גישה | Dell נתוני הגנת של בית

לגשת תוכל ,זה מחלון .זה יישום של לתכונות לגישה פתיחה נקודת מהווה **גישה | Dell נתוני הגנת** של הבית דף הבאות לתכונות:

System Access Wizard
גישה אפשרויות
Self-Encrypting Drive
מתקדמות אפשרויות

לאפשרויות לגשת כדי ללחוץ תוכל שעליו ,**מתקדם** המכונה קישור מופיע החלון של התחתונה הימנית בפינה התמקדמות.

מ[מתקדמות אפשרויות](), הקישור על ללחוץ תוכל ,**בית** הבית לדף לחזור כדי החלון של התחתונה הימנית בפינה.

System Access Wizard

האשף .מופעל **גישה | Dell נתוני הגנת** שהיישום הראשונה בפעם אוטומטית מופעל System Access Wizard אצבע טביעת או בלבד הסיסמ ,למשל) האיך כולל ,שלך במערכת האבטחה היבטי כל בהגדרת אותך ינחה למערכת אם ,בנוסף .למערכת הכניסה של הרצויים (וגם גם או Pre-Windows-ב ,Windows-ב) והמתי (וסיסמה יש שלך Self-Encrypting Drive, האשף באמצעות תצורתו את לקבוע תוכל.

מערכת מנהל פונקציות

הבאות הפונקציות לביצוע זכויות יש במערכת Windows של מערכת מנהל אותהרש עם שהוגדרו למשתמשים **הגנה | Dell נתוני הגנת**ב, לבצע יכולים לא רגילים שמשתמשים.

- מערכת סיסמת לשנות/להגדיר (Pre-Windows)
- קשיח כונן סיסמת לשנות/להגדיר
- מערכת מנהל סיסמת לשנות/להגדיר
- TPM בעל סיסמת לשנות/להגדיר
- ControlVault של מערכת מנהל סיסמת לשנות/הגדירל
- מערכת איפוס
- אישורים ולשחזר בארכיון לאחסן
- Smartcard של מערכת מנהל PIN לשנות/להגדיר
- Smartcard לשנות/להגדיר
- Windows-ל Dell של מאובטחת כניסה להשבית/להפעיל
- Windows-ל כניסה מדיניות להגדיר
- לנהל Self-Encrypting Drives, זה בכלל:
    - o נעילת להשבית/להפעיל Self-Encrypting Drives
    - o סיסמת סינכרון להשבית/להפעיל Windows (WPS)
    - o להשבית/להפעיל Single Sign On (SSO)
    - o קריפטוגרפית מחיקה לבצע

מרחוק ניהול

גישה | Dell נתוני הגנת היישום של טחההאב פונקציות של מרכזי ניהול עם סביבה להגדיר יכול שלך הארגון כגון ,Windows של אבטחה בתשתית להשתמש ניתן ,זה במקרה .(מרוחק ניהול כלומר) מרובות בפלטפורמות Active Directory, כדי **גישה | Dell נתוני הגנת** של ספציפיות תכונות מאובטח באופן לנהל.

הגנת פונקציונליות של המקומי הניהול ,(מרוחק מערכת מנהל "בבעלות" למשל) מרחוק מנוהל המחשב כאשר **גישה | Dell נתוני** זמין לבלתי יהפוך ;מקומי באופן נגישים יהיו לא היישום של הניהול חלונות .את לנהל ניתן מרחוק הבאות הפונקציות:

- Trusted Platform Module (TPM)
- ControlVault
- כניסת Pre-Windows
- מערכת איפוס
- סיסמאות BIOS
- ל-Windows כניסה מדיניות
- Self-Encrypting Drives
- ו-Smartcard אצבע טביעת רישום

Wave Systems' EMBASSY® (ERAS) של המרוחק הניהול בשרת השימוש אודות נוספים פרטים לבקש כדי מכירות איש אל פנה ,מרחוק ניהול עבור Dell אל עבור או שלך dell.com.

גישה אפשרויות

שלך למערכת הגישה קבלת אופן את להגדיר תוכל ,גישה אפשרויות בחלון.

(למשל, הזמינות האפשרויות עם הבית בדף יוצגו הן ,**גישה | Dell נתוני הגנת** של כלשהן אפשרויות הגדרת אם לחלון אותך תעביר עליהם שלחיצה קישורים הן הזמינות האפשרויות .(Pre-Windows כניסת עבור סיסמה שנה (נוספת אצבע טביעת רישום או Pre-Windows סיסמת שינוי, למשל) ספציפית משימה לביצוע, המתאים).

כללי

כניסה לבצע מתי לציין תוכל ,תחילה (Windows, Pre-Windows וגם גם או) וכיצד (וסיסמה אצבע טביעת ללמש) Smartcard, אצבע טביעת של שילובים זה בכלל; הכניסה לאופן שתיים או אחת אפשרות לבחור תוכל .להיכנס .וסיסמה התמיכה ועל ,שלך הסביבה על המוחלת הכניסה מדיניות על מבוססות המופיעות האפשרויות נותנת שלך שהפלטפורמה.

אצבע טביעת

למערכת בכניסה לשימוש אצבע טביעות לעדכן או לרשום תוכל ,אצבע טביעת קורא מכילה שלך המערכת אם. כדי ,המערכת של האצבע טביעות בקורא הרשומות האצבעות את להעביר תוכל ,האצבע טביעות רישום לאחר עיין .(הכלליות גישהה באפשרויות שציינת למה בהתאם) וגם גם או Windows, Pre-Windows-ב למערכת לגשת נוספים לפרטים [משתמש של אצבע טביעות רישום](#)ב.

כניסת Pre-Windows

סיסמת מכונה לעתים) כתמער סיסמת להגדיר עליך ,Pre-Windows כניסת לבצע חייבים שמשתמשים קבעת אם עת בכל הסיסמה את לשנות יוכל המערכת מנהל ,זאת שתגדיר לאחר .Pre-Windows לגישת (Pre-Windows.

סיסמת את להזין עליך יהיה ,זאת לעשות כדי; זה ממסך זמינה ללא Pre-Windows כניסת להפוך גם תוכל **השבת** הלחצן על לחוץ מכן ולאחר נכונה שהסיסמה לאמת ,שלך הנוכחית המערכת.

Smartcard

מסורתי יותר או אחד Smartcard לרשום עליך ,לכניסה Smartcard-ב להשתמש משתמשים שעל קבעת אם רישום אשף את להפעיל כדי **נוסף Smartcard רשום** הקישור על לחץ .Contactless או (Contacted) .לכניסה שימוש עבור Smartcard הגדרת פירושו רישום .Smartcard

רישום לאחר Smartcard, להגדיר או לשנות תוכל ,PIN עבור כרטיס זה הקישור באמצעות **הגדר או שנה** **Smartcard PIN**.

Pre-Windows Login

כניסת כאשר Pre-Windowsמוגדרת, אימות לספק עליך (סיסמה, אצבע טביעת או Smartcard) המערכת כאשר מופעלת, טעינת לפני Windows. כניסת פונקציונליות Pre-Windows מספקת נוספת אבטחה ולמערכת, ומרחיקה המחשב גניבת של במקרה, למשל) למחשב וגישה Windows-ל מחדירה מורשים-בלתי משתמשים).

סיסמת לשנות או ליצור וכן Pre-Windows כניסת להגדיר יכול המערכת מנהל, 'Pre-Windows כניסת' מחלון זה מחלון Pre-Windows כניסת להשבית תוכל, מוגדרת כבר זו סיסמה אם (מערכת); Pre-Windows כניסת הבאות הפעולות את שיבצע אשף תפעיל Pre-Windows כניסת הגדרת:

- מערכת סיסמת: כתמער סיסמת גם מכונה) Pre-Windows גישת עבור Pre-Windows. גישה לקבל כדי, למשל) נוספים אימות גורמי יש למשתמש שבהם במקרים כגיבוי גם משמשת זו סיסמה האצבע טביעות בחיישן בעיה קיימת אם למערכת).
- Smartcard: או אצבע טביעת הגדר Smartcard או אצבע טביעת בכניסת לשימוש Pre-Windows, וציין לה בנוסף או Pre-Windows סיסמת במקום ישמש זה אימות גורם אם.
- Single Sign On: מחדל כברירת, אימות Pre-Windows שלך (סיסמה, אצבע טביעת או Smartcard) אל אוטומטית לכניסה גם תשמש Windows (שמכונה מה Single Sign On). בחר, זו תכונה לבטל כדי ב-Windows" גם כניסה לבצע ברצוני" והסימו בתיבת".
- לשנות האפשרות גם לך תהיה, Pre-Windows לסיסמת בנוסף הוגדרה BIOS של קשיח כונן סיסמת אם הקשיח הכונן סיסמת את להשבית או.

הערה: תוכל, בכל תומך אינו שלך הקורא אם. Pre-Windows באימות תומכים האצבע טביעות קוראי כל לא למערכת תואם ספציפי אצבע טביעות קורא אם לברר כדי. בלבד Windows לכניסת אצבע טביעות לרשום פנה, נתמכים אצבע טביעות קוראי של לרשימה support.dell.com אל עבור או המערכת למנהל.

כניסת השבתת Pre-Windows
סיסמת את להזין עליך יהיה, זאת לעשות כדי; זה מחלון זמינה ללא Pre-Windows כניסת להפוך גם תוכל Pre-Windows (מערכת) הנוכחית שלך, לאמת שהסיסמה נכונה ולאחר מכן ללחוץ על הלחצן **השבת**. שלאחר לב שים רשומים יישארו הרשומים Smartcards או אצבעה טביעות כל, Pre-Windows כניסת השבתת.

אצבע טביעות של הסרה/רישום

כניסת Pre-Windows או לאימות להשתמש ניתן שבהן אצבע טביעות לעדכן או לרשום יכולים משתמשים קיימות אם, תהרשומו האצבעות את מציגות ידיים של תמונות, האצבע טביעות בכרטיסיית .למערכת Windows. בתהליך אותך שמנחה, האצבעות טביעות רישום אשף את מפעילה **נוספת אצבע רשום** הקישור על לחיצה טביעות קורא לך דרוש, האצבע טביעת לרישום .בכניסה לשימוש אצבע טביעת שמירת פירושו "רישום" .הרישום כראוי ומוגדר שמותקן חוקי אצבע.

הערה: כניסת Pre-Windows. תנסה אם תופיע שגיאה הודעת עבור לשמש יכולים צבעהא טביעות קוראי כל לא למנהל פנה, למערכת תואם ההתקן אם לברר כדי .תואם קורא ללא Pre-Windows עבור אצבע טביעות לרשום נתמכים אצבע תטביעו קוראי של לרשימה support.dell.com אל עבור או המערכת.

שלך המדיניות אם .זהותך את לאמת כדי שלך Windows סיסמת את להזין תתבקש, אצבע טביעות רישום בעת בסיסמת להשתמש ניתן (מערכת) Pre-Windows סיסמת סיסמת גם להזין תתבקש, זאת דורשת Pre-Windows האצבע טביעות בקורא בעיה קיימת אם למערכת גישה לקבלת.

הערות:

- הרישום בתהליך אצבע טביעות שתי לפחות לרשום ממליצים אנו.
- אצבע טביעות של אימות יכולות של ההפעלה לפני כראוי נרשמו האצבע שטביעות לוודא עליך.
- שני בין מעבר .החדש וראהק עם אצבע טביעות שוב לרשום עליך, במערכת אצבע טביעות קוראי תחליף אם מומלץ אינו אצבע טביעות של שונים קוראים.
- קורא את מזהה אינו שהמחשב ייתכן, אצבע טביעות רישום בעת מופיעות "מיקוד איבד החיישן" הודעות אם האצבע טביעות קורא של מחדש וחיבור ניתוק, חיצוני אצבע טביעות בקורא מדובר אם .האצבע טביעות הבעיה את כלל בדרך פותרים.

רשומות אצבע טביעות ניקוי

לבטל כדי) על לחיצה או **אצבע טביעת הסר** הקישור על לחיצה ידי-על רשומות אצבע טביעות להסיר תוכל האצבעות טביעות רישום באשף רשומה אצבע טביעת (בחירה.

לבטל יכול המערכת מנהל, Pre-Windows אימות עבור תרשומו אצבעות טביעות עם ספציפי משתמש להסיר כדי המשתמש עבור הרשומות האצבעות טביעות בכל הבחירה את.

הערה: באתר לעיין תוכל, האצבעות טביעות רישום בתהליך כלשהן שגיאה הודעות יופיעו אם wave.com/support/Dell נוספים לפרטים.

רישום Smartcards

נתוני הגנת Dell | גישה מעניקה לך את האפשרות להשתמש ב-Smartcard מסורתי (Contacted) או Contactless הקישור לחץ, Smartcard בכרטיסייה. Pre-Windows אימות או Windows לחשבון כניסה עבור. רישום בתהליך אותך שינחה, Smartcard רישום אשף תא להפעיל כדי **נוסף Smartcard רשום** על. לכניסה שימוש עבור Smartcard הגדרת פירושו.

הרישום לביצוע, Smartcard אימות התקן לך דרוש כראוי ומוגדר שמותקן חוקי.

הערה: לרשימה support.dell.com אל עבור או המערכת למנהל פנה, למערכת תואם ספציפי התקן אם לברר כדי של Smartcards נתמכים.

רישום
רישום בעת Smartcard, שלך המדיניות אם. זהותך את לאמת כדי שלך Windows סיסמת את להזין תתבקש בסיסמת להשתמש ניתן (מערכת) Pre-Windows סיסמת סיסמת גם להזין תתבקש, זאת דורשת Pre-Windows בקורא בעיה קיימת אם למערכת גישה לקבלת Smartcards.

הרישום במהלך, Smartcard PIN להזין תתבקש, אם כזה הוגדר. הוגדר וטרם PIN דורשת שלך המדיניות אם, אחד ליצור תתבקש, כזה.

הערות:

- Pre-Windows ב-Smartcard ב לשימוש שופר שהמשתמש לאחר, אותו להסיר ניתן לא.
- PIN את לשנות יכול המערכת ומנהל, Smartcard ב-המשתמש PIN את לשנות יכולים רגילים משתמשים המשתמש PIN את וגם המערכת מנהל.
- Smartcard ב-Smartcard ותלאים להשתמש ניתן לא, האיפוס לאחר; Smartcard לאפס גם יכול המערכת מנהל מחדש לרישומו עד Pre-Windows או Windows-ל בכניסה.

הערה: רישום Smartcard של בתהליך TPM אישורי לרשום יכולים מערכת מנהלי, TPM אישורי אימות עבור ההצפנה ישירות כספק "Wave TCG-Enabled CSP" באפשרות לבחור מערכת מנהלי על Microsoft Windows. מדיניות עם Dell של מאובטחת גישה להפעיל יש, בנוסף. זה יישום עם תאימות עבור Smartcard CSP במקום הלקוח עבור המתאימה האימות סוג.

הערה: זה שירות מחדש להפעיל / להפעיל תוכל, פועל אינו Smartcard שירות שלפיה שגיאה הודעת תקבל אם הבאות הפעולות ביצוע ידי-לע:

- הימני העכבר לחצן באמצעות לחץ מכן ולאחר, שירות בחר, הבקרה מלוח 'מערכת מנהל כלי' החלון אל נווט 'מחדש הפעל' או 'הפעל' ובחר Smartcard על.
- wave.com/support/Dell. אל עבור, ספציפית שגיאה הודעת אודות יותר מפורט במידע מעוניין אתה אם

Self-Encrypting Drive

נתוני הגנת Dell | גישה של החומרה מבוססות האבטחה פונקציות את מנהלת Self-Encrypting Drives, עם לנתונים לגשת יוכלו מורשים משתמשים שרק מבטיחה זו פונקציונליות בחומרת המוטבעת נתונים הצפנת .הכונן (מופעלת הכונן נעילת כאשר) מוצפנים

התחתונה הכרטיסייה על לחיצה ידי-על Self-Encrypting Drive לחלון גש **Self-Encrypting Drive**. כרטיסייה במערכת קיים יותר או אחד (SED) Self-Encrypting Drive כאשר רק מופיעה זו.

מנהל סיסמת תיצור, זה באשף Self-Encrypting Drive Setup Wizard את להפעיל כדי **הגדרה** הקישור על לחץ .שלך הכונן הצפנת הגדרות את ותחיל, זו סיסמה תגבה, כונן של מערכת Self-ל לגשת יכולים מערכת מנהלי רק Encrypting Drive Setup Wizard.

!חשוב הבאים הפעולה אופני, נעול הכונן כאשר. לזמינים יהפכו כונן נעילתו נתונים הגנת, הכונן הגדרת לאחר :חלים

- מכובה שהכונן פעם בכל *נעול* למצב נכנס הכונן.
- בחלון (אצבע טביעת או) הנכונים והסיסמה המשתמש שם את יזין שהמשתמש מבלי מחדש יופעל לא הכונן כניסת Pre-Windows. במחשב משתמש לכל נגישים בכונן הנתונים, לזמינה כונן נעילת הפיכת לפני.
- הכונן לנתוני לגשת כדי אימות דרוש; משני ככונן אחר למחשב מחובר הוא כאשר גם מאובטח הכונן.

סיסמת לשינוי משתמשים עבור וקישור הכוננים את ויציג יופיע Self-Encrypting Drive החלון, הכונן הגדרת לאחר כונן קיים אם. זה מחלון כונן משתמשי להסיר או להוסיף גם תוכל, כונן של מערכת מנהל אתה אם. שלהם הכונן נעילתו את לבטל אפשרות ותהיה, זה בחלון יוצג הוא, הוגדר שלא חיצוני.

הערה: שבמהמח עצמאי באופן הכונן את לכבות יש, חיצוני משני כונן לנעול כדי.

ב הכונן הגדרות את לנהל יכול הכונן של המערכת מנהל **התקנים>מתקדם**. נוספים לפרטים, ראה [התקנים ניהול - Self-Encrypting Drives.]

כונן הגדרת
הבאים יסהמושג את לזכור חשוב. שלך הכוננים בהגדרת אותך ינחה Self-Encrypting Drive Setup Wizard התהליך במהלך.

כונן של מערכת מנהל
(הכונן של המערכת מנהל סיסמת את ומגדיר) לכונן גישה שמגדיר מערכת מנהל זכויות בעל הראשון המשתמש להבטיח כדי. לכונן בגישה שינויים לביצוע זכויות עם היחיד המשתמש זהו; הכונן של המערכת למנהל יהפוך "מבין אני" הסימון בתיבת לבחור עליך, הכונן של המערכת מנהל להיות אמור באמת המוגדר הראשון שהמשתמש .זה בשלב להמשיך כדי

כונן של מערכת מנהל סיסמת
סיסמת את להזין עליך. כאישור הסיסמה את שוב ולהזין כונן של מערכת מנהל סיסמת ליצור ממך יבקש האשף למשתמש. הכונן של המערכת מנהל סיסמת את ליצור שתוכל לפני זהותך את לאמת כדי שלך Windows זו סיסמה ליצור כדי מערכת מנהל זכויות דרושות הנוכחי Windows.

כונן אישורי גיבוי
הכונן של המערכת מנהל אישורי של גיבוי עותק לשמור כדי, מיקום לבחור כדי **עיון** הלחצן על לחץ או מיקום הקלד.

חשוב**!**
- (נשלפים אחסון אמצעי כמו) הראשי הקשיח הכונן שאינו בכונן מומלץ, אלה אישורים לגבות מאוד מומלץ. לגיבוי לגשת תוכל לא, שלך לכונן גישה תאבד אם, אחרת.
- (אצבע טביעת וא) והסיסמה המשתמש שם את להזין יידרשו המשתמשיכל, הכונן הגדרת השלמת לאחר תופעל שהמערכת הבאה בפעם למערכת לגשת כדי, Windows טעינת לפני שלהם הנכונים.

כונן משתמש הוסף
הוספת בעת .חוקיים Windows משתמשי המהווים ,לכונן אחרים משתמשים להוסיף יכול המערכת מנהל
.הראשונה בכניסה שלו הסיסמה את לאפס מהמשתמש לדרוש אפשרות יש המערכת למנהל ,לכונן משתמשים
.הכונן נעילת ביטול לפני Pre-Windows אימות במסך שלו הסיסמה את לאפס יידרש המשתמש

מתקדמות הגדרות

- *Single Sign On* - מחדל כברירת סיסמת ,Self-Encrypting Drive המוזנת ב-Pre-Windows כדי .(Single Sign On שמכונה מה) Windows-ל אוטומטית לכניסה גם תשמש ,לכונן הגישה את לאמת קביעת בעת "Windows הפעלת בעת שוב כניסה לבצע ברצוני" הסימון בתיבת בחר ,זו תכונה לבטל .שלך הכונן הגדרות
- *אצבע בטביעת כניסת* - נתמכות בפלטפורמות ,Self-Encrypting-ל כניסתך את לאמת שברצונך לציין תוכל סיסמה במקום אצבע טביעת באמצעות Drive.
- *המתנה/שינהב תמיכה (S3)* (בפלטפורמה נתמך אם) - ,זמינה זו אפשרות אם ,Self-להעביר ניתן Encrypting Drive ממצב לחזרה Pre-Windows אימות ויידרש ,(S3 מצב גם מכונה) המתנה/שינה למצב .המתנה/שינה

הערות:

- ב-S3 תמיכה כאשר ,זמינה ב-BIOS הקיימות הסיסמה מגבלות לכל כפופות הכונן הצפנת סיסמאות. שעשויות BIOS סיסמת של ספציפיות מגבלות על נוסף מידע לקבלת המערכת חומרת יצרן עם התייעץ .במערכת להימצא
- במצב תומך הכונן אם לך ייוודע ,כונן הגדרת במהלך S3. במצב תומך Self-Encrypting Drive כל לא בקשות אוטומטית יומרו Windos S3 ,זה במצב תומכים שאינם כוננים עבור .לא או שינה/המתנה (במחשב לזמין תרדמה מצב להפוך מאוד מומלץ) זמין תרדמה מצב אם ,תרדמה
- בבקשה יושהה התהליך ,(SSO) Single Sign On האפשרות הגדרת לאחר שתיכנס הראשונה בפעם לצורך מאובטחת בצורה שיאומת Windows אימות לטופס להיכנס תתבקש ,שלך .Windows לכניסת אותך תכניס SSO ,מחדש תופעל שהמערכת הבאה בפעם .Windows-ל עתידיים כניסה ניסיונות משתמש של Windows אימות שינוי בעת גם דרוש התהליך אותו .Windows-ל אוטומטית (סיסמה ,טביעת אצבע, Smartcard PIN). על להקיש הדורשת מדיניות יש ולתחום ,בתחום נמצא המחשב אם .תכובד זו מדיניות ,Windows כניסת עבור ctrl+alt+del

זהירות! נתוני הגנת את לבטל עליך יהיה תחילה, **גישה | Dell נתוני הגנת** היישום של ההתקנה את תסיר אם .הכונן נעילת את ולבטל Self-Encrypting Drive

Self-Encrypting Drive-ב משתמש פונקציות

כונן משתמשי .המשתמשים וניהול הכונן אבטחת ניהול פעולות כל את מבצעים Self-Encrypting Drives מנהלי הבאות המשימות את רק לבצע יכולים הכונן מנהל שאינם:

- לכונן סיסמתם שינוי
- כונן נעילת ביטול

מהכרטיסייה אלה למשימות לגשת ניתן **Self-Encrypting Drive נתוני הגנתב | Dell גישה**.

סיסמה שנה
הכונן עבור חדשה אימות סיסמת ליצור רשומים למשתמשים מאפשרת זו פונקציה .Self-Encrypting Drive-ל סיסמתך את להזין עליך .החדש הערך לפי הכונן סיסמת הגדרת לפני

הערות:

- סיסמת של המדיניות אם .מאופשרים הם אם ,הסיסמה של המורכבות ומדיניות האורך את כופה היישום לב שים .תווים 32 הוא Self-Encrypting Drive סיסמת של המרבי האורך ,מאופשרת אינה Windows .מאופשר אינו (המתנה/שינה) S3 אם תווים 127 הוא המרבי שהאורך
- או שינוי .המשתמש של Windows מסיסמת נפרדת הינה Self-Encrypting Drive-ל משתמש סיסמת ,אלא אם ,המשתמש של הכונן סיסמת על פיעיםמש אינם המשתמש של Windows סיסמת של איפוס .לפרטים Self-Encrypting Drives: התקניםב עיין .הופעל 'Windows סיסמת סינכרון'
- בסיסמת בהם להשתמש ניתן שלא מוגבלים תווים של ערכה קיימת ,באנגלית שאינן מסוימות במקלדות ,המוגבלים מהתווים כלשהו תו מכילה Windows סיסמת אם .Self-Encrypting Drive סיסמת וסינכרון ,מאופשר Windows .שגיאה הודעת ותופיע ייכשל הסינכרון

כונן נעילת ביטול
למצב נכנס הכונן ,מאופשרת כונן נעילת .נעול כונן נעילה לבטל רשום כונן למשתמש מאפשר כונן נעילת ביטול סיסמתך הזנת ידי-על בכונן אימות לבצע עליך ,שוב מופעלת המערכת כאשר .מכובה שהמחשב פעם בכל נעול .Pre-Windows של האימות במסך

הערות:

- חשבונות אם אפשרית בלתי להיות עשויה (תרדמה או המתנה/שינה כלומר) בחשמל חיסכון למצב כניסה .במחשב זמנית-בו פעילים Self-Encrypting Drive-ב שימשתמ של מרובים
- של המשתמשים שמות בתור משמשים 'וכו "2 משתמש", "1 משתמש", ,Pre-Windows של האימות במסך .ורוסית קוריאנית ,יפנית ,סינית :הבאות לשפות המותאמות היישום בגרסאות הכונן

מתקדמות אפשרויות

את לנהל מערכת מנהל הרשאות עם למשתמש מאפשרות **גישה | Dell נתוני הגנת** ב המתקדמות האפשרויות היישום של הבאים ההיבטים:

תחזוקה
סיסמאות
התקנים

הערה: המתקדמות באפשרויות שינויים לבצע יכולים מערכת מנהל הרשאות עם משתמשים רק; רגילים משתמשים אותן לשנות לא אך אלה הגדרות להציג יכולים.

תחזוקה

להכין כדי מערכת לאפס ,Windows-ל כניסה העדפות להגדיר כדי התחזוקה בחלון להשתמש יכולים מערכת מנהלי
.המערכת של האבטחה בחומרת השמורים משתמש אישורי ולשחזר בארכיון לאחסן או מחדש לייעוד אותה
:הבאים בנושאים עיין ,לפרטים

גישה העדפות
מערכת איפוס
&אישורים ושחזור בארכיון אחסון

גישה העדפות

במערכת המשתמשים כל עבור Windows-ל כניסה העדפות לציין מערכת נהלילמ מאפשר גישה העדפות חלון.

Dell של מאובטחת כניסה אפשר
שונים בגורמים להשתמש לך מאפשרת Windows של הסטנדרטי ctrl-alt-delete מסך את להחליף האפשרות כגורם אצבע טביעת להוסיף לבחור תוכל Windows. אל גישה עבור Windows לסיסמת (בנוסף או) מלבד לאימות עבור לאימות נוספים גורמים להוסיף ניתן .Windows-ל הכניסה בתהליך האבטחה את לחזק כדי, נוסף אימות כניסה ל-Windows, כולל Smartcard אישור או TPM.

הערות:

- במערכת המשתמשים כל על משפיעה לזמינה Dell של מאובטחת כניסה הפיכת.
- Smartcard-ה או האצבע טביעות את רשמו שמשתמשים לאחר רק לזמינה זו אפשרות להפוך מומלץ שלהם.
- Windows-ל כניסתך את לאמת תתבקש, זו אפשרות הגדרת לאחר כניסה שתבצע הראשונה בפעם שלך החדשים האימות בגורמי להשתמש עליך יהיה מכן ולאחר, שלך הסטנדרטית למדיניות בהתאם הבאה בהפעלה.

זמינה ללא Dell של מאובטחת כניסה הפוך
כאשר .Windows-ל כניסה עבור זמינות ללא **גישה | Dell נתוני הגנת** של הפונקציות כל את תהפוך זו אפשרות שלך דרטיתהסטנ Windows-ל הכניסה למדיניות תחזור, נבחרת זו אפשרות.

הערות:

- אפשרות את הפוך, כניסה ניסיון בעת Windows-ל המאובטחת לכניסה בנוגע שגיאה מקבל אתה אם שוב לזמינה אותה הפוך ואז, זמינה ללא Dell של המאובטחת הכניסה.
- ספציפית שגיאה הודעת אודות יותר מפורט במידע מעוניין אתה אם, אל עבור wave.com/support/Dell.

מערכת איפוס

זו פעולה ;בפלטפורמה האבטחה חומרת מכל המשתמש נתוני כל לניקוי משמשת 'מערכת איפוס' הפונקציה סיסמאות מלבד ,במערכת ותהסיסמא כל את תנקה זו אפשרות .המחשב של מחדש לייעוד ,לדוגמה ,משמשת ControlVault, TPM כלומר) החומרה בהתקני הנתונים כל את גם כמו ,משתמש של Windows טביעות וקוראי לנתוני לגשת שניתן כך ,הנתונים הגנת את מבטלת גם זו פונקציה ,Self-Encrypting Drives עבור .(אצבעות הכונן.

תידרש ,המערכת את לאפס כדי .**הבא** על ללחוץ מכן ולאחר המערכת את מאפס שאתה מבין שאתה לאשר עליך הוגדרו אם ,אבטחה התקן כל עבור הסיסמה את להזין:

- בעל TPM
- מנהל ControlVault
- מנהל BIOS
- מערכת BIOS (טרום-Windows)
- קשיח כונן (BIOS)
- מנהל Self-Encrypting Drive

הערה: עבור Self-Encrypting Drives, בלבד הכונן מנהל סיסמת נדרשת, ולא כל סיסמאות משתמשי הכונן.

חשוב! אם .בעבר שנשמר מארכיון לשחזר היא המערכת איפוס בעת שנוקו כלשהם נתונים לשחזר היחידה הדרך ;נמחקים לא ,ההגדרה נתוני רק נמחקים ,Self-Encrypting Drive עבור .אלה נתונים לשחזר ניתן לא ,ארכיון לך אין .אישיים נתונים ומהכונן

אישורים ושחזור בארכיון אחסון

כניסה פרטי) המשתמשים אישורי כל של ושחזור לגיבוי משמשת 'אישורים ושחזור בארכיון אחסון' הפונקציונליות (והצפנה ב-ControlVault ו-Trusted Platform Module (TPM). בעת חשוב הינו אלה נתונים גיבוי כל את לשחזר פשוט תוכל, זה במקרה. בחומרה כשל של במקרה נתונים שחזור עבור או מחשב של מחדש הקצאה שמור ארכיון מקובץ החדש למחשב האישורים.

רכתבמע המשתמשים כל עבור או יחיד משתמש עבור אישורים לשחזר או בארכיון לאחסן לבחור תוכל.

Smartcard, ונתוני רשומות אצבעות טביעות כגון ,Pre-Windows-ב המשמשים נתונים כוללים המשתמש אישורי אישור יצירת, לדוגמה; אבטחה יישומי ידי-על כנדרש מפתחות ייצור ה-TPM. ב השמורים מפתחות וכן TPM-ב מפתחות תיצור דיגיטלי.

הערה: היישום של בתיעוד עיין, בארכיון TPM מפתחות לאחסן יכולה **גישה | Dell נתוני הגנת** אם לקבוע כדי יישומים הם מפתחות להפקת "Wave TCG-Enabled CSP"-ב המשתמשים יישומים, כללי באופן. המאובטח נתמכים.

בארכיון אישורים אחסון
הבאות הפעולות את לבצע עליך, בארכיון אישורים לאחסן כדי:

- במערכת משתמשים עבור או עצמך עבור בארכיון אישורים מאחסן אתה אם ציין.
- מערכת מנהל סיסמת (Pre-Windows), מערכת סיסמת הזנת ידי-על האבטחה לחומרת אימות ספק TPM בעל וסיסמת ControlVault.
- אישורים גיבוי סיסמת צור.
- Flash כונן כגון, נשלף אחסון אמצעי להיות הארכיון מיקום על **זעיו** הלחצן באמצעות, ארכיון מיקום ציין. הקשיח בכונן כשל מפני להגן כדי, רשת כונן או USB מסוג.

חשובות הערות:
- שלו האישורים פרטי אחסון עבור למשתמש יידרש זה שמידע כיוון, הארכיון מיקום את רשום.
- שלא כיוון חשובה זו פעולה. הנתונים את לשחזר יהיה שניתן להבטיח כדי, האישורים גיבוי סיסמת את רשום זו סיסמה לשחזר ניתן.
- של ההגדרה בהוראות עיין או המערכת מנהל עם קשר צור, TPM של הבעלים סיסמת את יודע אינך אם במחשב TPM.

אישורים שחזור
הבאות הפעולות את לבצע עליך, אישורים לאחסן כדי:

- במערכת משתמשים עבור או עצמך עבור בארכיון אישורים מאחסן אתה אם ציין.
- הארכיון קובץ את ובחר הארכיון למיקום עבור.
- הארכיון הגדרת בעת שנוצרה הארכיון גיבוי סיסמת את הזן.
- מערכת מנהל סיסמת (Pre-Windows), מערכת סיסמת הזנת ידי-על האבטחה לחומרת אימות ספק TPM בעל וסיסמת ControlVault.

הערות:
- לבצע נסה, שחזור לבצע פעמים כמה וניסית, נכשל האישורים שחזור שלפיה שגיאה הודעת תקבל אם מהארכיון לשחזר ונסה אחר אישורים ארכיון צור, תצליח לא זו פעולה אם. אחר ארכיון קובץ עבור שחזור החדש.
- את נקה מכן ולאחר אישורים ארכיון צור, TPM מפתחות לשחזר ניתן לא שלפיה שגיאה הודעת תקבל אם ה-TPM את לנקות כדי. BIOS-ב ה-TPM, המחשב את מחדש הפעל, מקש על הקש **F2** ההפעלה בעת. אבטחה>TPM אבטחה אל נווט מכן ולאחר, BIOS-ה הגדרות אל לגשת כדי מחדש הגדר מכן לאחר. האישורים את לשחזר שוב ונסה TPM-ה על בעלות.
- אל עבור, ספציפית שגיאה הודעת אודות יותר מפורט במידע מעוניין אתה אם wave.com/support/Dell.

סיסמאות ניהול

שלך במערכת האבטחה סיסמאות כל את לשנות או ליצור יכול מערכת מנהל ,'סיסמאות ניהול' מהחלון:

- מערכת (גם מכונה Pre-Windows)*
- מערכת מנהל*
- קשיח כונן*
- ControlVault
- בעל TPM
- ראשית TPM
- סיסמאות מאגר TPM
- Self-Encrypting Drive

הערות:

- תצורת לפי ישתנה זה שחלון כך ;יוצגו הנוכחית הפלטפורמה לתצורת הרלוונטיות אלה סיסמאות רק ומצבה המערכת.
- סיסמאות הן למעלה לצדן * עם הסיסמאות BIOS, דרך גם אותן לשנות וניתן BIOS המערכת.
- ה-BIOS מנהל ידי-על נדחו סיסמאות שינויי אם ה-BIOS רמת של הסיסמאות את לשנות או ליצור ניתן לא.
- Self-Encrypting Drive את מפעילה Self-Encrypting Drive Setup Wizard; על לחיצה **הגדרה** הקישור על לחיצה של יותר או אחת סיסמה לשנות למשתמש מאפשרת **ניהול** Self-Encrypting Drive.
- הסיסמאות את לשנות או להציג תוכל שבו חלון מציגה TPM סיסמאות מאגר עבור **ניהול** הקישור על לחיצה באקראי נוצרת הסיסמה, מוצר סיסמה הדורש TPM מפתח כאשר .שלך TPM-ה מפתחות על המגנות ראשי TPM סיסמת שתיצור עד TPM-ה סיסמאות מאגר את לנהל תוכל לא .הסיסמאות במאגר ומוצבת.

Windows סיסמת של מורכבות כללי

גישה | Dell נתוני הגנת סיסמת של הסיסמה מורכבות בכללי עומדת הבאה שהסיסמה אמוור במחשב Windows:

- TPM-ה של בעלים סיסמת

הבאים לשלבים בהתאם פעל ,במחשב Windows סיסמת של המורכבות מדיניות את לקבוע כדי:

1. הבקרה ללוח גש.
2. 'ניהול כלי' על פעמיים לחץ'.
3. 'מקומית אבטחה מדיניות' על פעמיים לחץ'.
4. 'סיסמה מדיניות' ובחר 'חשבונות מדיניות' את הרחב'.

התקנים

לצפות תוכל ,התקן כל עבור .במערכת המותקנים האבטחה התקני כל לניהול מערכת מנהלי משמש ההתקנים חלון כדי **הסתר** על או ,קלהת כל עבור פרטים להציג כדי **הצג** על לחץ .הקושחה גרסת כגון ,נוסף מפורט ובמידע במצב שלך הפלטפורמה לתכולת בהתאם ,לנהל שניתן ההתקנים להלן .זה מקטע לצמצם:

Trusted Platform Module (TPM)
*ControlVault®
Self-Encrypting Drives
אימות התקן פרטי

Trusted Platform Module (TPM)

המתקדמות האבטחה בתכונולת להשתמש כדי TPM על בעלות ולהגדיר TPM של האבטחה שבב את להפעיל יש **נתוני הגנת Dell | גישה** עם הזמינות TPM-וה.

חלון Trusted Platform Module ב**התקנים ניהול** מופיע TPM כאשר רק מזוהה שלך במערכת.

TPM ניהול

TPM-ה את לנהל המערכת למנהל מאפשרות אלה פונקציות.

מצב

TPM-ה עבור *פעיל לא* או *פעיל* מצב מציג TPM. שה פירושו "פעיל" מצב TPM-ב הופעל BIOS-ב ומוכן (כלומר להגדרה (זמין) פעיל אינו TPM-ה אם שלו האבטחה לתכונות לגשת או TPM-ה את לנהל ניתן לא .(בעלות להגדיר ניתן).

בחלון **הפעל** הקישור על לחיצה ידי-על לזמין אותו להפוך תוכל ,(זמין) פעיל אינו אך במערכת מזוהה TPM-ה אם את מחדש להפעיל יש ,זו תכונה צעותבאמ TPM של ההפעלה לאחר .המערכת BIOS-ל להיכנס מבלי ,זה השינויים את לקבל תתבקש ,מסוימים במקרים ,מחדש ההפעלה במהלך .המחשב

הערה: ההפעלה אם .זה מיישום (פעיל) לזמין TPM-ה את להפוך ביכולת יתמכו לא מסוימות שפלטפורמות ייתכן על הקש ,המערכת את מחדש הפעל ,זאת לעשות כדי .ערכתהמ BIOS-ב לזמינה אותה להפוך עליך ,נתמכת אינה אבטחה TPM>אבטחה אל נווט מכן ולאחר ,BIOS-ה להגדרת להיכנס כדי Windows טעינת לפני **F2** מקש TPM-ה את ולהפעיל.

אותו יהפוך TPM-ה הפעלת ביטול; **הפעלה בטל** הקישור על לחיצה ידי-על מכאן TPM *הפעלת לבטל* גם תוכל או כלשהן TPM הגדרות משנה אינו ההפעלה ביטול ,זאת עם .המתקדמות האבטחה תכונות עבור זמין לבלתי TPM-ב שנשמרו כלשהם מקשים או פרטים משנה או מוחק.

בבעלות

בעלות להגדיר יש .TPM-ה בעל את לשנות או להגדיר לך ומאפשר ("בבעלות נמצא" כלומר) בעלות מצב מציג TPM-ה את להפוך יש ,בעלות הגדרת לפני .לזמינות האבטחה תכונות את להפוך כדי TPM (מופעל) לזמין.

זו שסיסמה לאחר .TPM בעל סיסמת ליצור (מערכת מנהל הרשאות עם) המשתמש על ,הבעלות הגדרת בתהליך לשימוש מוכן TPM-ו נוצרת הבעלות ,מוגדרת.

הערה: שלך המערכת עבור Windows סיסמת של מורכבות כלליב לעמוד חייבת TPM בעל סיסמת.

חשוב! האבטחה לפונקציות לגישה נדרשת שהיא כיוון , TPM בעל סיסמת את תשכח או תאבד שלא חשוב **נתוני הגנתב Dell | גישה** FTP-ה עבור המתקדמות.

נעול

נעול למצב ייכנס TPM-ה ;TPM-ה של אבטחה תכונת היא "נעילה" .TPM-ה עבור *נעול לא* או *נעול* מצב יגמצ TPM-ה נעילת את לבטל יכול TPM-ה בעל .TPM בעל סיסמת להזנת שגויים ניסיונות של מוגדר מספר לאחר TPM בעל סיסמת הזנת נדרשת ;מכאן TPM.

הערות:

- BIOS-ב TPM-ה את נקה ,TPM-ה על בעלות להגדיר ניתן לא שלפיה שגיאה ודעתה מקבל אתה אם **F2** מקש על הקש ,המחשב את מחדש הפעל ,TPM-ה את לנקות כדי .בעלות שוב להגדיר ונסה המערכת אבטחה>TPM אבטחה אל נווט מכן ולאחר ,BIOS-ה הגדרות אל לגשת כדי ההפעלה בעת.
- TPM בעל סיסמת לשנות תוני לא שלפיה שגיאה הודעת תקבל אם ,TPM-ה נתוני את בארכיון שמור נתוני ושמור TPM-ה על בעלות מחדש הגדר ,BIOS-ב TPM-ה את נקה ,(אישורים ארכיון) TPM (אישורים שחזור).
- אל עבור ,ספציפית שגיאה הודעת אודות יותר מפורט במידע מעוניין אתה אם wave.com/support/Dell.

Dell ControlVault®

Dell ControlVault® (CV) כניסת בעת המשמשים משתמשים אישורי עבור מאובטחת חומרה מאגר הוא Pre-Windows (למשל, סיסמאות משתמש או נתוני טביעות אצבע). חלון ControlVault ב**התקנים ניהול** שלך במערכת מזוהה ControlVault כאשר רק מופיע.

ניהול ControlVault
במערכת ControlVault את לנהל המערכת למנהל מאפשרות אלה פונקציות.

מצב
שלך במערכת זמין אינו ControlVault-ש פירושו "פעיל אל" מצב. ControlVault עבור *פעיל לא* או *פעיל* מצב מציג ControlVault. מכילה המערכת אם לקבוע כדי Dell מערכת בתיעוד התייעץ. אחסון עבור

סיסמה
כבר אם) אותה ותלשנ או סיסמה להגדיר לך ומאפשר, הוגדרה ControlVault של מערכת מנהל סיסמת אם מציין הוגדרה). של מערכת מנהל סיסמת להגדיר יש. זו סיסמה לשנות או להגדיר יכולים מערכת מנהלי רק הבאות הפעולות את לבצע מנת על ControlVault:

- אישורים של שחזור או בארכיון אחסון ביצוע
- (המשתמשים כל עבור) משתמש נתוני ניקוי

הערה: מוגדרת לא עדיין ControlVault של המערכת מנהל סיסמת כאשר שחזור או בארכיון אחסון לבצע ניסיון, המערכת מנהל הוא המשתמש אם) סיסמה ליצור בקשה יציג.

רשומים משתמשים
חכמים יסיכרט או אצבע טביעות, סיסמאות נתוני כמו) רשומים כניסה אישורי יש כלשהם למשתמשים אם מציין ב-ControlVault כעת המאוחסנים.

משתמש נתוני ניקוי
בשימוש בבעיות נתקלים משתמשים אם, לדוגמה, ControlVault-ב הנתונים את מתישהו לנקות צורך שיהיה ייתכן; או יחיד משתמש עבור, ינוקו ControlVault-ב המאוחסנים הנתונים כל. לאימות Pre-Windows אישורי ברישום זה מחלון, המשתמשים כל.

תתבקש. בפלטפורמה המשתמשים כל נתוני את לנקות כדי ControlVault של המערכת מנהל סיסמת את להזין יש כל נתוני את תנקה כאשר. כלשהם Pre-Windows אישורי רשומים אם (Pre-Windows) מערכת סיסמת להזין גם היחידה הדרך שזוהי לב שים; יתאפסו המערכת וסיסמת ControlVault של המערכת מנהל סיסמת, המשתמשים של המערכת מנהל סיסמת את לנקות ControlVault.

הערה: חשוב, המערכת של תקין לתפקוד. מחדש המחשב את להפעיל תתבקש, המשתמשים כל נתוני ניקוי לאחר המחשב את מחדש שתפעיל.

לחיצה בעת. יחיד משתמש של אישורים לנקות כדי ControlVault של המערכת מנהל סיסמת את להגדיר צורך אין לאחר. שלו ControlVault אישורי את למחוק שברצונך המשתמש את לבחור תתבקש, **משתמשים נתוני ניקוי** על (רשומים Pre-Windows אישורי אם רק) המערכת סיסמת את להזין תתבקש, משתמש שתבחר.

הערות:
- לאחסן עליך, ControlVault של המערכת מנהל סיסמת את ליצור ניתן לא שלפיה שגיאה הודעת תקבל אם את מחדש להפעיל, ControlVault-מ המשתמשים נתוני כל את לנקות, שלך האישורים את בארכיון הסיסמה את ליצור שוב ולנסות המחשב.
- עליך,יחיד משתמש עבור ControlVault-מ ריקהאישו את לנקות ניתן לא שלפיה שגיאה הודעת תקבל אם את שוב לנסות מכן ולאחר המשתמשים נתוני כל את לנקות לנסות, בארכיון שלך האישורים את לאחסן יחיד משתמש אותו עבור הנתונים.
- המשתמשים כל עבור ControlVault-מ האישורים את לנקות ניתן לא שלפיה שגיאה הודעת תקבל אם, כיוון, איפוס ביצוע לפני 'מערכת איפוס' של העזרה נושא את סקור **חשוב!**. מערכת איפוס ועביץ לשקול עליך המשתמשים של האבטחה נתוני כל את תנקה זו שפעולה.

- נתוני לגבות ניתן לא שלפיה שגיאה הודעת תקבל אם ,TPM את השבת BIOS-ב TPM ו-ControlVault. כדי ההפעלה בעת **F2** מקש על הקשה ,המחשב של מחדש הפעלה ידי-על מתבצעת זו פעולה .המערכת ה-BIOS, אבטחה>TPM. אבטחה אל ניווט מכן ולאחר ,מכן לאחר ,מחדש הפעל את ה-הגדרות אל לגשת בארכיון שלך ControlVault נתוני את לאחסן שוב ונסה TPM.
- אל עבור ,ספציפית שגיאה הודעת אודות יותר מפורט במידע מעוניין אתה אם wave.com/support/Dell.

Self-Encrypting Drives: מתקדם

נתוני הגנת Dell | גישה של החומרה מבוססות האבטחה פונקציות את מנהלת Self-Encrypting Drives, עם מוצפנים לנתונים לגשת יוכלו מורשים משתמשים שרק מבטיח זה ניהול. הכונן בחומרת המוטבעת נתונים הצפנת מופעלת הכונן נעילת כאשר.

Self-Encrypting Drive החלון ב**התקנים ניהול** כאשר רק מופיע Self-Encrypting Drive (SED) או אחד במערכת קיים יותר.

חשוב! נעילתו נתונים הגנת, הכונן הגדרת לאחר Self-Encrypting Drives לזמינים יהפכו.

התקנים ניהול

הכונן של אבטחה בהגדרות שינויים. הכונן אבטחתהגדרות את לנהל המערכת מנהלל מאפשרות אלה פונקציות הכונן כיבוי לאחר לתוקף ייכנסו.

נתונים הגנת

ב-Self-Encrypting Drive. הנתונים הגנת עבור *מושבת* או *מאופשר* של מצב מציג פירושו "מאופשר" של מצב. הכונן, *נעילת* להפעלת עד, אחרת; הוגדרה הכונן שאבטחת לגישת אימות לבצע יצטרכו לא המשתמשים Pre-Windows בכונן.

המתקדמות האבטחה פונקציות כל, מושבתת היא כאשר. מכאן Self-Encrypting Drive נתוני הגנת להשבית תוכל הגדרות כל את גם מוחקת נתותנים הגנת השבתת. רגיל ככונן יתפקד והכונן, יבוטלו Self-Encrypting Drive של האישורים לרבות, האבטחה, או משנה אינה הפונקציה, זאת עם. הכונן ומשתמשי הכונן של המערכת מנהל של בכונן משתמשים נתוני מסירה.

נעילה

לפרטים Self-Encrypting Drive בנושא עיין. Self-Encrypting Drive עבור *מושבת* או *מאופשר* של מצב מציג נעול כונן של הפעולה אופן אודות.

צורך שאין כיוון, מומלצת אינה זו עולהפ. מכאן לבצע שניתן מה, כונן נעילת זמני באופן להשבית צורך שיהיה ייתכן בכונן לנתונים לגשת יוכל בפלטפורמה משתמש שכל כך, מושבתת הכונן נעילת כאשר לכונן לגשת כדי באישורים. הכונן ומשתמשי הכונן מערכת מנהל של האישורים כולל, כלשהן אבטחה הגדרות אינהמוחקת הכונן נעילת השבתת, ונקבכ כלשהם משתמשים נתוני או.

זהירות! נתוני הגנת **Dell | גישה**, היישום של ההתקנה את תסיר אם הכונן נעילת את ולבטל Self-Encrypting Drive.

הכונן מערכת מנהל

מנהל יהיה משתמש איזה מכאן לקבוע יכול הכונן של המערכת מנהל. הכונן של הנוכחי המערכת מנהל את מציג מנהל הרשאות עם, במערכת חוקי Windows משתמש להיות החדש המערכת מנהל על. הכונן של המערכת. מערכת הכונן של בלבד אחד מערכת מנהל לכלול יכולה המערכת.

כונן משתמשי

נתמכים משתמשים של המרבי המספר. כעת הרשומים המשתמשים מספר ואת הרשומים הכונן משתמשי את מציג ה-Self-Encrypting Drive (כעת 4 משתמשים עבור כונני Seagate ו-24 כונני עבור Samsung).

Windows סיסמאות סינכרון

ב-Self-Encrypting Drive משתמשים סיסמאות אוטומטית מגדירה Windows (WPS) סיסמאות סינכרון תכונת הכונן משתמשי על חלה היא; הכונן מנהל על נאכפת אינה זו פונקציה. שלהם Windows לסיסמת זהות שיהיו רק ספציפיים זמן במרווחי סיסמאות להחליף יש שבהן ארגוניות בסביבות לשמש יכולה WPS פונקציונליות. בלבד

יעודכנו Self-Encrypting Drive-ב המשתמשים סיסמאות כל, מופעלת זו אפשרות כאשר ;(יום 90 כל למשל)
אלה Windows סיסמאות החלפת בעת אוטומטית.

הערה: סיסמאות סינכרון כאשר Windows (WPS) מופעל, לא ניתן לשנות סיסמת משתמש ב-Self-Encrypting Drive; יש להחליף סיסמת Windows כדי לעדכן את סיסמת הכונן אוטומטית.

אחרון משתמש שם זכור
אימות במסך **משתמש שם** בשדה מחדל כברירת יוצג שהוזן האחרון המשתמש שם, מופעלת זו אפשרות כאשר Pre-Windows.

משתמש שם בחירת
אימות במסך **משתמש שם** בשדה המשתמשים שמות כל את להציג יכולים משתמשים, מופעלת זו אפשרות כאשר Pre-Windows.

קריפטוגרפית מחיקה
את מוחקת באמת לא זו פעולה .Self-Encrypting Drive-ב הנתונים כל את "למחוק" כדי לשמש יכולה זו אפשרות לשימוש ניתנים לבלתי הנתונים את הופכת וכך, הנתונים להצפנת המשמשים המפתחות את מוחקת אלא, הנתונים. קריפטוגרפית מחיקה לאחר כונן נתוני לשחזר אפשרות יוא כן, כמו ;Self-Encrypting Drive-ב נתונים הגנת מחדש לייעוד מוכן והכונן, זמינה לבלתי הופכת.

הערות:

- Self-Encrypting Drive, המחשב את כבה של הניהול לפונקציות הקשורות שגיאה הודעות תקבל אם מחדש הפעל ואז, (שמחד הפעלה לא) לחלוטין.
- ספציפית שגיאה הודעת אודות יותר מפורט במידע מעוניין אתה אם, אל עבור wave.com/support/Dell.

אימות התקן פרטי

קורא כמו) המחוברים האימות התקני כל עבור ומצבים מידע מציג **התקנים ניהול**ב 'אימות התקני פרטי' חלון
במערכת (Contactless או מסורתיים Smartcards קורא ,אצבע טביעות.

טכנית תמיכה

בכתובת למצוא ניתן **גישה | Dell נתוני הגנת** תוכנת עבור טכנית תמיכה
http://www.wave.com/support.dell.com.

Wave TCG-Enabled CSP

הגנת ביישום כלול (TCG) Wave Systems Trusted Computing Group תומך (CSP) ההצפנה שירותי ספק מרשימת לבחירה או מהיישום בקריאה ישירות - נדרש CSP שבו מקום בכל לשימוש וזמין, **גישה | Dell נתוני** מפתחותה את יוצר PTM-שה להבטיח כדי Wave TCG-Enabled CSP-ב בחר, כשאפשר .מותקנים CSP **גישה | Dell נתוני תהגנ** ידי-על מנוהלים שלהם והסיסמאות ושהמפתחות.

ה-Wave Systems TCG-enabled CSP תואמות בפלטפורמות הזמינות בפונקציות להשתמש ליישומים מאפשר פונקציונליות מספק TCG באמצעות המשופר MSCAPI CSP באמצעות ישירות TCG MSCAPI. מודול בדרישות תלות ללא ,TPM ידי-על המסופקת המשופרת האבטחה את וממנף TPM-ב ותמפתח של אסימטרית לספק בנוגע לספק ספציפיות Trusted Software Stack (TSS).

הערה: מפתחות אם TPM ידי-על שנוצרו Wave TCG-enabled CSP סיסמה דורשים, סיסמת יצר והמשתמש TPM. סיסמאות מאגרב ויישמרו באקראי ייווצרו השונות המפתח סיסמאות, ראשית TPM