσετε πάλι τον κωδικό πρόσβασης.
- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι δεν ήταν δυνατή η απαλοιφή των διαπιστευτηρίων από το ControlVault για ένα μόνο χρήστη, θα πρέπει να αρχειοθετήσετε τα διαπιστευτήριά σας, να προσπαθήσετε να απαλείψετε τα δεδομένα όλων των χρηστών και στη συνέχεια να προσπαθήσετε να απαλείψετε πάλι τα δεδομένα για το συγκεκριμένο χρήστη.
- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι δεν ήταν δυνατή η απαλοιφή των διαπιστευτηρίων από το ControlVault για όλους τους χρήστες, θα πρέπει να εξετάσετε το ενδεχόμενο να εκτελέσετε επαναφορά συστήματος. **Σημαντικό!** Διαβάστε το θέμα Επαναφορά Συστήματος στη βοήθεια πριν πραγματοποιήσετε μια επαναφορά, καθώς κάτι τέτοιο θα διαγράψει τα δεδομένα ασφαλείας ΟΛΩΝ των χρηστών.
- Εάν εμφανιστεί ένα σφάλμα που δηλώνει ότι δεν ήταν δυνατή η δημιουργία αντιγράφων ασφαλείας για το ControlVault και το TPM, απενεργοποιήστε το TPM στο BIOS του συστήματος. Για να το κάνετε αυτό, επανεκκινήστε τον υπολογιστή, πιέστε το πλήκτρο **F2** κατά την επανέναρξη για να εισέλθετε στις ρυθμίσεις BIOS, και στη συνέχεια πλοηγηθείτε στο Ασφάλεια>TPM Ασφάλεια. Κατόπιν ενεργοποιήστε πάλι το TPM και προσπαθήστε ξανά να αρχειοθετήσετε τα δεδομένα σας για το ControlVault.
- Εάν επιθυμείτε αναλυτικότερες πληροφορίες για ένα συγκεκριμένο μήνυμα σφάλματος, πηγαίνετε στην ιστοσελίδα wave.com/support/Dell.

Self-Encrypting Drive: Συσκευές

Η **Προστασία | Πρόσβαση Δεδομένων Dell** διαχειρίζεται τις βασιζόμενες στον υλικό εξοπλισμό λειτουργίες ασφαλείας των μονάδων self-encrypting drive , οι οποίες διαθέτουν κρυπτογράφηση δεδομένων ενσωματωμένη στο υλικό της μονάδας. Αυτή η διαχείριση χρησιμοποιείται για να διασφαλίσει ότι μόνο εξουσιοδοτημένοι χρήστες μπορούν να έχουν πρόσβαση σε κρυπτογραφημένα δεδομένα όταν είναι ενεργοποιημένο το κλείδωμα μονάδας.

Το παράθυρο Self-Encrypting Drive στη **Διαχείριση Συσκευών** εμφανίζεται μόνο όταν υπάρχουν στο σύστημά σας μία ή περισσότερες μονάδες self-encrypting drive (SED).

Σημαντικό! Μετά την εγκατάσταση της μονάδας, η προστασία δεδομένων και το κλείδωμα της μονάδας self-encrypting drive "ενεργοποιούνται".

Διαχείριση Μονάδας

Αυτές οι λειτουργίες επιτρέπουν στο διαχειριστή της μονάδας να διαχειρίζεται ρυθμίσεις ασφαλείας της μονάδας. Οι αλλαγές στις ρυθμίσεις ασφαλείας της μονάδας τίθενται σε εφαρμογή μετά την απενεργοποίηση της μονάδας.

Προστασία Δεδομένων

Εμφανίζει την κατάσταση *ενεργοποιημένη* ή *απενεργοποιημένη* για την προστασία δεδομένων της μονάδας self-encrypting drive. Η "ενεργοποιημένη" κατάσταση σημαίνει ότι έχει ρυθμιστεί η ασφάλεια της μονάδας, ωστόσο, μέχρι να ενεργοποιηθεί το *κλείδωμα* μονάδας, οι χρήστες δεν χρειάζεται να προβούν σε έλεγχο ταυτότητας στη μονάδα για πρόσβαση κατά τη σύνδεση pre-Windows.

Από εδώ μπορείτε να απενεργοποιήσετε την προστασία δεδομένων της μονάδας self-encrypting drive. Όταν είναι απενεργοποιημένη, όλες οι προηγμένες λειτουργίες ασφαλείας της μονάδας self-encrypting drive είναι ανενεργές και η μονάδα λειτουργεί σαν μια τυπική μονάδα δίσκου. Η απενεργοποίηση της προστασίας δεδομένων διαγράφει όλες τις ρυθμίσεις ασφαλείας, συμπεριλαμβανομένων των διαπιστευτηρίων του διαχειριστή της μονάδας και των χρηστών της μονάδας. Ωστόσο,αυτή η λειτουργία δεν τροποποιεί ούτε καταργεί δεδομένα χρήστη στη μονάδα.

Κλείδωμα

Εμφανίζει την κατάσταση *ενεργοποιημένη* ή *απενεργοποιημένη* για τη(τις) μονάδα(ες) self-encrypting drive. Ανατρέξτε στο θέμα Self-Encrypting Drive για πληροφορίες σχετικά με τη συμπεριφορά μιας κλειδωμένης μονάδας.

Ίσως χρειαστεί να απενεργοποιήσετε προσωρινά το κλείδωμα μονάδας, κάτι που μπορείτε να κάνετε από εδώ. Αυτό δεν συνιστάται, καθώς δεν απαιτούνται διαπιστευτήρια για την πρόσβαση στη μονάδα όταν το κλείδωμα μονάδας είναι απενεργοποιημένο, επομένως οποιοσδήποτε χρήστης της πλατφόρμας μπορεί να αποκτήσει πρόσβαση στα δεδομένα της μονάδας. Η απενεργοποίηση του κλειδώματος μονάδας δενδιαγράφει ρυθμίσεις ασφαλείας, συμπεριλαμβανομένων των διαπιστευτηρίων του διαχειριστή της μονάδας και των χρηστών της μονάδας, ούτε δεδομένα χρήστη που βρίσκονται στη μονάδα.

ΠΡΟΣΟΧΗ! Εάν απεγκαταστήσετε την εφαρμογή **Προστασία | Πρόσβαση Δεδομένων Dell**, πρέπει πρώτα να απενεργοποιήσετε την προστασία δεδομένων στη μονάδα self-encrypting drive και να ξεκλειδώσετε τη μονάδα.

Διαχειριστής Μονάδας

Εμφανίζει τον τρέχοντα διαχειριστή της μονάδας. Από εδώ ο διαχειριστής μονάδας μπορεί να αλλάξει το χρήστη που θα είναι ο διαχειριστής της μονάδας. Ο νέος διαχειριστής πρέπει να είναι έγκυρος χρήστης των Windows στο σύστημα και να έχει προνόμια διαχειριστή. Μπορεί να υπάρξει μόνο ένας διαχειριστής μονάδας στο σύστημα.

Χρήστες Μονάδας

Εμφανίζει τους καταχωρημένους χρήστες της μονάδας και τον αριθμό των τρεχόντων καταχωρημένων χρηστών. Ο μέγιστος αριθμός χρηστών που υποστηρίζεται εξαρτάται από τη μονάδα self-encrypting drive (επί του παρόντος 4 χρήστες για μονάδες δίσκου Seagate και 24 για μονάδες δίσκου Samsung).

Συγχρον. Κωδικού Πρόσβασηςστα Windows
Η λειτουργία συγχρονισμού κωδικού πρόσβασης στα Windows (WPS) αλλάζει αυτόματα τους κωδικούς πρόσβασης Self-Encrypting Drive των χρηστών ώστε να είναι ίδιοι με τον κωδικό πρόσβασής τους στα Windows. Αυτή η λειτουργία δεν επιβάλλεται για τον διαχειριστή της μονάδας και ισχύει μόνο για χρήστες της μονάδας. Η λειτουργία WPS μπορεί να χρησιμοποιηθεί σε εταιρικά περιβάλλοντα όπου οι κωδικοί πρόσβασης πρέπει να αλλάζουν σε συγκεκριμένα χρονικά διαστήματα (π.χ., κάθε 90 ημέρες). Όταν αυτή η επιλογή είναι ενεργοποιημένη, οι κωδικοί πρόσβασης σε μονάδες self-encrypting drive όλων των χρηστών ενημερώνονται αυτόματα όταν οι εν λόγω κωδικοί πρόσβασης στα Windows αλλάξουν.

ΣΗΜΕΙΩΣΗ: Όταν ο συγχρονισμός κωδικού πρόσβασης στα Windows (WPS) είναι ενεργοποιημένος, ο κωδικός πρόσβασης ενός χρήστη σε μονάδα Self-Encrypting Drive δεν μπορεί να αλλάξει. Για να ενημερωθεί αυτόματα ο κωδικός πρόσβασης στη μονάδα, πρέπει πρώτα να αλλάξει ο κωδικός πρόσβασης του χρήστη στα Windows.

Απομνημόνευση ΤελευταίουΟνόματος Χρήστη
Όταν αυτή η επιλογή είναι ενεργοποιημένη, το τελευταίο όνομα χρήστη που εισάγεται θα εμφανίζεται από προεπιλογή στο πεδίο **Όνομα χρήστη** της οθόνης ελέγχου ταυτότητας κατά τη σύνδεση pre-Windows.

ΕπιλογήΟνόματος Χρήστη
Όταν αυτή η επιλογή είναι ενεργοποιημένη, οι χρήστες μπορούν να δουν όλα τα ονόματα χρηστών της μονάδας στο πεδίο **Όνομα χρήστη** της οθόνης ελέγχου ταυτότητας κατά τη σύνδεση pre-Windows.

ΚρυπτογραφικήΔιαγραφή
Αυτή η επιλογή μπορεί να χρησιμοποιηθεί για τη "διαγραφή" όλων των δεδομένων της μονάδας self-encrypting drive. Αυτό δεν διαγράφει πραγματικά τα δεδομένα, αλλά διαγράφει τα πλήκτρα που χρησιμοποιούνται για την κρυπτογράφηση των δεδομένων, καθιστώντας συνεπώς αδύνατη τη χρήση των δεδομένων. Δεν υπάρχει κανένας τρόπος ανάκτησης των δεδομένων της μονάδας μετά την κρυπτογραφική διαγραφή. Επίσης, η προστασία δεδομένων μονάδας self-encrypting drive απενεργοποιείται και η μονάδα είναι έτοιμη να χρησιμοποιηθεί για άλλο σκοπό.

ΣΗΜΕΙΩΣΕΙΣ:

- Εάν εμφανιστούν σφάλματα σχετικά με τις λειτουργίες διαχείρισης της μονάδας self-encrypting drive, απενεργοποιήστε τελείως τον υπολογιστή σας (χωρίς παράλληλη επανεκκίνηση) και στη συνέχεια επανεκκινήστε τον.
- Εάν επιθυμείτε αναλυτικότερες πληροφορίες για ένα συγκεκριμένο μήνυμα σφάλματος, πηγαίνετε στην ιστοσελίδα wave.com/support/Dell.

Πληροφορίες Συσκευών Ελέγχου Ταυτότητας

Το παράθυρο Πληροφορίες Συσκευών Ελέγχου Ταυτότητας στο **Διαχείριση Συσκευών** εμφανίζει πληροφορίες και την κατάσταση για όλες τις συνδεδεμένες συσκευές ελέγχου ταυτότητας(π.χ. συσκευή ανάγνωσης δακτυλικών αποτυπωμάτων, συσκευή ανάγνωσης κλασσικής ή contactless smartcard) στο σύστημα.

Τεχνική Υποστήριξη

Θα βρείτε την Τεχνική υποστήριξη για το λογισμικό **Προστασία | Πρόσβαση Δεδομένων Dell** στην ιστοσελίδα http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

Το Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) της Wave Systems περιλαμβάνεται με την εφαρμογή **Προστασία | Πρόσβαση Δεδομένων Dell** και είναι διαθέσιμο για χρήση όποτε απαιτείται CSP – που είτε καλείται άμεσα από μια εφαρμογή είτε μπορεί να επιλεγεί από μια λίστα εγκατεστημένων CSP. Όταν είναι εφικτό, επιλέξτε "Wave TCG-Enabled CSP" για να διασφαλίσετε ότι το TPM δημιουργεί τα κλειδιά και ότι η διαχείριση των κλειδιών και των κωδικών πρόσβασής τους γίνεται από την εφαρμογή **Προστασία | Πρόσβαση Δεδομένων Dell**.

Το TCG-Enabled CSP της Wave Systems επιτρέπει στις εφαρμογές να χρησιμοποιούν τις λειτουργίες που είναι διαθέσιμες σε πλατφόρμες συμβατές με TCG απευθείας μέσω MSCAPI. Πρόκειται μια μονάδα MSCAPI CSP ενισχυμένη με TCG η οποία παρέχει λειτουργία ασύμμετρου κλειδιού στο TPM και χρησιμοποιεί την ενισχυμένη ασφάλεια που παρέχεται από το TPM, ανεξάρτητα από τις συγκεκριμένες απαιτήσεις του κατασκευαστή σχετικά με τον πάροχο του Trusted Software Stack (TSS).

ΣΗΜΕΙΩΣΗ: Εάν τα κλειδιά TPM που δημιουργούνται από το Wave TCG-enabled CSP απαιτούν κωδικό πρόσβασης και ο χρήστης έχει δημιουργήσει έναν Κύριο κωδικό πρόσβασης TPM, οι μεμονωμένοι κωδικοί πρόσβασης των κλειδιών θα δημιουργηθούν τυχαία και θα αποθηκευτούν στο TPM Password Vault.