หน้าแรกของ Dell Data Protection | Access

หน้าแรกของ **Dell Data Protection | Access** คือจุดเริ่มต้นสำหรับการเข้าถึงคุณสมบัติต่างๆ ของโปรแกรมประยุกต์นี้ จากหน้าต่างนี้ คุณสามารถเข้าถึงส่วนต่างๆ ต่อไปนี้:

System Access Wizard
ตัวเลือกการเข้าถึง
Self-Encrypting Drive
ตัวเลือกขั้นสูง

ที่มุมขวาล่างของหน้าต่างนี้คือลิงก์ที่เรียกว่า **ขั้นสูง** ที่คุณสามารถคลิกเพื่อเข้าถึงตัวเลือกการทำงานขั้นสูง

จาก ตัวเลือกขั้นสูง คุณสามารถคลิกลิงก์ **หน้าแรก** ที่มุมขวาด้านล่างของหน้าต่างเพื่อกลับมายังหน้าแรก

System Access Wizard

System Access Wizard ทำงานโดยอัตโนมัติในครั้งแรกที่เรียกใช้งานโปรแกรมประยุกต์ **Dell Data Protection | Access** ตัวช่วยสร้างนี้จะแนะนำคุณตลอดขั้นตอนการตั้งค่าระบบรักษาความปลอดภัยทั้งหมดในระบบของคุณ รวมถึงวิธีการ (เช่น รหัสผ่านเท่านั้นหรือลายนิ้วมือและรหัสผ่าน) และช่วงเวลา (ขั้น Windows, pre-Windows หรือทั้งสองกรณี) ที่คุณต้องการเข้าสู่ระบบ นอกจากนี้ หากระบบของคุณมี self-encrypting drive คุณสามารถกำหนดค่าได้ผ่านทางตัวช่วยสร้างนี้

ฟังก์ชันผู้ดูแล

ผู้ใช้ที่ได้รับการตั้งค่าให้มีสิทธิ์ระดับผู้ดูแล Windows ในระบบมีสิทธิ์ที่จะดำเนินการฟังก์ชันต่อไปนี้ใน **Dell Data Access | Protection** ซึ่งผู้ใช้มาตรฐานไม่สามารถทำได้:

- ตั้ง / เปลี่ยนรหัสผ่านระบบ (Pre-Windows)
- ตั้ง / เปลี่ยนรหัสผ่านฮาร์ดไดรฟ์
- ตั้ง / เปลี่ยนรหัสผ่านผู้ดูแล
- ตั้ง / เปลี่ยนรหัสผ่านเจ้าของ TPM
- ตั้ง / เปลี่ยนรหัสผ่านผู้ดูแล ControlVault
- รีเซ็ตระบบ
- เก็บถาวรและเรียกคืนใบรับรอง
- ตั้ง / เปลี่ยน PIN ผู้ดูแล smartcard
- ล้าง / รีเซ็ต smartcard
- เปิดใช้งาน / ยกเลิกใช้งานการเข้าสู่ระบบที่ปลอดภัยของ Dell ใน Windows
- ตั้งนโยบายการเข้าสู่ระบบ Windows
- จัดการ self-encrypting drives ซึ่งรวมถึง:
    - เปิดใช้งาน / ยกเลิกใช้งานการล็อค self-encrypting drive
    - เปิดใช้งาน / ยกเลิกใช้งานการซิงโครไนซ์รหัสผ่าน Windows (WPS)
    - เปิดใช้งาน / ยกเลิกใช้งาน Single Sign On (SSO)
    - ดำเนินการลบการเข้ารหัส

การจัดการระยะไกล

องค์กรของคุณสามารถกำหนดสภาพแวดล้อมที่ให้ฟังก์ชันการรักษาความปลอดภัยของโปรแกรมประยุกต์ **Dell Data Protection | Access** บนแพลตฟอร์มหลายแพลตฟอร์มได้รับการจัดการจากระบบศูนย์กลาง (เช่น การจัดการระยะไกล) ในกรณีนี้ โครงสร้างพื้นฐานระบบรักษาความปลอดภัยของ Windows เช่น Active Directory สามารถใช้เพื่อจัดการคุณสมบัติเฉพาะของ **Dell Data Protection | Access**

เมื่อคอมพิวเตอร์ถูกจัดการจากระยะไกล (เช่น "เป็นเจ้าของแล้ว" โดยผู้ดูแลระยะไกล) การจัดการดูแลในเครื่องของการทำงาน **Dell Data Protection | Access** จะถูกยกเลิกใช้งาน หน้าต่างการจัดการของโปรแกรมจะไม่สามารถเข้าถึงได้จากในเครื่อง การจัดการของฟังก์ชันต่อไปนี้สามารถดำเนินการได้จากระยะไกล:

- Trusted Platform Module (TPM)
- ControlVault
- การเข้าสู่ระบบ Pre-Windows
- รีเซ็ตระบบ
- รหัสผ่าน BIOS
- นโยบายเข้าสู่ระบบของ Windows
- Self-Encrypting Drive
- การลงทะเบียนลายนิ้วมือและ Smartcard

หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับการใช้ Wave Systems' EMBASSY® Remote Administration Server (ERAS) สำหรับการจัดการระยะไกล โปรดติดต่อตัวแทนจำหน่าย Dell ของคุณ หรือไปที่ dell.com

ตัวเลือกการเข้าถึง

จากหน้าต่าง ตัวเลือกการเข้าถึง คุณสามารถตั้งค่าวิธีที่คุณจะเข้าถึงระบบของคุณ

หากคุณมีการตั้งค่าตัวเลือก **Dell Data Protection | Access** ใดๆ ไว้แล้ว ตัวเลือกที่สามารถใช้ได้เหล่านั้นจะแสดงให้เห็นที่หน้าแรก (เช่น เปลี่ยนรหัสผ่านสำหรับการเข้าสู่ระบบ Pre-Windows) ตัวเลือกที่สามารถใช้ได้นี้เป็นทางลัด ซึ่งเมื่อคลิกจะนำคุณไปยังหน้าต่างที่เกี่ยวข้องสำหรับทำงานเฉพาะนั้นๆ (เช่น เปลี่ยนรหัสผ่าน pre-Windows ของคุณหรือลงทะเบียนลายนิ้วมืออื่น)

ทั่วไป
อันดับแรก คุณสามารถระบุช่วงที่จะเข้าสู่ระบบ (Windows, pre-Windows หรือทั้งสองแบบ) และวิธีการเข้าสู่ระบบ (เช่น ลายนิ้วมือหรือรหัสผ่าน) คุณสามารถเลือกตัวเลือกหนึ่งหรือสองตัวเลือกสำหรับวิธีการเข้าสู่ระบบ ซึ่งได้แก่ การรวมวิธีระหว่างลายนิ้วมือ, smartcard และรหัสผ่าน ตัวเลือกที่แสดงจะยึดตามนโยบายการเข้าสู่ระบบที่ใช้กับสภาพแวดล้อมของคุณและสิ่งที่แพลตฟอร์มนั้นสนับสนุน

ลายนิ้วมือ
หากระบบของคุณมีตัวอ่านลายนิ้วมือ คุณสามารถลงทะเบียนหรืออัพเดตลายนิ้วมือเพื่อใช้ในการเข้าสู่ระบบของคุณ เมื่อคุณลงทะเบียนลายนิ้วมือแล้ว คุณสามารถกวาดนิ้วบนตัวอ่านลายนิ้วมือของระบบเพื่อเข้าสู่ระบบที่ Windows, pre-Windows หรือทั้งสองกรณี (ขึ้นอยู่กับตัวเลือกที่คุณระบุไว้ใน การเข้าถึงทั่วไป) โปรดดูการลงทะเบียนลายนิ้วมือผู้ใช้ สำหรับรายละเอียดเพิ่มเติม

การเข้าสู่ระบบ Pre-Windows
หากคุณได้ระบุให้ผู้ใช้ต้องเข้าสู่ระบบ pre-Windows คุณต้องตั้งค่ารหัสผ่านระบบ (หรือบางครั้งเรียกว่ารหัสผ่าน pre-Windows) สำหรับการเข้าถึง pre-Windows เมื่อตั้งค่าแล้ว ผู้ดูแลระบบสามารถเปลี่ยนรหัสผ่านนี้ได้ทุกเมื่อ

คุณสามารถปิดใช้งานการเข้าสู่ระบบ pre-Windows ได้จากหน้าจอนี้ โดยคุณจะต้องป้อนรหัสผ่านระบบที่ใช้ในปัจจุบันยืนยันว่ารหัสผ่านนั้นถูกต้อง จากนั้นคลิกปุ่ม **ยกเลิกใช้งาน**

Smartcard
หากคุณได้ระบุให้ผู้ใช้ต้องใช้ smartcard เพื่อเข้าสู่ระบบ คุณต้องลงทะเบียน smartcard แบบทั่วไป (contacted) หรือ contactless smartcard อย่างน้อยหนึ่งใบ คลิกลิงก์ **ลงทะเบียน smartcard อื่น** เพื่อเรียกใช้ตัวช่วยสร้างการลงทะเบียน smartcard การลงทะเบียนหมายถึงการตั้งค่า smartcard ของคุณเพื่อใช้ในการเข้าสู่ระบบ

เมื่อคุณลงทะเบียน smartcard แล้ว คุณสามารถเปลี่ยนหรือตั้งค่ารหัส PIN สำหรับการ์ดนั้นโดยใช้ลิงก์ **เปลี่ยนหรือตั้งค่า smartcard PIN**

การเข้าสู่ระบบ Pre-Windows

เมื่อตั้งค่าการเข้าสู่ระบบ pre-Windows คุณต้องระบุการรับรอง (รหัสผ่าน ลายนิ้วมือ หรือ smartcard) เมื่อเปิดระบบก่อนโหลด Windows การทำงานการเข้าสู่ระบบ pre-Windows เป็นการรักษาความปลอดภัยเพิ่มเติมให้กับระบบ โดยป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตจากการเข้าสู่ Windows และเข้าถึงคอมพิวเตอร์ (เช่น เมื่อถูกขโมย)

จากหน้าจอการเข้าสู่ระบบ Pre-Windows ผู้ดูแลสามารถตั้งค่าการเข้าสู่ระบบ pre-Windows หรือสร้างหรือเปลี่ยนแปลงรหัสผ่าน pre-Windows (ระบบ) หากมีการตั้งรหัสผ่านนี้ไว้แล้ว คุณสามารถยกเลิกใช้งานการเข้าสู่ระบบ pre-Windows ได้จากหน้าต่างนี้ การตั้งค่าการเข้าสู่ระบบ pre-Windows จะเรียกใช้ตัวช่วยสร้าง ซึ่งจะทำงานต่อไปนี้:

- รหัสผ่านระบบ: ตั้งรหัสผ่านระบบ (หรือที่เรียกว่ารหัสผ่าน pre-Windows) สำหรับเข้าถึง pre-Windows รหัสผ่านนี้ยังจะใช้เป็นรหัสสำรองในกรณีที่ผู้ใช้มีองค์ประกอบการรับรองเพิ่มเติม (เช่น เพื่อเข้าถึงระบบหากมีปัญหากับตัวตรวจจับลายนิ้วมือ)
- ลายนิ้วมือหรือ Smartcard: กำหนดลายนิ้วมือหรือ smartcard สำหรับใช้ในการเข้าสู่ระบบ pre-Windows และระบุว่าองค์ประกอบการรับรองใดจะถูกใช้แทนหรือเพิ่มเติมจากรหัสผ่าน pre-Windows
- Single Sign On: ตามค่าเริ่มต้น การรับรอง pre-Windows ของคุณ (รหัสผ่าน ลายนิ้วมือ หรือ smartcard) จะถูกใช้เพื่อลงชื่อคุณเข้าสู่ Windows โดยอัตโนมัติเช่นกัน (ซึ่งเรียกว่า "Single Sign On") หากต้องการยกเลิกใช้งานคุณสมบัตินี้ เลือกกล่องกาเครื่องหมาย "ฉันต้องการเข้าสู่ระบบอีกครั้งที่ Windows"
- หากรหัสผ่านฮาร์ดไดรฟ์ BIOS ถูกกำหนดเพิ่มเติมกับรหัสผ่าน pre-Windows คุณยังจะมีตัวเลือกในการเปลี่ยนแปลงหรือยกเลิกใช้งานรหัสผ่านฮาร์ดไดรฟ์ด้วย

หมายเหตุ: ตัวอ่านลายนิ้วมือบางประเภทไม่สามารถเปิดใช้งานสำหรับการรับรอง pre-Windows หากตัวอ่านของคุณไม่สามารถใช้งานร่วมกันได้ คุณจะสามารถลงทะเบียนลายนิ้วมือสำหรับการเข้าสู่ระบบ Windows เท่านั้น หากต้องการตรวจว่าตัวอ่านลายนิ้วมือนั้นๆ สามารถใช้งานร่วมกันได้หรือไม่ ติดต่อผู้ดูแลระบบของคุณหรือไปที่ support.dell.com เพื่อดูรายการตัวอ่านลายนิ้วมือที่สนับสนุน

ยกเลิกใช้งานการเข้าสู่ระบบ Pre-Windows

คุณสามารถปิดใช้งานการเข้าสู่ระบบ pre-Windows ได้จากหน้าต่างนี้ โดยคุณจะต้องป้อนรหัสผ่าน pre-Windows (ระบบ) ที่ใช้ในปัจจุบัน ยืนยันว่ารหัสผ่านนั้นถูกต้อง จากนั้นคลิกปุ่ม **ยกเลิกใช้งาน** โปรดทราบว่าเมื่อคุณยกเลิกใช้งานการเข้าสู่ระบบ pre-Windows ลายนิ้วมือหรือ smartcard ใดๆ ที่ลงทะเบียนไว้ยังคงลงทะเบียนอยู่

การลงทะเบียน / การลบลายนิ้วมือ

ผู้ใช้สามารถลงทะเบียนหรืออัพเดตลายนิ้วมือ ที่นำไปใช้เพื่อรับรองกับระบบทั้งเมื่ออยู่ที่ pre-Windows หรือเพื่อเข้าสู่ระบบ Windows ในแท็บลายนิ้วมือ ภาพของมือแสดงนิ้วที่ได้ลงทะเบียนไว้ หากมี เมื่อคลิกลิงก์ **ลงทะเบียนนิ้วอื่น** จะเรียกใช้งานตัวช่วยสร้างการลงทะเบียนลายนิ้วมือ ซึ่งจะแนะนำคุณตลอดขั้นตอนการลงทะเบียน "การลงทะเบียน" หมายถึงการบันทึกลายนิ้วมือที่จะใช้สำหรับการเข้าสู่ระบบ คุณต้องมีตัวอ่านลายนิ้วมือที่ใช้ได้ติดตั้งและกำหนดค่าไว้อย่างเหมาะสมแล้วเพื่อลงทะเบียนลายนิ้วมือ

หมายเหตุ: ตัวอ่านลายนิ้วมือบางประเภทไม่สามารถใช้สำหรับการเข้าสู่ระบบ pre-Windows ข้อความแสดงข้อผิดพลาดจะแสดงขึ้นหากคุณพยายามลงทะเบียนในขั้น pre-Windows ด้วยตัวอ่านที่ไม่สามารถใช้งานร่วมกันได้ หากต้องการตรวจว่าอุปกรณ์สามารถใช้งานร่วมกันได้หรือไม่ ติดต่อผู้ดูแลระบบของคุณหรือไปที่ support.dell.com เพื่อดูรายการตัวอ่านลายนิ้วมือที่สนับสนุน

เมื่อลงทะเบียนลายนิ้วมือ ระบบจะแจ้งให้คุณป้อนรหัสผ่าน Windows ของคุณเพื่อตรวจสอบตัวตน หากนโยบายของคุณกำหนดไว้ คุณจะได้รับแจ้งให้ป้อนรหัสผ่าน Pre-Windows (ระบบ) ด้วยเช่นกัน คุณสามารถใช้รหัสผ่าน Pre-Windows เพื่อเข้าถึงระบบหากมีปัญหากับตัวอ่านลายนิ้วมือ

หมายเหตุ:

- ขอแนะนำให้คุณลงทะเบียนลายนิ้วมืออย่างน้อยสองนิ้วระหว่างขั้นตอนการลงทะเบียนนี้
- คุณต้องแน่ใจว่าลายนิ้วมือได้รับการลงทะเบียนอย่างถูกต้องก่อนเปิดใช้งานคุณสมบัติการรับรองด้วยลายนิ้วมือ
- หากคุณเปลี่ยนตัวอ่านลายนิ้วมือบนระบบ คุณต้องลงทะเบียนลายนิ้วมืออีกครั้งกับตัวอ่านเครื่องใหม่ ไม่แนะนำให้สลับการใช้ไปมาระหว่างตัวอ่านลายนิ้วมือที่ต่างกันสองเครื่อง
- หากคุณเห็นข้อความ "เซนเซอร์สูญเสียโฟกัส" เกิดขึ้นซ้ำๆ เมื่อลงทะเบียนลายนิ้วมือ อาจหมายความว่าคอมพิวเตอร์ไม่รู้จักตัวอ่านลายนิ้วมือเครื่องนั้น หากตัวอ่านลายนิ้วมือเป็นอุปกรณ์ภายนอก การถอดการเชื่อมต่อตัวอ่านลายนิ้วมือแล้วเชื่อมต่อใหม่มักจะแก้ปัญหานี้ได้

การล้างลายนิ้วมือที่ลงทะเบียนไว้
คุณสามารถลบลายนิ้วมือที่ลงทะเบียนไว้โดยคลิกลิงก์ **ลบลายนิ้วมือ** หรือคลิกที่ (เพื่อยกเลิกการเลือก) ลายนิ้วมือที่ลงทะเบียนไว้ในตัวช่วยสร้างการลงทะเบียนลายนิ้วมือ

หากต้องการลบผู้ใช้เฉพาะรายที่มีลายนิ้วมือลงทะเบียนไว้สำหรับการรับรอง pre-Windows ผู้ดูแลสามารถยกเลิกการเลือกลายนิ้วมือทั้งหมดที่ลงทะเบียนไว้สำหรับผู้ใช้รายนั้น

หมายเหตุ: หากคุณได้รับข้อผิดพลาดระหว่างขั้นตอนการลงทะเบียนลายนิ้วมือ คุณสามารถดูที่ wave.com/support/Dell สำหรับรายละเอียดเพิ่มเติม

การลงทะเบียน Smart Cards

Dell Data Protection | Access ให้คุณมีทางเลือกในการใช้ smartcard แบบธรรมดา (สัมผัส) หรือ contactless smartcard สำหรับการเข้าสู่บัญชี Windows ของคุณ หรือสำหรับการรับรองเมื่ออยู่ที่ pre-Windows โดยในแท็บ Smartcard คลิกลิงก์ **ลงทะเบียน smartcard อื่น** เพื่อเรียกใช้งานตัวช่วยสร้างการลงทะเบียน Smartcard ซึ่งจะแนะนำคุณตลอดขั้นตอนการลงทะเบียน "การลงทะเบียน" หมายถึงการตั้งค่า smartcard ของคุณเพื่อใช้ในการเข้าสู่ระบบ

คุณต้องมีอุปกรณ์การตรวจรับรอง smartcard ที่ใช้ได้ติดตั้งและกำหนดค่าไว้แล้วเพื่อดำเนินการลงทะเบียนนี้

หมายเหตุ: หากต้องการตรวจว่าอุปกรณ์ที่มีสามารถใช้งานร่วมกันได้หรือไม่ ติดต่อผู้ดูแลระบบของคุณหรือไปที่ support.dell.com เพื่อดูรายการ smartcard ที่สนับสนุน

การลงทะเบียน
เมื่อลงทะเบียน smartcard ระบบจะแจ้งให้คุณป้อนรหัสผ่าน Windows ของคุณเพื่อตรวจสอบตัวตน หากนโยบายของคุณกำหนดไว้ คุณจะได้รับแจ้งให้ป้อนรหัสผ่าน Pre-Windows (ระบบ) ด้วยเช่นกัน คุณสามารถใช้รหัสผ่าน Pre-Windows เพื่อเข้าถึงระบบหากมีปัญหากับตัวอ่าน smartcard

ระหว่างการลงทะเบียน คุณจะได้รับแจ้งให้ป้อน smartcard PIN หากมีการตั้งไว้ หากนโยบายของคุณกำหนดให้ใช้ PIN และยังไม่มีการตั้งไว้ ระบบจะแจ้งให้คุณสร้างรหัส

หมายเหตุ:

- เมื่อผู้ใช้ถูกลงทะเบียน smartcard สำหรับใช้ในขั้น pre-Windows แล้ว จะไม่สามารถลบออกได้
- ผู้ใช้ทั่วไปสามารถเปลี่ยนแปลง PIN ของผู้ใช้บน smartcard และผู้ดูแลสามารถเปลี่ยนแปลงทั้ง PIN ของผู้ดูแล และ PIN ของผู้ใช้
- ผู้ดูแลยังสามารถรีเซ็ต smartcard เมื่อรีเซ็ตแล้ว จะไม่สามารถใช้ smartcard นั้นสำหรับการรับรองเมื่อเข้าสู่ระบบ Windows หรือเมื่ออยู่ที่ pre-Windows จนกว่าจะมีการลงทะเบียนอีกครั้ง

หมายเหตุ: สำหรับการรับรองใบรับรอง TPM ผู้ดูแลสามารถลงทะเบียนใบรับรอง TPM ผ่านทางขั้นตอนการลงทะเบียน Microsoft Windows smartcard ผู้ดูแลต้องเลือก "Wave TCG-Enabled CSP" เป็นผู้ให้บริการการเข้ารหัส (Cryptographic Service Provider) แทน Smartcard CSP เพื่อให้สามารถใช้งานร่วมกันได้กับโปรแกรมประยุกต์นี้ นอกจากนี้ ยังต้องเปิดใช้งานการเข้าสู่ระบบที่ปลอดภัยของ Dell พร้อมทั้งกำหนดนโยบายประเภทการรับรองที่เหมาะสมสำหรับไคลเอนต์ด้วย

หมายเหตุ: หากคุณได้รับข้อผิดพลาดที่ระบุว่า บริการ Smartcard ไม่ทำงาน คุณต้องเริ่มต้น/เริ่มต้นบริการนี้ใหม่ โดยดำเนินการดังนี้:

- นำทางไปที่หน้าต่างเครื่องมือผู้ดูแลระบบจาก Control Panel เลือก บริการ จากนั้นคลิกขวาที่ Smartcard และเลือก เริ่มต้น หรือ เริ่มต้นใหม่
- หากคุณต้องการข้อมูลโดยละเอียดเกี่ยวกับข้อความแสดงข้อผิดพลาดที่เจาะจง ไปที่ wave.com/support/Dell

ภาพรวม Self-Encrypting Drive

Dell Data Protection | Access จัดการฟังก์ชันการรักษาความปลอดภัยที่ใช้ฮาร์ดแวร์ของ self-encrypting drives ซึ่งมีการเข้ารหัสข้อมูลที่ฝังอยู่ในฮาร์ดแวร์ของไดรฟ์ การทำงานฟังก์ชันนี้ใช้เพื่อให้ความมั่นใจว่ามีเพียงผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลที่เข้ารหัส (เมื่อเปิดใช้งานการล็อคไดรฟ์)

หน้าต่าง Self-Encrypting Drive สามารถเข้าถึงได้โดยคลิกแท็บด้านล่าง **Self-Encrypting Drive** แท็บนี้แสดงให้เห็นต่อเมื่อมี self-encrypting drives (SED) หนึ่งตัวขึ้นไปในระบบของคุณเท่านั้น

คลิกลิงก์ **ตั้งค่า** เพื่อเริ่มตัวช่วยสร้างการตั้งค่า Self-Encrypting Drive ในตัวช่วยสร้างนี้ คุณจะสร้างรหัสผ่านผู้ดูแลไดรฟ์ สำรองข้อมูลรหัสผ่านนี้ และใช้การตั้งค่าการเข้ารหัสไดรฟ์ของคุณ เฉพาะผู้ดูแลระบบเท่านั้นที่สามารถเข้าถึงตัวช่วยสร้างการตั้งค่า Self-Encrypting Drive

สิ่งสำคัญ! เมื่อตั้งค่าไดรฟ์แล้ว การป้องกันข้อมูลและการล็อคไดรฟ์ จะถูก "เปิดใช้งาน" เมื่อไดรฟ์ถูกล็อค สิ่งต่อไปนี้จะเกิดขึ้น:

- ไดรฟ์เข้าสู่โหมด *ล็อค* ทุกครั้งที่ปิดการจ่ายไฟเข้าไดรฟ์
- ไดรฟ์จะไม่บูตเว้นแต่ผู้ใช้ป้อนชื่อผู้ใช้และรหัสผ่าน (หรือลายนิ้วมือ) ถูกต้องที่หน้าจอเข้าสู่ระบบ Pre-Windows ก่อนเปิดใช้งานการล็อคไดรฟ์ ผู้ใช้ทุกคนบนคอมพิวเตอร์เครื่องนั้นสามารถเข้าถึงข้อมูลในไดรฟ์ได้
- ไดรฟ์ได้รับการรักษาความปลอดภัยแม้ในเวลาที่ปลั๊กเข้ากับคอมพิวเตอร์เครื่องอื่นเพื่อใช้เป็นไดรฟ์ที่สอง โดยต้องผ่านการรับรองเพื่อเข้าถึงข้อมูลในไดรฟ์

เมื่อตั้งค่าไดรฟ์แล้ว หน้าต่าง Self-Encrypting Drive จะแสดงไดรฟ์และลิงก์สำหรับผู้ใช้เพื่อเปลี่ยนรหัสผ่านไดรฟ์ของตน หากคุณคือผู้ดูแลไดรฟ์ คุณยังจะสามารถเพิ่มหรือลบผู้ใช้ไดรฟ์ออกได้จากหน้าต่างนี้ หากมีไดรฟ์ภายนอกที่ถูกตั้งค่าไว้ ก็จะแสดงให้เห็นในหน้าต่างนี้และสามารถปลดล็อคได้

หมายเหตุ: ในการล็อคไดรฟ์ที่สองภายนอก ไดรฟ์นั้นต้องได้รับการตัดไฟแยกจากคอมพิวเตอร์

ผู้ดูแลไดรฟ์สามารถจัดการการตั้งค่าไดรฟ์ได้ใน **ขั้นสูง > อุปกรณ์** สำหรับข้อมูลเพิ่มเติม โปรดดู การจัดการอุปกรณ์ - Self-Encrypting Drives

การตั้งค่าไดรฟ์

ตัวช่วยสร้างการตั้งค่า Self-Encrypting Drive จะแนะนำคุณตลอดขั้นตอนการตั้งค่าไดรฟ์ของคุณ แนวคิดต่อไปนี้เป็นสิ่งสำคัญที่พึงระลึกถึงเมื่อดำเนินการตามขั้นตอนนี้

ผู้ดูแลไดรฟ์

ผู้ใช้คนแรกที่มีสิทธิ์การใช้ระดับผู้ดูแลระบบ ซึ่งเป็นผู้ตั้งค่าการเข้าถึงไดรฟ์ (และตั้งรหัสผ่านผู้ดูแลไดรฟ์) ถือเป็นผู้ดูแลไดรฟ์และจะเป็นผู้ใช้คนเดียวที่มีสิทธิ์ทำการเปลี่ยนแปลงการเข้าถึงไดรฟ์ เพื่อให้แน่ใจว่าผู้ใช้คนแรกได้รับการตั้งโดยเจตนาให้เป็นผู้ดูแลไดรฟ์ คุณต้องเลือกกล่องกาเครื่องหมาย "ข้าพเจ้าเข้าใจ" เพื่อดำเนินการต่อไปในขั้นตอนนี้

รหัสผ่านผู้ดูแลไดรฟ์

ตัวช่วยสร้างจะแจ้งให้คุณสร้างรหัสผ่านผู้ดูแลไดรฟ์และให้ป้อนรหัสผ่านดังกล่าวอีกครั้งเพื่อเป็นการยืนยัน คุณต้องป้อนรหัสผ่าน Windows ของคุณเพื่อสร้างข้อมูลเฉพาะตัวของคุณก่อนที่คุณจะสามารถสร้างรหัสผ่านผู้ดูแลไดรฟ์ ผู้ใช้ Windows ปัจจุบันต้องมีสิทธิ์ระดับผู้ดูแลในการสร้างรหัสผ่านนี้

สำรองข้อมูลใบรับรองไดรฟ์

พิมพ์ที่ตั้ง หรือคลิกปุ่ม **Browse** เพื่อเลือกที่ตั้ง เพื่อบันทึกสำเนาสำรองของใบรับรองผู้ดูแลไดรฟ์ของคุณ

สิ่งสำคัญ!

- ขอแนะนำอย่างจริงจังให้คุณสำรองข้อมูลใบรับรองเหล่านี้ และทำการสำรองข้อมูลลงในไดรฟ์อื่นที่ไม่ใช่ฮาร์ดไดรฟ์หลักของคุณ (เช่น สื่อเก็บข้อมูลแบบถอดได้) มิเช่นนั้น หากคุณไม่สามารถเข้าถึงไดรฟ์ของคุณได้ คุณจะไม่สามารถเข้าถึงข้อมูลสำรองด้วย
- เมื่อคุณตั้งค่าไดรฟ์เรียบร้อยแล้ว ผู้ใช้ทุกคนจะต้องป้อนชื่อผู้ใช้และรหัสผ่าน (หรือลายนิ้วมือ) ที่ถูกต้อง ก่อน Windows จะโหลด เพื่อเข้าถึงระบบในครั้งถัดไปที่เปิดระบบ

เพิ่มผู้ใช้ไดรฟ์
ผู้ดูแลไดรฟ์สามารถเพิ่มผู้ใช้อื่นให้กับไดรฟ์ ซึ่งเป็นผู้ใช้ Windows ที่ถูกต้อง เมื่อเพิ่มผู้ใช้ให้กับไดรฟ์ ผู้ดูแลมีทางเลือกที่จะกำหนดให้ผู้ใช้ต้องรีเซ็ตรหัสผ่านของตนเมื่อเข้าสู่ระบบเป็นครั้งแรก ผู้ใช้จะถูกกำหนดให้รีเซ็ตรหัสผ่านของตนที่หน้าจอการรับรอง pre-Windows ก่อนไดรฟ์จะปลดล็อค

การตั้งค่าขั้นสูง

- *Single Sign On* - ตามค่าเริ่มต้น รหัสผ่าน Self-Encrypting Drive ของคุณ ซึ่งคุณป้อนใน pre-Windows เพื่อรับรองความถูกต้องกับไดรฟ์ จะถูกใช้เพื่อลงชื่อคุณเข้าสู่ Windows โดยอัตโนมัติเช่นกัน (ซึ่งเรียกว่า "Single Sign On") หากต้องการยกเลิกใช้คุณสมบัตินี้ เลือกกล่องกาเครื่องหมาย "ฉันต้องการเข้าสู่ระบบอีกครั้งเมื่อ Windows เริ่มต้น" เมื่อกำหนดค่าการตั้งค่าไดรฟ์ของคุณ
- *เข้าสู่ระบบด้วยลายนิ้วมือ* - บนแพลตฟอร์มที่สนับสนุน คุณสามารถระบุว่าคุณต้องการให้มีการรับรองกับ self-encrypting drive ของคุณโดยใช้ลายนิ้วมือแทนรหัสผ่าน
- *สนับสนุนโหมดพัก/สแตนด์บาย(S3)* (หากแพลตฟอร์มสนับสนุน) - หากเปิดใช้งาน, Self-encrypting drive ของคุณสามารถเข้าสู่โหมดพัก/สแตนด์บาย (หรือเรียกว่าโหมด S3) ที่ปลอดภัยได้และจะต้องมีการรับรอง pre-Windows เมื่อออกจากโหมดพัก/สแตนด์บาย

หมายเหตุ:

- เมื่อการสนับสนุน S3 ถูกเปิดใช้งาน รหัสผ่านการเข้ารหัสไดรฟ์จะเป็นไปตามข้อจำกัดรหัสผ่าน BIOS ใดๆ ที่อาจมีอยู่ ตรวจสอบกับผู้ผลิตฮาร์ดแวร์ระบบสำหรับข้อมูลเพิ่มเติมเกี่ยวกับข้อจำกัดรหัสผ่าน BIOS เจาะจงที่อาจมีอยู่ในระบบนั้น
- Self-encrypting drives บางตัวอาจไม่สนับสนุนโหมด S3 คุณจะได้รับแจ้งว่าไดรฟ์นั้นสนับสนุนโหมดพัก/สแตนด์บายหรือไม่ระหว่างการตั้งค่าไดรฟ์ สำหรับไดรฟ์ที่ไม่สนับสนุนโหมดนี้ การขอ Windows S3 จะถูกแปลงเป็นการขอไฮเบอร์เนตโดยอัตโนมัติหากเปิดใช้งานโหมดไฮเบอร์เนตไว้ (ขอแนะนำอย่างจริงจังให้คุณเปิดใช้งานโหมดไฮเบอร์เนตบนคอมพิวเตอร์ของคุณ)
- ในครั้งแรกที่คุณเข้าสู่ระบบหลังจากตั้งตัวเลือก Single Sign On (SSO) ขั้นตอนนี้จะหยุดชั่วคราวที่หน้าแจ้งเข้าสู่ระบบ Windows คุณจะต้องป้อนรูปแบบการรับรอง Windows ของคุณ ซึ่งจะถูกจัดเก็บอย่างปลอดภัยสำหรับใช้ในการเข้าสู่ระบบ Windows ในอนาคต ครั้งถัดไปที่ระบบถูกบูต SSO จะนำคุณเข้าสู่ Windows โดยอัตโนมัติ จำเป็นต้องใช้ขั้นตอนเดียวกันนี้ด้วยเมื่อเปลี่ยนรูปแบบการรับรอง Windows (รหัสผ่าน ลายนิ้วมือ, Smartcard PIN) ของผู้ใช้ หากคอมพิวเตอร์อยู่ในโดเมน และโดเมนนั้นมีนโยบายที่กำหนดให้กด ctrl+alt+del สำหรับการเข้าสู่ระบบ Windows ก็จะต้องทำตามนโยบายนี้

ข้อควรระวัง! หากคุณถอนการติดตั้งโปรแกรมประยุกต์ **Dell Data Protection | Access** ก่อนอื่นคุณต้องยกเลิกใช้งานการป้องกันข้อมูลของ self-encrypting drive และปลดล็อคไดรฟ์

ฟังก์ชันผู้ใช้ Self-Encrypting Drive

ผู้ดูแล Self-encrypting drive ดำเนินการจัดการการรักษาความปลอดภัยทั้งหมดของไดรฟ์และผู้ใช้ ผู้ใช้ไดรฟ์ที่ไม่ใช่ผู้ดูแลไดรฟ์สามารถดำเนินการเฉพาะงานต่อไปนี้:

- เปลี่ยนรหัสผ่านไดรฟ์ของตนเอง
- ปลดล็อคไดรฟ์

งานเหล่านี้สามารถเข้าถึงได้จากแท็บ **Self-Encrypting Drive** ใน **Dell Data Protection | Access**

เปลี่ยนรหัสผ่าน

ช่วยให้ผู้ใช้ที่ลงทะเบียนสามารถสร้างรหัสผ่านใหม่เพื่อการรับรองไดรฟ์ของตนเอง คุณต้องป้อนรหัสผ่าน Self-Encrypting Drive ปัจจุบันก่อนตั้งรหัสผ่านไดรฟ์เป็นค่าใหม่

หมายเหตุ:

- โปรแกรมประยุกต์นี้จะบังคับใช้นโยบายความซับซ้อนในรหัสผ่านและความยาวรหัสผ่านของ Windows หากมีการเปิดใช้งานไว้ หากไม่มีการเปิดใช้งานนโยบายรหัสผ่านของ Windows ความยาวสูงสุดสำหรับรหัสผ่านของ Self-Encrypting Drive คือ 32 อักขระ โปรดทราบว่าความยาวสูงสุดนี้คือ 127 อักขระหากไม่ได้เปิดใช้งาน S3 (พัก/สแตนด์บาย)
- รหัสผ่าน Self-Encrypting Drive ของผู้ใช้แยกต่างหากจากรหัสผ่านของ Windows เมื่อมีการเปลี่ยนหรือรีเซ็ตรหัสผ่าน Windows ของผู้ใช้ จะไม่มีผลต่อรหัสผ่านไดรฟ์ของผู้ใช้ เว้นแต่มีการเปิดใช้งานการซิงโครไนซ์รหัสผ่าน Windows โปรดดู อุปกรณ์: Self-Encrypting Drives สำหรับรายละเอียด
- บางแป้นพิมพ์ที่ไม่ใช่ภาษาอังกฤษ มีอักขระจำกัดบางชุดที่ไม่สามารถนำมาใช้ในรหัสผ่านของ self-encrypting drive หากรหัสผ่าน Windows ประกอบด้วยอักขระจำกัดใดๆ เหล่านั้น และมีการเปิดใช้งานการซิงโครไนซ์รหัสผ่าน Windows การซิงโครไนซ์จะล้มเหลวและส่งผลแจ้งข้อความแสดงข้อผิดพลาด

ปลดล็อคไดรฟ์

การปลดล็อคไดรฟ์ช่วยให้ผู้ใช้ไดรฟ์ที่ลงทะเบียนไว้สามารถปลดล็อค ไดรฟ์ที่ถูกล็อค หากการล็อคไดรฟ์ถูกเปิดใช้งาน ไดรฟ์จะเข้าสู่สถานะล็อคเมื่อใดก็ตามที่ปิดคอมพิวเตอร์ เมื่อเปิดระบบขึ้นอีกครั้ง คุณต้องผ่านการรับรองกับไดรฟ์โดยการป้อนรหัสผ่านของคุณในหน้าจอการรับรอง pre-Windows

หมายเหตุ:

- การเข้าสู่โหมดประหยัดพลังงาน (เช่น พัก/สแตนด์บายหรือไฮเบอร์เนต) อาจประสบปัญหาไม่สามารถทำได้หากมีบัญชีผู้ใช้ไดรฟ์ self-encrypting drive หลายคนทำงานพร้อมกันบนคอมพิวเตอร์
- ที่หน้าจอการรับรอง pre-Windows, "User 1", "User 2", ฯลฯ ถูกใช้แทนชื่อผู้ใช้ไดรฟ์ในเวอร์ชันของโปรแกรมที่ได้รับการแปลเป็นภาษาต่อไปนี้: จีน ญี่ปุ่น เกาหลี และรัสเซีย

ตัวเลือกขั้นสูง

ตัวเลือกขั้นสูงใน **Dell Data Protection | Access** ช่วยให้ผู้ใช้ที่มีสิทธิ์ระดับผู้ดูแลสามารถจัดการการใช้งานต่อไปนี้:

การดูแลรักษา
รหัสผ่าน
อุปกรณ์

หมายเหตุ: เฉพาะผู้ใช้ที่มีสิทธิ์ระดับผู้ดูแลเท่านั้นที่สามารถดำเนินการแก้ไขในตัวเลือกขั้นสูง ผู้ใช้ทั่วไปสามารถดูการตั้งค่าเหล่านี้ได้แต่ไม่สามารถเปลี่ยนแปลงใดๆ

ภาพรวมการดูแลรักษา

ผู้ดูแลสามารถใช้หน้าต่างการดูแลรักษาเพื่อตั้งค่าการกำหนดลักษณะการเข้าสู่ระบบ Windows, รีเซ็ตระบบเพื่อเตรียมสำหรับใช้ในจุดประสงค์อื่น หรือเพื่อเก็บถาวรหรือเรียกคืนใบรับรองผู้ใช้ที่จัดเก็บอยู่ในฮาร์ดแวร์รักษาความปลอดภัยของระบบ โปรดดูหัวข้อต่อไปนี้สำหรับรายละเอียด:

กำหนดลักษณะการเข้าถึง
รีเซ็ตระบบ
การเก็บถาวร & เรียกคืนใบรับรอง

กำหนดลักษณะการเข้าถึง

กำหนดลักษณะการเข้าถึงช่วยให้ผู้ดูแลสามารถระบุการกำหนดลักษณะเข้าสู่ระบบ Windows สำหรับผู้ใช้ทั้งหมดในระบบ

เปิดใช้งานการเข้าสู่ระบบที่ปลอดภัยของ Dell
ตัวเลือกที่ใช้แทนหน้าจอ ctrl-alt-delete มาตรฐานของ Windows นี้ช่วยให้คุณสามารถใช้องค์ประกอบการรับรองที่แตกต่างไปแทนที่ (หรือเพิ่มเติม) รหัสผ่าน Windows ที่ใช้สำหรับเข้าถึง Windows คุณสามารถเลือกที่จะเพิ่มลายนิ้วมือเป็นองค์ประกอบที่สองของการรับรองเพื่อให้การรักษาความปลอดภัยของขั้นตอนการเข้าสู่ระบบ Windows เข้มแข็งยิ่งขึ้น นอกจากนี้ยังสามารถเพิ่มองค์ประกอบการรับรองเพิ่มเติมสำหรับการเข้าสู่ระบบ Windows รวมถึง smartcard หรือใบรับรอง TPM

หมายเหตุ:
- การเปิดใช้งานการเข้าสู่ระบบที่ปลอดภัยของ Dell มีผลกับผู้ใช้ทุกคนในระบบ
- ขอแนะนำให้เปิดใช้งานตัวเลือกนี้หลังจาก ผู้ใช้ลงทะเบียนลายนิ้วมือหรือ smartcard แล้ว
- ครั้งแรกที่คุณเข้าสู่ระบบหลังจากตั้งตัวเลือกนี้ คุณจะได้รับแจ้งให้รับรองกับ Windows ตามรูปแบบนโยบายมาตรฐานของคุณ หลังจากนั้นคุณจะต้องใช้องค์ประกอบการรับรองใหม่ของคุณในครั้งถัดไปที่เริ่มต้นระบบ

ปิดใช้งานการเข้าสู่ระบบที่ปลอดภัยของ Dell
ตัวเลือกนี้จะยกเลิกใช้งานฟังก์ชัน **Dell Data Protection | Access** ทั้งหมดสำหรับการเข้าสู่ระบบ Windows เมื่อเลือกตัวเลือกนี้ คุณจะกลับไปใช้นโยบายเข้าสู่ระบบแบบมาตรฐานของ Windows

หมายเหตุ:
- หากคุณได้รับข้อผิดพลาดเกี่ยวกับการเข้าสู่ระบบ Windows ที่ปลอดภัยเมื่อคุณพยายามเข้าสู่ระบบ ให้ปิดแล้วเปิดใช้งานตัวเลือกการเข้าสู่ระบบที่ปลอดภัยของ Dell อีกครั้ง
- หากคุณต้องการข้อมูลโดยละเอียดเกี่ยวกับข้อความแสดงข้อผิดพลาดที่เจาะจง ไปที่ wave.com/support/Dell

รีเซ็ตระบบ

ฟังก์ชันรีเซ็ตระบบใช้เพื่อล้างข้อมูลผู้ใช้ทั้งหมดจากฮาร์ดแวร์รักษาความปลอดภัยบนแพลตฟอร์ม ตัวอย่างเช่น ใช้เพื่อเตรียมคอมพิวเตอร์สำหรับใช้ในจุดประสงค์อื่น ตัวเลือกนี้จะล้างรหัสผ่านทั้งหมดในระบบ ยกเว้นรหัสผ่านผู้ใช้ Windows รวมถึงข้อมูลทั้งหมดในอุปกรณ์ฮาร์ดแวร์ (เช่น ControlVault, TPM และตัวอ่านลายนิ้วมือ) สำหรับ self-encrypting drives ฟังก์ชันนี้ยังยกเลิกใช้งานการป้องกันข้อมูลด้วย ดังนั้นข้อมูลไดรฟ์จะสามารถเข้าถึงได้

คุณต้องยืนยันว่าคุณเข้าใจว่าคุณกำลังจะรีเซ็ตระบบ จากนั้นคลิก **ถัดไป** ในการรีเซ็ตระบบ คุณจะต้องป้อนรหัสผ่านสำหรับอุปกรณ์รักษาความปลอดภัยแต่ละชิ้น หากมีการตั้งไว้:

- เจ้าของ TPM
- ผู้ดูแล ControlVault
- ผู้ดูแล BIOS
- ระบบ BIOS (pre-Windows)
- ฮาร์ดไดรฟ์ (BIOS)
- ผู้ดูแล Self-Encrypting Drive

หมายเหตุ: สำหรับ self-encrypting drives ต้องใช้เฉพาะรหัสผ่านผู้ดูแลไดรฟ์เท่านั้น ไม่ต้องใช้รหัสผ่านของผู้ใช้ทุกคน

สิ่งสำคัญ! หนทางเดียวในการกู้คืนข้อมูลใดๆ ที่ล้างไปแล้วเมื่อคุณรีเซ็ตระบบคือการเรียกคืนจากที่เก็บถาวรที่บันทึกไว้ก่อนหน้านี้ หากคุณไม่มีที่เก็บถาวร ข้อมูลนี้จะไม่สามารถกู้คืนได้ สำหรับ self-encrypting drive เฉพาะข้อมูลการตั้งค่าเท่านั้นที่ถูกลบ ข้อมูลส่วนตัวบนไดรฟ์ไม่ได้ถูกลบ

การเก็บถาวรและเรียกคืนใบรับรอง

The การทำงานเก็บถาวรและเรียกคืนใบรับรองใช้เพื่อสำรองและเรียกคืนใบรับรองผู้ใช้ทั้งหมด (ข้อมูลการเข้าสู่ระบบและการเข้ารหัส) ที่จัดเก็บใน ControlVault และ Trusted Platform Module (TPM) การสำรองข้อมูลนี้เป็นสิ่งสำคัญเมื่อทำการจัดเตรียมคอมพิวเตอร์อีกครั้งหรือเพื่อเรียกคืนข้อมูลในกรณีที่ฮาร์ดแวร์ล้มเหลว ในกรณีนี้ คุณสามารถเพียงแค่เรียกคืนใบรับรองทั้งหมดของคุณจากไฟล์เก็บถาวรที่บันทึกไว้ไปไว้ในคอมพิวเตอร์เครื่องใหม่

คุณสามารถเลือกที่จะเก็บถาวรหรือเรียกคืนใบรับรองสำหรับผู้ใช้รายเดียวหรือผู้ใช้ทั้งหมดในระบบ

ใบรับรองผู้ใช้ประกอบด้วยข้อมูลที่ใช้ใน pre-Windows เช่น ลายนิ้วมือและข้อมูล smartcard ที่ลงทะเบียนไว้ และคีย์ที่จัดเก็บใน TPM ทั้งนี้ TPM จะสร้างคีย์ตามคำขอจากโปรแกรมประยุกต์ที่ปลอดภัย โดยการสร้างใบรับรองดิจิทัลจะสร้างคีย์ใน TPM

หมายเหตุ: ในการพิจารณาว่าคีย์ TPM สามารถถูกเก็บถาวรโดย **Dell Data Protection | Access** หรือไม่ โปรดดูเอกสารประกอบสำหรับโปรแกรมประยุกต์ที่ปลอดภัย โดยทั่วไป โปรแกรมประยุกต์ที่ใช้ "Wave TCG-Enabled CSP" เพื่อสร้างคีย์จะได้รับการสนับสนุน

การเก็บถาวรใบรับรอง
หากต้องการเก็บถาวรใบรับรอง คุณต้องดำเนินการต่อไปนี้:

- ระบุว่าคุณกำลังจะเก็บถาวรใบรับรองสำหรับตัวเองหรือผู้ใช้ทั้งหมดในระบบ
- แจ้งข้อมูลการรับรองให้กับฮาร์ดแวร์ที่ปลอดภัยโดยป้อนรหัสผ่านระบบ (pre-Windows), รหัสผ่านผู้ดูแล ControlVault และรหัสผ่านเจ้าของ TPM
- สร้างรหัสผ่านการสำรองข้อมูลใบรับรอง
- ระบุที่ตั้งที่เก็บถาวร โดยใช้ปุ่ม **Browse** ที่ตั้งที่เก็บถาวรควรเป็นสื่อที่ถอดได้ เช่น แฟลชไดรฟ์ USB หรือไดรฟ์เครือข่าย เพื่อป้องกันปัญหาฮาร์ดแวร์ล้มเหลว

หมายเหตุสำคัญ:
- จดบันทึกที่ตั้งที่เก็บถาวรนี้เพราะผู้ใช้จะต้องใช้ข้อมูลนี้เพื่อเรียกคืนข้อมูลใบรับรอง
- จดบันทึกรหัสผ่านการสำรองข้อมูลใบรับรองเพื่อให้แน่ใจว่าสามารถเรียกคืนข้อมูลได้ สิ่งนี้สำคัญมากเพราะรหัสผ่านนี้ไม่สามารถกู้คืนได้
- หากคุณไม่รู้รหัสผ่านเจ้าของ TPM โปรดติดต่อผู้ดูแลระบบหรือดูคำแนะนำการตั้งค่า TPM ของคอมพิวเตอร์

การเรียกคืนใบรับรอง
หากต้องการเรียกคืนใบรับรอง คุณต้องดำเนินการต่อไปนี้:

- ระบุว่าคุณกำลังจะเรียกคืนใบรับรองสำหรับตัวเองหรือผู้ใช้ทั้งหมดในระบบ
- เรียกดูที่ตั้งที่เก็บถาวร และเลือกไฟล์เก็บถาวร
- ป้อนรหัสผ่านการสำรองข้อมูลใบรับรองที่สร้างไว้เมื่อคุณตั้งค่าที่เก็บถาวร
- แจ้งข้อมูลการรับรองให้กับฮาร์ดแวร์ที่ปลอดภัยโดยป้อนรหัสผ่านระบบ (pre-Windows), รหัสผ่านผู้ดูแล ControlVault และรหัสผ่านเจ้าของ TPM

หมายเหตุ:
- หากคุณได้รับแจ้งข้อผิดพลาดว่าการเรียกคืนใบรับรองล้มเหลวและคุณลองทำการเรียกคืนหลายครั้งแล้ว ให้ลองเรียกคืนจากไฟล์เก็บถาวรไฟล์อื่น หากไม่เป็นผลสำเร็จ ให้สร้างที่เก็บถาวรใบรับรองที่อื่นและพยายามเรียกคืนจากที่เก็บถาวรที่ใหม่
- หากคุณได้รับแจ้งข้อผิดพลาดว่าคีย์ TPM ไม่สามารถเรียกคืนได้ ให้สร้างที่เก็บถาวรใบรับรอง จากนั้นลบ TPM นั้น ใน BIOS ในการลบ TPM ให้เริ่มต้นคอมพิวเตอร์ใหม่ กดปุ่ม **F2** เมื่อระบบเริ่มอีกครั้งเพื่อเข้าถึงการตั้งค่า BIOS จากนั้นเลื่อนไปที่ ความปลอดภัย > ความปลอดภัย TPM แล้วสร้างการเป็นเจ้าของ TPM อีกครั้งและพยายามเรียกคืนใบรับรองอีกครั้ง
- หากคุณต้องการข้อมูลโดยละเอียดเกี่ยวกับข้อความแสดงข้อผิดพลาดที่เจาะจง ไปที่ wave.com/support/Dell

การจัดการรหัสผ่าน

จากหน้าต่าง การจัดการรหัสผ่าน ผู้ดูแลสามารถสร้างหรือเปลี่ยนแปลงรหัสผ่านการรักษาความปลอดภัยทั้งหมดบนระบบของคุณ:

- ระบบ (หรือที่เรียกว่า Pre-Windows)*
- ผู้ดูแล*
- ฮาร์ดไดรฟ์*
- ControlVault
- เจ้าของ TPM
- TPM หลัก
- ห้องนิรภัยรหัสผ่าน TPM
- Self-Encrypting Drive

หมายเหตุ:

- เฉพาะรหัสผ่านที่มีการใช้กับโครงแบบแพลตฟอร์มปัจจุบันเท่านั้นที่จะแสดงให้เห็น ดังนั้นหน้าต่างนี้จะเปลี่ยนแปลงตามโครงแบบและสถานะของระบบ
- รหัสผ่านที่มีเครื่องหมาย * ถัดอยู่ข้างต้นคือรหัสผ่าน BIOS และสามารถเปลี่ยนแปลงได้ทาง BIOS ระบบ
- รหัสผ่านระดับ BIOS ไม่สามารถสร้างหรือเปลี่ยนแปลงได้หากผู้ดูแล BIOS ไม่กำหนดให้เปลี่ยนแปลงรหัสผ่านได้
- การคลิกลิงก์ **ตั้งค่า** สำหรับ self-encrypting drive จะเรียกใช้งานตัวช่วยสร้างการตั้งค่า Self-Encrypting Drive ส่วนการคลิก **จัดการ** ช่วยให้ผู้ใช้สามารถเปลี่ยนรหัสผ่าน Self-Encrypting Drive หนึ่งหรือหลายรหัสได้
- การคลิกลิงก์ **จัดการ** สำหรับห้องนิรภัยรหัสผ่าน TPM จะแสดงหน้าต่างที่คุณสามารถดูหรือเปลี่ยนรหัสผ่านที่ป้องกันคีย์ TPM ของคุณ เมื่อคีย์ TPM ที่ต้องมีรหัสผ่านถูกสร้างขึ้น รหัสผ่านจะได้รับการสร้างแบบสุ่มและเก็บไว้ในห้องนิรภัย คุณไม่สามารถจัดการห้องนิรภัยรหัสผ่าน TPM จนกว่าคุณจะสร้างรหัสผ่าน TPM หลัก

กฎความซับซ้อนในรหัสผ่านของ Windows

Dell Data Protection | Access ช่วยให้มั่นใจได้ว่ารหัสผ่านต่อไปนี้จะเป็นไปตามกฎความซับซ้อนในรหัสผ่านของ Windows สำหรับเครื่องนั้นๆ:

- รหัสผ่านเจ้าของ TPM

เพื่อกำหนดนโยบายความซับซ้อนในรหัสผ่านของ Windows สำหรับเครื่อง ให้ทำตามขั้นตอนเหล่านี้:

1. เข้าไปที่ Control Panel
2. ดับเบิลคลิกที่ Administrative Tools
3. ดับเบิลคลิกที่ Local Security Policy
4. ขยาย Account Policies และเลือก Password Policy

ภาพรวมอุปกรณ

หน้าต่างอุปกรณ์ใช้สำหรับ ผู้ดูแลในการจัดการอุปกรณ์รักษาความปลอดภัยทั้งหมดที่ติดตั้งบนระบบ สำหรับแต่ละอุปกรณ์ คุณสามารถดูสถานะและข้อมูลเพิ่มเติมโดยละเอียด เช่น เวอร์ชันของเฟิร์มแวร์ คลิก **แสดง** เพื่อดูข้อมูลแต่ละอุปกรณ์ หรือ **ซ่อน** เพื่อยุบข้อมูลส่วนนั้น อุปกรณ์ที่สามารถจัดการได้มีดังนี้ ทั้งนี้ขึ้นอยู่กับว่าแพลตฟอร์มของคุณมีสิ่งใดรวมอยู่:

Trusted Platform Module (TPM)
ControlVault®
Self-Encrypting Drive(s)
ข้อมูลอุปกรณ์การรับรอง

Trusted Platform Module (TPM)

ชิปความปลอดภัย TPM ต้องถูกเปิดใช้งานและต้องสร้างการเป็นเจ้าของ TPM เพื่อให้สามารถใช้คุณสมบัติการรักษาความปลอดภัยขั้นสูงที่มีอยู่ใน **Dell Data Protection | Access** และ TPM

หน้าต่าง Trusted Platform Module ใน **การจัดการอุปกรณ์** จะแสดงต่อเมื่อตรวจพบ TPM ในระบบของคุณ

การจัดการ TPM
ฟังก์ชันเหล่านี้ช่วยให้ผู้ดูแลระบบสามารถจัดการ TPM

สถานะ
แสดงสถานะ *ทำงาน* หรือ *ไม่ทำงาน* สำหรับ TPM สถานะ "ทำงาน" หมายความว่ามีการเปิดใช้งาน TPM ใน BIOS และพร้อมสำหรับการตั้งค่า (เช่น สามารถแสดงความเป็นเจ้าของได้) หาก TPM ไม่ทำงาน (ถูกเปิดใช้งาน) จะไม่สามารถจัดการ TPM และไม่สามารถเข้าถึงคุณสมบัติการรักษาความปลอดภัยได้

หากตรวจพบ TPM บนระบบแต่ไม่ได้ทำงาน (ถูกเปิดใช้งาน) คุณสามารถเปิดใช้งานโดยคลิกลิงก์ **ทำงาน** ที่หน้าต่างนี้ โดยไม่ต้องเข้าสู่ BIOS ระบบ หลังจากเปิดใช้งาน TPM โดยใช้คุณสมบัตินี้ จะต้องเริ่มต้นคอมพิวเตอร์ใหม่ ระหว่างเริ่มต้นใหม่ ข้อความแจ้งจะปรากฏขึ้นในบางกรณี โดยการขอให้คุณยอมรับการเปลี่ยนแปลง

หมายเหตุ: ความสามารถในการเปิดใช้งาน (ทำงาน) TPM จากโปรแกรมประยุกต์นี้อาจไม่ได้รับการสนับสนุนในบางแพลตฟอร์ม หากไม่สนับสนุน คุณต้องเปิดใช้งานใน BIOS ระบบ โดยการเริ่มต้นระบบใหม่ กดปุ่ม **F2** ก่อนโหลด Windows เพื่อเข้าสู่การตั้งค่า BIOS จากนั้นไปที่ ความปลอดภัย >TPM ความปลอดภัย และเรียกทำงาน TPM

คุณยังสามารถ *ยกเลิกทำงาน* TPM ได้จากที่นี่โดยคลิกลิงก์ **ยกเลิกทำงาน** การยกเลิกทำงาน TPM จะทำให้ไม่สามารถใช้งานได้ในคุณสมบัติการรักษาความปลอดภัยขั้นสูง อย่างไรก็ตาม การยกเลิกทำงานนี้ไม่ได้เปลี่ยนแปลงการตั้งค่าใดๆ ของ TPM หรือลบหรือเปลี่ยนแปลงข้อมูลหรือคีย์ใดๆ ที่จัดเก็บอยู่ใน TPM

เป็นเจ้าของแล้ว
แสดงสถานะ ความเป็นเจ้าของ (เช่น "เป็นเจ้าของแล้ว") และให้คุณสร้างหรือเปลี่ยนแปลงเจ้าของ TPM โดยคุณต้องสร้างการเป็นเจ้าของ TPM เพื่อให้คุณสมบัติการรักษาความปลอดภัยสามารถใช้ได้ ก่อนสร้างการเป็นเจ้าของ TPM ต้องถูกเปิดใช้งาน (ทำงาน)

ขั้นตอนการสร้างการเป็นเจ้าของประกอบด้วยผู้ใช้ (ที่มีสิทธิ์ระดับผู้ดูแล) สร้างรหัสผ่านเจ้าของ TPM เมื่อระบุรหัสผ่านนี้แล้ว ความเป็นเจ้าของจะถูกสร้างขึ้นและ TPM ก็พร้อมสำหรับใช้งาน

หมายเหตุ: รหัสผ่านเจ้าของ TPM ต้องสอดคล้องตาม กฎความซับซ้อนในรหัสผ่านของ Windows สำหรับระบบของคุณ

สิ่งสำคัญ! เป็นสิ่งสำคัญที่คุณต้องไม่ลืมหรือทำรหัสผ่านเจ้าของ TPM สูญหาย เพราะเป็นสิ่งจำเป็นสำหรับการเข้าถึงฟังก์ชันการรักษาความปลอดภัยขั้นสูงของ TPM ใน **Dell Data Protection | Access**

ถูกล็อค
แสดงสถานะ*ถูกล็อค* หรือ *ปลดล็อคแล้ว* สำหรับ TPM "การล็อค" คือคุณสมบัติด้านความปลอดภัยของ TPM โดย TPM จะเข้าสู่สถานะถูกล็อคหลังจากมีการป้อนรหัสผ่านเจ้าของ TPM ไม่ถูกต้องครบตามจำนวนที่ระบุ เจ้าของ TPM สามารถปลดล็อค TPM ได้จากที่นี่ โดยจำเป็นต้องป้อนรหัสผ่านเจ้าของ TPM

หมายเหตุ:

- หากคุณได้รับข้อผิดพลาดที่ระบุว่าความเป็นเจ้าของ TPM ไม่สามารถสร้างได้ ให้ลบ TPM ใน BIOS ระบบ และพยายามสร้างความเป็นเจ้าของอีกครั้ง ให้เริ่มต้นคอมพิวเตอร์ใหม่ กดปุ่ม **F2** เมื่อระบบเริ่มอีกครั้งเพื่อเข้าถึงการตั้งค่า BIOS จากนั้นเลื่อนไปที่ ความปลอดภัย >ความปลอดภัย TPM
- หากคุณได้รับข้อผิดพลาดที่ระบุว่ารหัสผ่านเจ้าของ TPM ไม่สามารถเปลี่ยนได้ ให้เก็บถาวรข้อมูล TPM (เก็บถาวรใบรับรอง) ลบ TPM ใน BIOS, สร้างความเป็นเจ้าของ TPM อีกครั้ง และเรียกคืนข้อมูล TPM (เรียกคืนใบรับรอง)
- หากคุณต้องการข้อมูลโดยละเอียดเกี่ยวกับข้อความแสดงข้อผิดพลาดที่เจาะจง ไปที่ wave.com/support/Dell

Dell ControlVault®

Dell ControlVault® (CV) คือที่จัดเก็บฮาร์ดแวร์ที่ปลอดภัยสำหรับใบรับรองผู้ใช้ที่ใช้ระหว่างการเข้าสู่ระบบ pre-Windows (เช่น รหัสผ่านผู้ใช้หรือข้อมูลลายนิ้วมือที่ลงทะเบียนไว้) หน้าต่าง ControlVault ใน **การจัดการอุปกรณ์** จะแสดงต่อเมื่อตรวจพบ ControlVault ในระบบของคุณ

การจัดการ ControlVault
ฟังก์ชันเหล่านี้ช่วยให้ผู้ดูแลระบบสามารถจัดการ ControlVault ของระบบ

สถานะ
แสดงสถานะ *ทำงาน* หรือ *ไม่ทำงาน* สำหรับ ControlVault สถานะ "ไม่ทำงาน" หมายความว่าไม่สามารถใช้ ControlVault สำหรับการจัดเก็บในระบบของคุณ โปรดดูเอกสารของระบบ Dell เพื่อดูว่าระบบมี ControlVault หรือไม่

รหัสผ่าน
ระบุว่ามีการตั้งรหัสผ่านผู้ดูแล ControlVault หรือไม่ และให้คุณตั้งหรือเปลี่ยนรหัสผ่านดังกล่าวได้ (หากมีการตั้งไว้แล้ว) เฉพาะผู้ดูแลระบบเท่านั้นที่สามารถตั้งหรือเปลี่ยนรหัสผ่านนี้ โดยต้องตั้งรหัสผ่านผู้ดูแล ControlVault เพื่อให้สามารถดำเนินการต่อไปนี้:

- ดำเนินการเก็บถาวรหรือเรียกคืนใบรับรอง
- ล้างข้อมูลผู้ใช้ (สำหรับผู้ใช้ทั้งหมด)

หมายเหตุ: หากมีการพยายามเก็บถาวรหรือเรียกคืนเมื่อยังไม่ได้ตั้งรหัสผ่านผู้ดูแล ControlVault ระบบจะแจ้งให้สร้างรหัสผ่าน (หากผู้ใช้เป็นผู้ดูแล)

ผู้ใช้ที่ลงทะเบียน
ระบุว่ามีผู้ใช้คนใดลงทะเบียนใบรับรองการเข้าสู่ระบบ (เช่น รหัสผ่าน ลายนิ้วมือ หรือข้อมูล smartcard) ที่ปัจจุบันจัดเก็บอยู่ใน ControlVault

ลบข้อมูลผู้ใช้
ในบางครั้งอาจจำเป็นต้องล้างข้อมูลใน ControlVault เช่นในกรณีที่ผู้ใช้ประสบปัญหาในการใช้หรือลงทะเบียนใบรับรอง pre-Windows เพื่อรับการรับรอง ข้อมูลทั้งหมดที่จัดเก็บใน ControlVault สามารถล้างออกได้จากหน้าต่างนี้ ทั้งสำหรับผู้ใช้รายเดียวหรือทุกราย

ต้องป้อนรหัสผ่านผู้ดูแล ControlVault เพื่อล้างข้อมูลผู้ใช้ทั้งหมดออกจากแพลตฟอร์ม คุณยังจะได้รับแจ้งให้ป้อนรหัสผ่านระบบ (pre-Windows) หากมีการลงทะเบียนใบรับรอง pre-Windows ใดๆ ไว้ เมื่อคุณล้างข้อมูลผู้ใช้ทั้งหมด รหัสผ่านผู้ดูแล ControlVault และรหัสผ่านระบบจะถูกรีเซ็ต โปรดทราบว่านี่คือวิธีเดียวในการล้างรหัสผ่านผู้ดูแล ControlVault

หมายเหตุ: เมื่อคุณล้างข้อมูลผู้ใช้ทั้งหมด คุณจะได้รับแจ้งให้เริ่มต้นคอมพิวเตอร์ใหม่ เป็นสิ่งสำคัญที่คุณจะต้องเริ่มต้นคอมพิวเตอร์ใหม่เพื่อให้ระบบทำงานอย่างเหมาะสม

ไม่จำเป็นต้องตั้งรหัสผ่านผู้ดูแล ControlVault สำหรับการล้างใบรับรองของผู้ใช้รายเดียว เมื่อคุณคลิก **ล้างข้อมูลผู้ใช้** ระบบจะแจ้งให้คุณเลือกผู้ใช้ที่คุณต้องการล้างใบรับรอง ControlVault ของบุคคลนั้น เมื่อคุณเลือกผู้ใช้ ระบบจะแจ้งให้คุณป้อนรหัสผ่านระบบ (หากมีการลงทะเบียนใบรับรอง pre-Windows ไว้เท่านั้น)

หมายเหตุ:
- หากคุณได้รับข้อผิดพลาดระบุว่าไม่สามารถสร้างรหัสผ่านผู้ดูแล ControlVault คุณควรเก็บถาวรใบรับรองของคุณ ล้างข้อมูลผู้ใช้ทั้งหมดออกจาก ControlVault เริ่มต้นคอมพิวเตอร์ใหม่ และพยายามสร้างรหัสผ่านอีกครั้ง
- หากคุณได้รับข้อผิดพลาดระบุว่าไม่สามารถล้างใบรับรองสำหรับผู้ใช้รายเดียวนั้นจาก ControlVault ได้ คุณควรเก็บถาวรใบรับรองของคุณ ลองล้างข้อมูลผู้ใช้ทั้งหมดแล้วจึงพยายามล้างข้อมูลของผู้ใช้รายเดียวนั้นอีกครั้ง
- หากคุณได้รับข้อผิดพลาดระบุว่าไม่สามารถล้างใบรับรองของผู้ใช้ทั้งหมดออกจาก ControlVault คุณควรพิจารณาดำเนินการรีเซ็ตระบบ**สิ่งสำคัญ!** อ่านหัวข้อความช่วยเหลือในการรีเซ็ตระบบก่อนดำเนินการรีเซ็ต เพราะการทำเช่นนี้จะล้างข้อมูลการรักษาความปลอดภัยของผู้ใช้ทั้งหมด

- หากคุณได้รับข้อผิดพลาดระบุว่าไม่สามารถสำรองข้อมูล ControlVault และ TPM ให้ยกเลิกใช้งาน TPM ใน BIOS ระบบ ซึ่งทำได้โดยการเริ่มต้นคอมพิวเตอร์ใหม่ แล้วกดปุ่ม **F2** เมื่อระบบเริ่มต้นอีกครั้งเพื่อเข้าถึงการตั้งค่า BIOS จากนั้นเลื่อนไปที่ ความปลอดภัย > ความปลอดภัย TPM จากนั้นเปิดใช้งาน TPM อีกครั้งและลองเก็บถาวรข้อมูล ControlVault ของคุณอีกครั้ง
- หากคุณต้องการข้อมูลโดยละเอียดเกี่ยวกับข้อความแสดงข้อผิดพลาดที่เจาะจง ไปที่ wave.com/support/Dell

Self-Encrypting Drives: ขั้นสูง

Dell Data Protection | Access จัดการฟังก์ชันการรักษาความปลอดภัยที่ใช้ฮาร์ดแวร์ของ self-encrypting drives ซึ่งมีการเข้ารหัสข้อมูลที่ฝังอยู่ในฮาร์ดแวร์ของไดรฟ์ การจัดการนี้ใช้เพื่อให้ความมั่นใจว่ามีเพียงผู้ใช้ที่ได้รับอนุญาตเท่านั้นที่สามารถเข้าถึงข้อมูลที่เข้ารหัส (เมื่อเปิดใช้งานการล็อคไดรฟ์)

หน้าต่าง Self-Encrypting Drive ใน **การจัดการอุปกรณ์** แสดงขึ้นต่อเมื่อมี self-encrypting drives (SED) หนึ่งตัวขึ้นไปอยู่ในระบบของคุณ

สิ่งสำคัญ! เมื่อตั้งค่าไดรฟ์แล้ว การป้องกันข้อมูลและการล็อคไดรฟ์ จะถูก "เปิดใช้งาน"

การจัดการไดรฟ์
ฟังก์ชันเหล่านี้ช่วยให้ผู้ดูแลไดรฟ์ สามารถจัดการการตั้งค่าความปลอดภัยของไดรฟ์ การเปลี่ยนแปลงในการตั้งค่าความปลอดภัยของไดรฟ์จะมีผลหลังจากปิดการจ่ายไฟเข้าไดรฟ์

การป้องกันข้อมูล
แสดงสถานะ *เปิดใช้งาน* หรือ *ยกเลิกใช้งาน* สำหรับการป้องกันข้อมูล self-encrypting drive สถานะ "เปิดใช้งาน" หมายความว่ามีการตั้งค่าความปลอดภัยของไดรฟ์ อย่างไรก็ตาม ผู้ใช้จะไม่ต้องผ่านการรับรองกับไดรฟ์สำหรับการเข้าถึงเมื่ออยู่ที่ pre-Windows จนกว่าจะมีการเปิด*การล็อค*ไดรฟ์

คุณสามารถยกเลิกใช้งานการป้องกันข้อมูล self-encrypting drive ได้จากที่นี่ เมื่อยกเลิกใช้งาน ฟังก์ชันความปลอดภัยขั้นสูงทั้งหมดของ self-encrypting drive จะถูกปิดและไดรฟ์ทำงานเป็นไดรฟ์แบบมาตรฐาน การยกเลิกใช้งานการป้องกันข้อมูลจะลบการตั้งค่าความปลอดภัยทั้งหมดด้วย รวมถึงใบรับรองของผู้ดูแลไดรฟ์และผู้ใช้ไดรฟ์ อย่างไรก็ตาม ฟังก์ชันนี้ไม่สามารถเปลี่ยนแปลงหรือลบข้อมูลผู้ใช้คนใดในไดรฟ์

การล็อค
แสดงสถานะ *เปิดใช้งาน* หรือ *ยกเลิกใช้งาน* สำหรับ self-encrypting drive โปรดดูหัวข้อ Self-Encrypting Drive สำหรับข้อมูลเกี่ยวกับลักษณะการทำงานของไดรฟ์ที่ถูกล็อค

การยกเลิกใช้งานการล็อคไดรฟ์ไว้ชั่วคราวอาจเป็นสิ่งจำเป็น ซึ่งคุณสามารถทำได้จากที่นี่ แต่ไม่แนะนำให้ทำเพราะจะทำให้ไม่ต้องใช้ใบรับรองในการเข้าถึงไดรฟ์เมื่อการล็อคไดรฟ์ถูกยกเลิกใช้งาน ดังนั้นผู้ใช้แพลตฟอร์มทุกคนจะสามารถเข้าถึงข้อมูลไดรฟ์ได้ การยกเลิกใช้งานการล็อคไดรฟ์ไม่ได้ลบการตั้งค่าความปลอดภัยใดๆ รวมถึงใบรับรองของผู้ดูแลไดรฟ์และผู้ใช้ไดรฟ์หรือข้อมูลผู้ใช้ใดๆ บนไดรฟ์

ข้อควรระวัง! หากคุณถอนการติดตั้งโปรแกรมประยุกต์ **Dell Data Protection | Access** ก่อนอื่นคุณต้องยกเลิกใช้งานการป้องกันข้อมูลของ self-encrypting drive และปลดล็อคไดรฟ์

ผู้ดูแลไดรฟ์
แสดงผู้ดูแลไดรฟ์ปัจจุบัน ผู้ดูแลไดรฟ์สามารถเปลี่ยนผู้ใช้ที่จะมาเป็นผู้ดูแลไดรฟ์ได้จากที่นี่ ผู้ดูแลคนใหม่ต้องเป็นผู้ใช้ Windows ที่ถูกต้องในระบบที่มีสิทธิ์ระดับผู้ดูแลระบบ ระบบสามารถมีผู้ดูแลไดรฟ์ได้เพียงหนึ่งชื่อเท่านั้น

ผู้ใช้ไดรฟ์
แสดงผู้ใช้ไดรฟ์ที่ลงทะเบียนไว้ และจำนวนผู้ใช้ปัจจุบันที่ลงทะเบียนไว้ จำนวนผู้ใช้สูงสุดที่สนับสนุนขึ้นอยู่กับ self-encrypting drive (ปัจจุบัน ผู้ใช้ 4 คนสำหรับไดรฟ์ Seagate และ 24 คนสำหรับไดรฟ์ Samsung)

การซิงค์รหัสผ่าน Window
คุณสมบัติการซิงโครไนซ์รหัสผ่าน Windows (WPS) กำหนดรหัสผ่าน Self-Encrypting Drive ของผู้ใช้ให้เหมือนกับรหัสผ่าน Windows โดยอัตโนมัติ ฟังก์ชันนี้ไม่ได้บังคับใช้กับผู้ดูแลไดรฟ์ มีผลกับผู้ใช้ไดรฟ์เท่านั้น การทำงานของ WPS สามารถนำไปใช้ในสภาพแวดล้อมระดับองค์กร ซึ่งต้องมีการเปลี่ยนรหัสผ่านเมื่อครบช่วงเวลาที่ระบุ (เช่น ทุกๆ 90

วัน) เมื่อเปิดใช้งานตัวเลือกนี้ รหัสผ่าน self-encrypting ของผู้ใช้ทั้งหมดจะได้รับการอัพเดตโดยอัตโนมัติเมื่อรหัสผ่าน Windows เหล่านี้ถูกเปลี่ยน

หมายเหตุ: เมื่อเปิดใช้งานการซิงโครไนซ์รหัสผ่าน Windows (WPS) จะไม่สามารถเปลี่ยนรหัสผ่าน Self-Encrypting Drive ของผู้ใช้ได้ โดยต้องเปลี่ยนรหัสผ่าน Windows เพื่อให้อัพเดตรหัสผ่านของไดรฟ์โดยอัตโนมัติ

จดจำชื่อผู้ใช้ล่าสุด
เมื่อเปิดใช้งานตัวเลือกนี้ ชื่อผู้ใช้ล่าสุดที่ป้อนจะแสดงขึ้นเป็นค่าเริ่มต้นในฟิลด์ **ชื่อผู้ใช้** ของหน้าจอการรับรอง pre-Windows

การเลือกชื่อผู้ใช้
เมื่อเปิดใช้งานตัวเลือกนี้ ผู้ใช้สามารถดูชื่อผู้ใช้ไดรฟ์ทั้งหมดในฟิลด์ **ชื่อผู้ใช้** ของหน้าจอการรับรอง pre-Windows

ลบการเข้ารหัส
ตัวเลือกนี้สามารถใช้เพื่อ "ลบ" ข้อมูลทั้งหมดใน self-encrypting drive ซึ่งที่จริงแล้วไม่ใช่การลบข้อมูล แต่เป็นการลบคีย์ที่ใช้เข้ารหัสข้อมูลนั้น จึงทำให้ข้อมูลนั้นไม่สามารถใช้ได้ ไม่มีทางใดที่จะกู้คืนข้อมูลไดรฟ์ได้หลังจากลบการเข้ารหัส นอกจากนี้ การป้องกันข้อมูล self-encrypting drive จะถูกยกเลิกใช้งานและไดรฟ์จะพร้อมสำหรับจุดประสงค์ใหม่

หมายเหตุ:

- หากคุณได้รับข้อผิดพลาดใดๆ เกี่ยวกับฟังก์ชันการจัดการ self-encrypting drive ให้ทำการปิดเครื่องคอมพิวเตอร์อย่างสมบูรณ์ (ไม่ใช่เริ่มระบบใหม่) แล้วรีสตาร์ท
- หากคุณต้องการข้อมูลโดยละเอียดเกี่ยวกับข้อความแสดงข้อผิดพลาดที่เจาะจง ไปที่ wave.com/support/Dell

ข้อมูลอุปกรณ์การรับรอง

หน้าต่างข้อมูลอุปกรณ์การรับรองใน **การจัดการอุปกรณ์** แสดงข้อมูลและสถานะของอุปกรณ์การรับรองทั้งหมดที่เชื่อมต่ออยู่ (เช่น ตัวอ่านลายนิ้วมือ ตัวอ่าน smartcard ทั่วไปหรือ contactless smartcard) บนระบบ

การสนับสนุนทางเทคนิค

การสนับสนุนทางเทคนิคสำหรับซอฟต์แวร์ **Dell Data Protection | Access** สามารถดูได้ที่ support.dell.com

Wave TCG-Enabled CSP

Wave Systems Trusted Computing Group (TCG)-enabled Cryptographic Service Provider (CSP) มีโปรแกรมประยุกต์ **Dell Data Protection | Access** รวมอยู่ และพร้อมสำหรับใช้ได้ทุกเมื่อที่จำเป็นต้องใช้ CSP ทั้งโดยการเรียกใช้โดยตรงจากโปรแกรมประยุกต์หรือสามารถเลือกได้จากรายการ CSP ที่ติดตั้งไว้ เมื่อทำได้ ให้เลือก "Wave TCG-Enabled CSP" เพื่อให้มั่นใจว่า TPM สร้างคีย์ และคีย์และรหัสผ่านของคีย์นั้นได้รับการจัดการโด **Dell Data Protection | Access**

Wave Systems TCG-enabled CSP ช่วยให้โปรแกรมประยุกต์สามารถใช้ฟังก์ชันที่มีอยู่บนแพล็ตฟอร์มที่สอดคล้องกับ TCG ได้โดยตรงผ่านทาง MSCAPI โมดูล TCG-enhanced MSCAPI CSP นี้เองที่ให้การทำงานแบบอะซิมเมตริกของคีย์บน TPM และใช้ประโยชน์จากระบบความปลอดภัยที่เพิ่มประสิทธิภาพที่ TPM มีให้ โดยไม่คำนึงถึงข้อกำหนดเจาะจงของผู้ค้าในส่วนที่เกี่ยวกับผู้ให้บริการ Trusted Software Stack (TSS)

หมายเหตุ: หากคีย์ TPM ที่สร้างโดย Wave TCG-enabled CSP ต้องการรหัสผ่าน และผู้ใช้ได้สร้างรหัสผ่านหลัก TPM รหัสผ่านของคีย์แต่ละตัวจะถูกสร้างแบบสุ่มและจัดเก็บไว้ในห้องนิรภัยรหัสผ่าน TPM