HP ProtectTools
คู่มือผู้ใช้

ข้อมูลที่ประกอบในที่นี้สามารถเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบ การรับประกันของผลิตภัณฑ์และบริการของ HP จะปรากฏอยู่ในประกาศการรับประกันอย่างชัดเจนที่จัดส่งให้พร้อมกับผลิตภัณฑ์และบริการดังกล่าวเท่านั้น ข้อความในที่นี้จะไม่มีผลเป็นการรับประกันเพิ่มเติมใดๆ ทั้งสิ้น HP จะไม่รับผิดชอบต่อความผิดพลาดหรือการขาดหายของข้อมูลด้านเทคนิคหรือเนื้อหาของเอกสารนี้

พิมพ์ครั้งที่สอง: ตุลาคม 2007

หมายเลขเอกสาร: 451271-282

สารบัญ

1 บทนำเรื่องการรักษาความปลอดภัย

ซอฟต์แวร์ HP ProtectTools Security Manager มาพร้อมกับคุณสมบัติด้านความปลอดภัยที่ช่วยป้องกันการล็อกอินเข้าใช้คอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสำคัญ ส่วนฟังก์ชันความปลอดภัยเพิ่มเติมมาพร้อมกับโมดูลซอฟต์แวร์ต่างๆ ต่อไปนี้:

- Credential Manager สำหรับ HP ProtectTools
- Embedded Security สำหรับ HP ProtectTools
- Java Card Security สำหรับ HP ProtectTools
- การกำหนดค่า BIOS สำหรับ HP ProtectTools
- การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools
- Device Access Manager สำหรับ HP ProtectTools

โมดูลซอฟต์แวร์สำหรับคอมพิวเตอร์ของคุณอาจแตกต่างกันตามรุ่นที่คุณมี ตัวอย่างเช่น Embedded Security สำหรับ HP ProtectTools มีให้ใช้เฉพาะกับคอมพิวเตอร์ที่ติดตั้งชิปความปลอดภัย Trusted Platform Module (TPM) แบบฝังตัว ลงในคอมพิวเตอร์

คุณอาจเลือกติดตั้งซ้ำ โหลดล่วงหน้าโมดูลซอฟต์แวร์ HP ProtectTools หรือโมดูลซอฟต์แวร์ดังกล่าวอาจมีให้พร้อมดาวน์โหลดจากเว็บไซต์ดังกล่าว สำหรับเดสก์ทอป HP Compaq บางรุ่น HP ProtectTools จะวางจำหน่ายเป็นชุดอุปกรณ์เสริม เยี่ยมชมที่ http://www.hp.com สำหรับข้อมูลเพิ่มเติม

หมายเหตุ: คำแนะนำในคู่มือเล่มนี้เขียนขึ้นภายใต้สมมุติฐานที่ว่า คุณได้ติดตั้งโมดูลซอฟต์แวร์ HP ProtectTools ที่นำมาใช้ได้แล้ว

คุณลักษณะของ HP ProtectTools

ตารางต่อไปนี้อธิบายรายละเอียดคุณลักษณะหลักๆ ของโมดูล HP ProtectTools:

โมดูล	คุณลักษณะหลัก
Credential Manager สำหรับ HP ProtectTools	• Credential Manager ทำหน้าที่ป้องกันรหัสผ่านส่วนบุคคล จัดหาความสามารถในการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) และอนุญาตให้ผู้ใช้กำหนดและปรับใช้ระบบรักษาความปลอดภัยที่เข้มงวดมากกว่าการใช้รหัสผ่านในการตรวจสอบความถูกต้องของผู้ใช้ • ส่วนที่ใช้จัดเก็บรหัสผ่านได้รับการป้องกันผ่านวิธีการเข้ารหัส และเพิ่มประสิทธิภาพได้ด้วยการใช้ชิปความปลอดภัย TPM แบบฝังตัว • นอกเหนือจากการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) แล้ว Credential Manager ยังรองรับการใช้เทคโนโลยีรักษาความปลอดภัยต่างๆ ร่วมกัน เช่น Java™ Card หรือไบโอเมตริกสำหรับการตรวจสอบความถูกต้องของผู้ใช้ควบคู่ไปกับการใช้รหัสผ่าน
Embedded Security สำหรับ HP ProtectTools	• Embedded Security จัดการตัวเลือกความปลอดภัยของผู้ใช้และผู้ดูแลระบบสำหรับการปกป้องคีย์การเข้ารหัสต่างๆ ที่ใช้เทคโนโลยี TPM บนคอมพิวเตอร์โลคัล เช่น EFS (Windows Encrypting File System) Personal Secure Drive (PSD) และใบรับรองดิจิตอลของผู้ผลิตรายอื่น • Embedded Security ใช้ชิปความปลอดภัย Trusted Platform Module (TPM) แบบฝังตัวเพื่อช่วยป้องกันการลักลอบเข้าสู่ข้อมูลที่มีความละเอียดอ่อนของผู้ใช้หรือข้อมูลลับที่จัดเก็บไว้บนคอมพิวเตอร์ TPM จัดเก็บคีย์การเข้ารหัสอย่างปลอดภัย และมีความสามารถในการสร้างคีย์ นอกจากนี้ยังป้องกันการโจมตีรหัสผ่านได้อีกด้วย • Embedded Security ยอมให้สร้างไดรฟ์ความปลอดภัยส่วนบุคคล (PSD) ซึ่งเป็นไดรฟ์เสมือนที่สามารถซ่อนจากมุมมองในระบบ เพื่อป้องกันข้อมูลของผู้ใช้ • Embedded Security สนับสนุนโปรแกรมประยุกต์ของบริษัทภายนอก (เช่น Microsoft Outlook และ Internet Explorer) สำหรับการดำเนินการด้วยใบรับรองดิจิตอลที่มีการป้องกัน
Java Card Security สำหรับ HP ProtectTools	• Java Card Security กำหนดค่า HP ProtectTools Java Card สำหรับการตรวจสอบความถูกต้องของผู้ใช้ก่อนบูตฮาร์ดไดรฟ์ Java Card Security สามารถเข้าใช้งานได้จาก Embedded Security, Java Card และรหัสผ่าน • Java Card Security กำหนดค่า Java Cards แยกต่างหากสำหรับผู้ดูแลระบบและผู้ใช้ • Java Card Security เป็นอินเตอร์เฟซซอฟต์แวร์การจัดการสำหรับ Java Card Java Card เป็นอุปกรณ์ความปลอดภัยส่วนบุคคลที่ปกป้องข้อมูลการตรวจสอบความถูกต้อง ซึ่งต้องใช้ทั้งการ์ดและรหัส PIN เพื่อให้สามารถเข้าใช้งาน Java Card สามารถใช้ในการเข้าใช้งาน Credential Manager, Drive Encryption, HP BIOS หรือจุดเข้าใช้งานใดๆ ของผู้ผลิตรายอื่น
การกำหนดค่า BIOS สำหรับ HP ProtectTools	• การกำหนดค่า BIOS ให้การเข้าถึงเพื่อการจัดการรหัสผ่านของผู้ใช้และผู้ดูแลระบบที่ใช้งานอยู่ • การกำหนดค่า BIOS ให้ทางเลือกหนึ่งสำหรับยูทิลิตีการกำหนดค่า BIOS ก่อนเครื่องจะบูตเข้าสู่ระบบที่รู้จักกันในชื่อ การตั้งค่าด้วยปุ่ม F10

โมดูล	คุณลักษณะหลัก
การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools	• การเข้ารหัสไดรฟ์ให้การเข้ารหัสฮาร์ดไดรฟ์แบบครบถ้วนและสมบูรณ์ • การเข้ารหัสไดรฟ์จะใช้การตรวจสอบความถูกต้องก่อนบูตเครื่องเข้าสู่ระบบเพื่อถอดรหัสและเข้าถึงข้อมูล • การเข้ารหัสไดรฟ์จัดหาเครื่องมือการจัดการการตรวจสอบความถูกต้องซึ่งใช้ในการเข้ารหัสพาร์ติชัน ฮาร์ดไดรฟ์ และฮาร์ดไดรฟ์หลายตัว
Device Access Manager สำหรับ HP ProtectTools	• Device Access Manager จัดหาการควบคุมแบบปรับแต่งได้สำหรับฮาร์ดแวร์ที่จัดเก็บและรับส่งข้อมูล (พอร์ต USB, COM & LPT, เครื่องเล่นเพลงส่วนบุคคล, ไดรฟ์ซีดี, การ์ดอินเตอร์เฟซเน็ตเวิร์ก ฯลฯ) • นอกจากนี้ Device Access Manager ยังจัดการผู้ใช้และกลุ่มผู้ใช้ เพื่อจัดหาสิทธิ์ในการอ่าน เขียน อนุญาต หรือปฏิเสธข้อมูลบนฮาร์ดแวร์

การเข้าถึง HP ProtectTools Security

ในการเข้าถึง HP ProtectTools Security จากแผงควบคุมของ Windows® :

- เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager** (หรือ **HP ProtectTools Security Manager for Administrators** ใน Windows Vista)

หมายเหตุ: หลังจากที่คุณกำหนดค่าโมดูล Credential Manager แล้ว คุณยังสามารถเปิด HP ProtectTools ได้ด้วยการล็อกออนเข้าสู่ Credential Manager โดยตรงจากหน้าล็อกออนของ Windows สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การล็อกออน Windows ด้วย Credential Manager ในหน้า 15”

สำหรับ Windows Vista ผู้ดูแลระบบจะต้องใช้ “HP ProtectTools Security Manager for Administrators” เมื่อเข้าถึงการเข้ารหัสไดรฟ์

การบรรลุวัตถุประสงค์ด้านความปลอดภัยหลัก

โมดูล HP ProtectTools สามารถทำงานพร้อมๆ กันเพื่อให้โซลูชั่นด้านความปลอดภัยแบบต่างๆ รวมถึงวัตถุประสงค์ด้านความปลอดภัยหลักดังต่อไปนี้:

- การป้องกันการโจรกรรมที่เป็นเป้าหมาย
- การจำกัดการเข้าถึงข้อมูลที่มีความละเอียดอ่อน
- การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากตำแหน่งภายในหรือภายนอก
- การสร้างและใช้รหัสผ่านที่มีความรัดกุม

การป้องกันการโจรกรรมที่เป็นเป้าหมาย

ตัวอย่างของเหตุการณ์ประเภทนี้น่าจะเป็นการโจรกรรมที่มีเป้าหมายอยู่ที่คอมพิวเตอร์ ที่ภายในบรรจุข้อมูลลับ และข้อมูลลูกค้าในสถานที่ทำงานหรือในสภาพแวดล้อมแบบเปิด คุณลักษณะต่อไปนี้ช่วยป้องกันการโจรกรรมเป้าหมาย:

- คุณลักษณะการตรวจสอบความถูกต้องก่อนบูตเครื่องเข้าสู่ระบบ ซึ่งหากเปิดใช้งาน จะช่วยป้องกันการเข้าถึงระบบปฏิบัติการ (ดูขั้นต่อต่อไปนี้:
  - “การตั้งชื่อให้กับ Java Card ในหน้า 32”
  - “Device Access Manager สำหรับ HP ProtectTools ในหน้า 41 ”
  - “การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools ในหน้า 46”
- DriveLock ช่วยรับประกันว่า ข้อมูลจะไม่สามารถเข้าถึงได้แม้นำฮาร์ดไดรฟ์ออกและติดตั้งลงในระบบที่ไม่มีความปลอดภัย โปรดดูที่ “Security ในหน้า 38”
- คุณลักษณะ Personal Secure Drive ของโมดูล Embedded Security สำหรับ HP ProtectTools จะเข้ารหัสข้อมูลที่มีความละเอียดอ่อน เพื่อช่วยรับประกันว่า ข้อมูลเหล่านั้นจะไม่สามารถเข้าถึงได้หากไม่มีการตรวจสอบความถูกต้อง (ดูขั้นตอนต่อไปนี้:
  - Embedded Security “ขั้นตอนการติดตั้ง ในหน้า 25”
  - “การใช้ไดรฟ์ความปลอดภัยส่วนบุคคล ในหน้า 27”

การจำกัดการเข้าถึงข้อมูลที่มีความละเอียดอ่อน

สมมุติว่า ผู้รับเหมากำลังทำงานอยู่นอกสถานที่และได้รับสิทธิ์เข้าถึงคอมพิวเตอร์ เพื่อทบทวนข้อมูลทางการเงินที่มีความละเอียดอ่อน คุณไม่ต้องการให้ผู้รับเหมาพิมพ์ไฟล์หรือบันทึกไฟล์ลงบนอุปกรณ์ที่สามารถเขียนได้ เช่น ซีดี คุณลักษณะต่อไปนี้ช่วยจำกัดการเข้าถึงข้อมูล:

- Device Access Manager สำหรับ HP ProtectTools ช่วยให้ผู้จัดการฝ่ายไอทีสามารถเข้าถึงอุปกรณ์ที่บันทึกได้ ดังนั้นจึงไม่สามารถพิมพ์หรือคัดลอกข้อมูลสำคัญจากฮาร์ดไดรฟ์ไปยังสื่อบันทึกที่ถอดออกได้ โปรดดูที่ “Device class configuration (ขั้นสูง) ในหน้า 44”
- DriveLock ช่วยรับประกันว่า ข้อมูลจะไม่สามารถเข้าถึงได้แม้นำฮาร์ดไดรฟ์ออกและติดตั้งลงในระบบที่ไม่มีความปลอดภัย โปรดดูที่ “Security ในหน้า 38”

การป้องกันการเข้าถึงโดยไม่ได้รับอนุญาตจากตำแหน่งภายในหรือภายนอก

หากคอมพิวเตอร์มีข้อมูลที่เป็นความลับและข้อมูลลูกค้าถูกเข้าใช้จากตำแหน่งภายในหรือภายนอก ผู้ใช้ที่ไม่ได้รับอนุญาตอาจสามารถเข้าถึงทรัพยากรเน็ตเวิร์กของบริษัท หรือข้อมูลจากบริการทางการเงิน ผู้บริหารระดับสูง หรือทีมวิจัยและพัฒนา คุณลักษณะต่อไปนี้ช่วยป้องกันการเข้าใช้โดยไม่ได้รับอนุญาต:

- คุณลักษณะการตรวจสอบความถูกต้องก่อนบูตเครื่องเข้าสู่ระบบ ซึ่งหากเปิดใช้งาน จะช่วยป้องกันการเข้าถึงระบบปฏิบัติการ (ดูขั้นตอนต่อไปนี้:
  - “การตั้งชื่อให้กับ Java Card ในหน้า 32”
  - “การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools ในหน้า 46”
- Embedded Security สำหรับ HP ProtectTools ช่วยป้องกันข้อมูลผู้ใช้ที่มีความละเอียดอ่อนหรือข้อมูลลับที่จัดเก็บไว้บนคอมพิวเตอร์โดยใช้ขั้นตอนต่อไปนี้:
  - Embedded Security “ขั้นตอนการติดตั้ง ในหน้า 25”
  - “การใช้ไดรฟ์ความปลอดภัยส่วนบุคคล ในหน้า 27”
- เมื่อใช้ขั้นตอนต่อไปนี้ Credential Manager สำหรับ HP ProtectTools จะช่วยรับประกันว่า ผู้ใช้ที่ไม่ได้รับอนุญาตจะไม่ได้รับรหัสผ่านหรือเข้าถึงโปรแกรมประยุกต์ที่มีรหัสผ่านป้องกัน
  - Credential Manager “ขั้นตอนการติดตั้ง ในหน้า 12”
  - “การใช้การลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) ในหน้า 16”
- Device Access Manager สำหรับ HP ProtectTools ช่วยให้ผู้จัดการฝ่ายไอทีสามารถเข้าถึงอุปกรณ์ที่บันทึกได้ ดังนั้นจึงไม่สามารถคัดลอกข้อมูลสำคัญจากฮาร์ดไดรฟ์ได้ โปรดดูที่ Simple configuration ในหน้า 43
- คุณลักษณะ Personal Secure Drive จะเข้ารหัสข้อมูลที่มีความละเอียดอ่อน เพื่อช่วยรับประกันว่า ข้อมูลเหล่านั้นจะไม่สามารถเข้าถึงได้หากไม่มีการตรวจสอบความถูกต้องผ่านขั้นตอนต่อไปนี้:
  - Embedded Security “ขั้นตอนการติดตั้ง ในหน้า 25”
  - “การใช้ไดรฟ์ความปลอดภัยส่วนบุคคล ในหน้า 27”

การสร้างและใช้รหัสผ่านที่มีความรัดกุม

เนื่องจากมีรหัสผ่านมากมายที่ต้องใช้ในการเข้าถึงเว็บไซต์หรือโปรแกรมประยุกต์ที่ปลอดภัย ผู้ใช้จึงมีแนวโน้มที่จะใช้รหัสผ่านที่จำได้ง่ายเพียงรหัสเดียวสำหรับทุกๆ โปรแกรมและทุกๆ เว็บไซต์ เพื่อป้องกันไม่ให้เกิดความสับสนว่ารหัสผ่านใดใช้กับโปรแกรมใด Credential Manager สำหรับ HP ProtectTools จัดเก็บรหัสผ่านอย่างปลอดภัย และเพิ่มความสะดวกในการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) โดยใช้ขั้นตอนต่อไปนี้:

- การสร้างรหัสผ่านที่มีความรัดกุม ในหน้า 8
- Credential Manager “ขั้นตอนการติดตั้ง ในหน้า 12”
- “การใช้การลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) ในหน้า 16”

เพื่อความปลอดภัยที่รัดกุมยิ่งขึ้น Embedded Security สำหรับ HP ProtectTools จะช่วยป้องกันหน่วยเก็บข้อมูลกลางของชื่อผู้ใช้และรหัสผ่าน ซึ่งจะช่วยให้ผู้ใช้รักษารหัสผ่านที่รัดกุมหลายๆ ตัวไว้ได้โดยไม่ต้องจดลงบนกระดาษหรือพยายามจดจำ โปรดดู Embedded Security “ขั้นตอนการติดตั้ง ในหน้า 25”

องค์ประกอบด้วยความปลอดภัยเพิ่มเติม

การกำหนดบทบาทด้านความปลอดภัย

ในการจัดการด้านความปลอดภัยของคอมพิวเตอร์ (โดยเฉพาะสำหรับองค์กรขนาดใหญ่) หลักปฏิบัติที่สำคัญประการหนึ่งคือการจัดสรรความรับผิดชอบและสิทธิ์ให้กับผู้ดูแลระบบและผู้ใช้ประเภทต่างๆ

หมายเหตุ: ในองค์กรขนาดเล็กหรือการใช้เดี่ยวๆ บทบาทเหล่านั้นอาจอยู่ในตัวบุคคลเพียงคนเดียว

สำหรับ HP ProtectTools ความรับผิดชอบและเอกสิทธิ์ด้านความปลอดภัยสามารถแบ่งออกเป็นหลายๆ บทบาทดังต่อไปนี้:

- เจ้าหน้าที่ด้านความปลอดภัย–กำหนดระดับความปลอดภัยสำหรับบริษัทหรือเน็ตเวิร์ก และกำหนดคุณลักษณะด้านความปลอดภัยที่จะนำมาใช้ เช่น Java Cards โปรแกรมอ่านไบโอเมตริก หรือ USB โทเคน

  หมายเหตุ: คุณลักษณะมากมายใน HP ProtectTools สามารถปรับเปลี่ยนโดยเจ้าหน้าที่ด้านความปลอดภัยภายใต้ความร่วมมือกับ HP สำหรับข้อมูลเพิ่มเติม โปรดดูที่เว็บไซต์ HP ที่ http://www.hp.com

- ผู้ดูแลระบบไอที–นำไปใช้และจัดการคุณลักษณะด้านความปลอดภัยที่กำหนดโดยเจ้าหน้าที่ด้านความปลอดภัย ผู้ดูแลระบบไอทีสามารถเปิดใช้งานและปิดใช้งานคุณลักษณะบางประการ ตัวอย่างเช่น หากเจ้าหน้าที่ด้านความปลอดภัยตัดสินใจใช้ Java Cards ผู้ดูแลระบบไอทีสามารถเปิดใช้งานโหมดความปลอดภัย Java Card BIOS

- ผู้ใช้–ใช้คุณลักษณะการป้องกันความปลอดภัย ตัวอย่างเช่น หากเจ้าหน้าที่ด้านความปลอดภัยและผู้ดูแลระบบไอทีเปิดใช้งาน Java Cards สำหรับระบบ ผู้ใช้สามารถตั้ง PIN สำหรับ Java Card และใช้การ์ดสำหรับการตรวจสอบความถูกต้อง

การจัดการรหัสผ่านของ HP ProtectTools

คุณลักษณะเกือบทั้งหมดของ HP ProtectTools Security Manager ได้รับการป้องกันด้วยรหัสผ่าน ตารางต่อไปนี้แสดงรายการรหัสผ่านที่ใช้กันโดยทั่วๆ ไป โมดูลซอฟต์แวร์ที่ใช้ตั้งรหัสผ่าน และฟังก์ชันของรหัสผ่าน

รหัสผ่านที่ถูกกำหนดและใช้โดยผู้ดูแลระบบไอทีเท่านั้นก็จะแสดงในตารางนี้ด้วย รหัสผ่านอื่นๆ ทั้งหมดอาจถูกกำหนดโดยผู้ใช้หรือผู้ดูแลระบบปกติ

รหัสผ่านของ HP ProtectTools	กำหนดในโมดูล HP ProtectTools นี้	ฟังก์ชัน
รหัสผ่านสำหรับการล็อกออน Credential Manager	Credential Manager	รหัสผ่านนี้มีตัวเลือก 2 ตัวเลือก: • สามารถนำมาใช้ในการล็อกออนแยกต่างหากเพื่อเข้าสู่ Credential Manager หลังจากล็อกออนเข้าสู่ Windows • สามารถนำมาใช้แทนขั้นตอนการล็อกออนเข้าสู่ Windows เพื่ออนุญาตให้มีการเข้าถึง Windows และ Credential Manager พร้อมๆ กัน
รหัสผ่านสำหรับไฟล์การกู้คืนของ Credential Manager	Credential Manager, โดยผู้ดูแลระบบไอที	ป้องกันการเข้าสู่ไฟล์การกู้คืนของ Credential Manager
รหัสผ่านของคีย์ผู้ใช้เบื้องต้น **หมายเหตุ:** หรือที่รู้จักกันในชื่อ: รหัสผ่านความปลอดภัยภายใน	Embedded Security	ใช้เพื่อเข้าสู่คุณลักษณะ Embedded Security เช่น การเข้ารหัสอีเมล์ ไฟล์และโฟลเดอร์เพื่อความปลอดภัย เมื่อใช้สำหรับการตรวจสอบความถูกต้องเมื่อเปิดเครื่อง รหัสผ่านนี้ยังป้องกันการเข้าสู่เนื้อหาภายในคอมพิวเตอร์เมื่อเปิด รีสตาร์ทหรือเรียกคืนคอมพิวเตอร์จากภาวะไฮเบอร์เนชั่น
รหัสผ่าน Emergency Recovery Token **หมายเหตุ:** หรือที่รู้จักกันในชื่อ: รหัสผ่านของคีย์ Emergency Recovery Token	Embedded Security, โดยผู้ดูแลระบบไอที	ป้องกันการเข้าสู่ Emergency Recovery Token ซึ่งก็คือไฟล์สำรองสำหรับชิปความปลอดภัยแบบฝังตัว

รหัสผ่านของ HP ProtectTools	กำหนดในโมดูล HP ProtectTools นี้	ฟังก์ชัน
รหัสผ่านผู้เป็นเจ้าของ	Embedded Security, โดยผู้ดูแลระบบไอที	ป้องกันระบบและชิป TPM จากการเข้าใช้ฟังก์ชันของผู้เป็นเจ้าของ Embedded Security โดยไม่ได้รับอนุญาต
PIN ของ Java Card	ความปลอดภัยของ Java Card	ป้องกันการเข้าสู่เนื้อหาของ Java Card และตรวจสอบความถูกต้องของผู้ใช้ Java Card เมื่อใช้สำหรับการตรวจสอบความถูกต้องเมื่อเปิดเครื่อง รหัสของ Java Card ยังป้องกันการเข้าสู่ยูทิลิตีการตั้งค่าคอมพิวเตอร์และเนื้อหาภายในคอมพิวเตอร์ ตรวจสอบความถูกต้องของผู้ใช้ Drive Encryption หากเลือกโทเคน Java Card
รหัสผ่านของการตั้งค่าคอมพิวเตอร์ **หมายเหตุ:** และรู้จักในชื่อรหัสผ่านผู้ดูแลระบบ BIOS รหัสผ่านการตั้งค่า F10 หรือรหัสผ่านการตั้งค่าความปลอดภัย	การกำหนดค่า BIOS, โดยผู้ดูแลระบบไอที	ป้องกันการเข้าสู่ยูทิลิตีการตั้งค่าคอมพิวเตอร์
รหัสผ่านป้องกันการเปิดเครื่อง	การกำหนดค่า BIOS	ป้องกันการเข้าสู่เนื้อหาของคอมพิวเตอร์เมื่อเปิด รีสตาร์ทหรือเรียกคืนคอมพิวเตอร์จากภาวะไฮเบอร์เนชัน
รหัสผ่านสำหรับการล็อกออน Windows	แผงควบคุมของ Windows	สามารถนำมาใช้สำหรับการล็อกออนด้วยตัวผู้ใช้เองหรือบันทึกบน Java Card

การสร้างรหัสผ่านที่มีความรัดกุม

เมื่อสร้างรหัสผ่าน คุณต้องทำตามข้อกำหนดเฉพาะใดๆ ที่ถูกกำหนดขึ้นด้วยโปรแกรมก่อน อย่างไรก็ตาม โดยทั่วไปนั้น ให้พิจารณาถึงแนวทางต่อไปนี้เพื่อช่วยคุณสร้างรหัสผ่านที่มีความรัดกุม และลดโอกาสที่รหัสผ่านของคุณจะถูกเจาะ:

- ใช้รหัสผ่านที่มีอักขระมากกว่า 6 ตัว ที่แนะนำคือมากกว่า 8 ตัว
- ผสมระหว่างตัวพิมพ์ใหญ่และพิมพ์เล็กในรหัสผ่าน
- เมื่อเป็นไปได้ ให้รวมทั้งอักขระที่เป็นตัวอักษรและตัวเลข รวมอักขระพิเศษและเครื่องหมายวรรคตอน
- แทนตัวอักษรในคำสำคัญด้วยอักขระพิเศษหรือตัวเลข ตัวอย่างเช่น คุณสามารถใช้เลข 1 แทนตัว I หรือ L
- รวมคำต่างๆ ด้วยภาษา 2 ภาษาหรือมากกว่านั้น
- แยกคำหรือวลีด้วยตัวเลขหรืออักขระพิเศษไว้ตรงกลาง เช่น “Mary2-2Cat45”
- ห้ามใช้รหัสผ่านที่อาจปรากฏในพจนานุกรม
- ห้ามใช้ชื่อของคุณเป็นรหัสผ่าน หรือข้อมูลส่วนบุคคลใดๆ เช่น วันเกิด ชื่อสัตว์เลี้ยง หรือนามสกุลก่อนแต่งงานของมารดา แม้คุณจะสะกดย้อนกลับ
- เปลี่ยนรหัสผ่านให้เป็นกิจวัตร คุณอาจเปลี่ยนอักขระครั้งละหนึ่งถึงสองตัว
- หากคุณจดรหัสผ่านไว้บนกระดาษ ห้ามเก็บกระดาษแผ่นนี้ไว้ในที่ๆ มองเห็นได้และใกล้ๆ กับคอมพิวเตอร์
- ห้ามบันทึกรหัสผ่านไว้ในไฟล์ เช่น อีเมล บนคอมพิวเตอร์
- ห้ามใช้บัญชีร่วมกับผู้อื่น หรือบอกรหัสผ่านของคุณให้กับผู้อื่น

การสำรองข้อมูลและการเรียกคืน HP ProtectTools

การสำรองข้อมูลและการเรียกคืน HP ProtectTools มาพร้อมกับวิธีการที่สะดวกและรวดเร็วเมื่อต้องการสำรองข้อมูลและเรียกคืนใบรับรองจากโมดูล HP ProtectTools ทั้งหมดที่ได้รับการสนับสนุน

การสำรองข้อมูลใบรับรองและการตั้งค่า

คุณสามารถสำรองข้อมูลใบรับรองได้ด้วยวิธีการต่อไปนี้:

- ใช้วิซาร์ดการสำรองข้อมูล HP ProtectTools เพื่อเลือกและสำรองข้อมูลโมดูล HP ProtectTools
- สำรองข้อมูลโมดูล HP ProtectTools ที่เลือกไว้ล่วงหน้า

หมายเหตุ: คุณต้องกำหนดตัวเลือกการสำรองข้อมูลก่อนจึงจะสามารถใช้วิธีนี้

- การกำหนดเวลาสำรองข้อมูล

หมายเหตุ: คุณต้องกำหนดตัวเลือกการสำรองข้อมูลก่อนจึงจะสามารถใช้วิธีนี้

การใช้วิซาร์ดการสำรองข้อมูล HP ProtectTools เพื่อเลือกและสำรองข้อมูลโมดูล HP ProtectTools

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ก **Backup and Restore**
3. ในแผงด้านขวา ให้คลิก **Backup Options** วิซาร์ดการสำรองข้อมูล HP ProtectTools จะเปิดออก ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อสำรองข้อมูลใบรับรอง

การกำหนดตัวเลือกการสำรองข้อมูล

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **HP ProtectTools** และคลิก **Backup and Restore**
3. ในแผงด้านขวา ให้คลิก **Backup Options** วิซาร์ดการสำรองข้อมูล HP ProtectTools จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ
5. หลังจากที่คุณกำหนดและยืนยัน **Storage File Password** แล้ว ให้เลือก **Remember all passwords and authentication values for future automated backups**
6. คลิก **Save Settings** และคลิก **Finish**

การสำรองข้อมูลโมดูล HP ProtectTools ที่เลือกไว้ล่วงหน้า

หมายเหตุ: คุณต้องกำหนดตัวเลือกการสำรองข้อมูลก่อนจึงจะสามารถใช้วิธีนี้

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **HP ProtectTools** และคลิก **Backup and Restore**
3. ในแผงด้านขวา ให้คลิก **Backup**

การกำหนดเวลาสำรองข้อมูล

หมายเหตุ: คุณต้องกำหนดตัวเลือกการสำรองข้อมูลก่อนจึงจะสามารถใช้วิธีนี้

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **HP ProtectTools** และคลิก **Backup and Restore**
3. ในแผงด้านขวา ให้คลิก **Schedule Backups**
4. บนแท็บ **Task** ให้เลือกกล่องตัวเลือก **Enabled** เพื่อเปิดใช้งานการสำรองข้อมูลที่กำหนดเวลาไว้
5. คลิก **Set Password** และพิมพ์และยืนยันรหัสผ่านของคุณในไดอะล็อกบ็อกซ์ **Set Password** คลิก **OK**
6. คลิก **Apply** คลิกแท็บ **Schedule** คลิกลูกศร **Schedule Task** และเลือกความถี่ในการสำรองข้อมูลโดยอัตโนมัติ
7. ใต้ **Start time** ให้ใช้ลูกศร **Start time** เพื่อเลือกเวลาที่แน่นอนสำหรับการเริ่มต้นสำรองข้อมูล

8. คลิก **Advanced** เพื่อเลือกวันที่เริ่มต้น และวันที่สิ้นสุด และการตั้งค่าการเกิดซ้ำของงาน คลิก **Apply**
9. คลิก **Settings** และเลือกการตั้งค่าสำหรับ **Scheduled Task Completed**, **Idle Time** และ **Power Management**
10. คลิก **Apply** และคลิก **OK** เพื่อปิดไดอะล็อกบ็อกซ์

การเรียกคืนใบรับรอง

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **HP ProtectTools** และคลิก **Backup and Restore**
3. ในแผงด้านขวา ให้คลิก **Restore** วิซาร์ดการเรียกคืน HP ProtectTools จะเปิดออก ทำตามคำแนะนำที่หน้าจอ

การกำหนดค่าการตั้งค่า

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **HP ProtectTools** และคลิก **Settings**
3. ในแผงด้านขวา ให้เลือกการตั้งค่าของคุณ และคลิก **OK**

2 Credential Manager สำหรับ HP ProtectTools

Credential Manager อนุญาตให้ผู้ใช้กำหนดและปรับใช้ระบบรักษาความปลอดภัยที่เข้มงวดมากกว่าการใช้รหัสผ่านในการตรวจสอบความถูกต้องของผู้ใช้ และป้องกันรหัสผ่านส่วนบุคคล พร้อมทั้งจัดหาความสามารถในการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) Credential Manager สำหรับ HP ProtectTools ช่วยป้องกันการล็อกอินเข้าใช้คอมพิวเตอร์ของคุณโดยใช้คุณสมบัติด้านความปลอดภัยดังต่อไปนี้:

- ทางเลือกอื่นนอกเหนือจากรหัสผ่านเมื่อล็อกเข้าสู่ Windows เช่น การใช้สมาร์ทการ์ดหรือโปรแกรมอ่านไบโอเมตริกเมื่อล็อกเข้าสู่ Windows สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การลงทะเบียนใบรับรอง ในหน้า 12”
- คุณสมบัติการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) จะจดจำใบรับรองสำหรับเว็บไซต์ รวมถึงโปรแกรมประยุกต์และทรัพยากรเน็ตเวิร์กที่มีการป้องกันให้โดยอัตโนมัติ
- การสนับสนุนสำหรับอุปกรณ์ป้องกันความปลอดภัยเสริม เช่น สมาร์ทการ์ด และโปรแกรมอ่านไบโอเมตริก
- การสนับสนุนสำหรับการตั้งค่าความปลอดภัยเพิ่มเติม เช่น การต้องใช้การตรวจสอบความถูกต้องโดยใช้อุปกรณ์ป้องกันความปลอดภัยเสริม เพื่อปลดล็อคคอมพิวเตอร์

ขั้นตอนการติดตั้ง

การล็อกออน Credential Manager

ขึ้นอยู่กับการกำหนดค่า คุณสามารถล็อกออนสู่ Credential Manager ด้วยหนึ่งในวิธีการต่างๆ ดังต่อไปนี้:

- วิซาร์ดการล็อกออนสู่ Credential Manager (แนะนำ)
- ไอคอน HP ProtectTools Security Manager ในเนื้อที่ประกาศ
- HP ProtectTools Security Manager

หมายเหตุ: หากคุณใช้พรอมต์การล็อกออนสู่ Credential Manager บนหน้าจอล็อกออนของ Windows คุณจะถูกล็อกเข้าสู่ Windows ด้วย

ในครั้งแรกที่คุณเปิด Credential Manager ให้ล็อกเข้าด้วยรหัสผ่านสำหรับล็อกออน Windows ปกติของคุณ หลังจากนั้น บัญชี Credential Manager จะถูกสร้างขึ้นโดยอัตโนมัติด้วยใบรับรองการล็อกออน Windows ของคุณ

หลังจากล็อกเข้าสู่ Credential Manager แล้ว คุณสามารถลงทะเบียนใบรับรองเพิ่มเติม เช่น ลายพิมพ์นิ้วมือหรือ Java Card สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การลงทะเบียนใบรับรอง ในหน้า 12”

ในการล็อกออนครั้งต่อไป คุณสามารถเลือกกฎเกณฑ์การล็อกออน และใช้ใบรับรองที่ลงทะเบียนแล้วหลายๆ ประเภทรวมกัน

การใช้วิซาร์ดการล็อกออนสู่ Credential Manager

ในการล็อกออนสู่ Credential Manager โดยใช้วิซาร์ดการล็อกออน Credential Manager ให้ใช้ขั้นตอนต่อไปนี้:

1. เปิดวิซาร์ดการล็อกออน Credential Manager ด้วยหนึ่งในวิธีการต่างๆ ดังต่อไปนี้:
   - จากหน้าจอล็อกออนของ Windows
   - จากเนื้อที่ประกาศ ให้คลิกสองครั้งที่ไอคอน **HP ProtectTools Security Manager**
   - จากหน้า “Credential Manager” ของ ProtectTools Security Manager ให้คลิกลิงค์ **Log On** ที่มุมบนขวาของหน้าต่าง
2. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อล็อกออนสู่ Credential Manager

การล็อกออนเป็นครั้งแรก

ก่อนเริ่มต้น คุณต้องล็อกเข้าสู่ Windows ด้วยบัญชีผู้ดูแลระบบก่อน แต่ไม่ต้องล็อกเข้าสู่ Credential Manager

1. เปิด HP ProtectTools Security Manager ได้ด้วยการคลิกสองครั้งที่ไอคอน HP ProtectTools Security Manager ในเนื้อที่ประกาศ หน้าต่าง HP ProtectTools Security Manager จะเปิดออก
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** และคลิก **Log On** ที่มุมบนขวาของแผงด้านขวา วิซาร์ดการล็อกออน Credential Manager จะเปิดออก
3. พิมพ์รหัสผ่านสำหรับ Windows ของคุณลงในกล่อง **Password** และคลิก **Next**

การลงทะเบียนใบรับรอง

คุณสามารถใช้หน้า “My Identity” เพื่อลงทะเบียนวิธีการตรวจสอบความถูกต้องหรือใบรับรองแบบต่างๆ ของคุณ หลังจากที่วิธีการเหล่านั้นได้รับการลงทะเบียนแล้ว คุณสามารถใช้วิธีการดังกล่าวเพื่อล็อกเข้าสู่ Credential Manager

การลงทะเบียนลายพิมพ์นิ้วมือ

โปรแกรมอ่านลายพิมพ์นิ้วมือจะอนุญาตให้คุณล็อกเข้าสู่ Windows ด้วยลายพิมพ์นิ้วมือของคุณสำหรับการตรวจสอบความถูกต้องแทนการใช้รหัสผ่านของ Windows หรือใช้ทั้งสองอย่างร่วมกัน

การกำหนดค่าโปรแกรมอ่านลายพิมพ์นิ้วมือ

1. หลังจากล็อกเข้าสู่ Credential Manager แล้ว ให้วางนิ้วมือผ่านโปรแกรมอ่านลายพิมพ์นิ้วมือ วิซาร์ดการลงทะเบียน Credential Manager จะเปิดออก
2. ทำตามคำแนะนำบนหน้าจอเพื่อทำการลงทะเบียนลายพิมพ์นิ้วมือและกำหนดค่าโปรแกรมอ่านลายพิมพ์นิ้วมือให้เสร็จสมบูรณ์
3. ในการกำหนดค่าโปรแกรมอ่านลายพิมพ์นิ้วมือสำหรับผู้ใช้ Windows ให้ล็อกเข้าสู่ Windows ในฐานะผู้ใช้รายดังกล่าว และทำตามขั้นตอนที่ 1 และ 2

การใช้ลายพิมพ์นิ้วมือที่ลงทะเบียนแล้วของคุณล็อกเข้าสู่ Windows

1. ทันทีหลังจากที่คุณลงทะเบียนลายพิมพ์นิ้วมือแล้ว ให้รีสตาร์ท Windows
2. ที่หน้าจอต้อนรับของ Windows ให้วางนิ้วมือของคุณที่ลงทะเบียนแล้วเพื่อล็อกเข้าสู่ Windows

การลงทะเบียน Java Card, USB eToken หรือโทเคนเสมือนจริง

หมายเหตุ: คุณต้องมีโปรแกรมอ่านการ์ดหรือแป้นพิมพ์สมาร์ทการ์ดที่กำหนดค่าไว้สำหรับขั้นตอนนี้ หากคุณเลือกที่จะไม่ใช้สมาร์ทการ์ด คุณสามารถลงทะเบียนโทเคนเสมือนจริงตามขั้นตอนที่อธิบายไว้ใน “การสร้างโทเคนเสมือนจริง ในหน้า 14”

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวา ให้คลิก **Register Smart Card or Token** วิซาร์ดการลงทะเบียน Credential Manager จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

การลงทะเบียน USB eToken

1. ตรวจสอบให้แน่ใจว่า ได้ติดตั้งไดรเวอร์ USB eToken แล้ว

   หมายเหตุ: โปรดดูที่คู่มือ USB eToken สำหรับข้อมูลเพิ่มเติม

2. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
3. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
4. ในแผงด้านขวา ให้คลิก **Register Smart Card or Token** วิซาร์ดการลงทะเบียน Credential Manager จะเปิดออก
5. ทำตามคำแนะนำที่หน้าจอ

การลงทะเบียนใบรับรองอื่นๆ

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวา ให้คลิก **Register Credentials** วิซาร์ดการลงทะเบียน Credential Manager จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

งานทั่วไป

ผู้ใช้ทุกคนมีสิทธิ์เข้าถึงหน้า “My Identity" ใน Credential Manager จากหน้า “My Identity” คุณสามารถทำงานต่างๆ ดังต่อไปนี้:

- การสร้างโทเคนเสมือนจริง
- การเปลี่ยนแปลงรหัสผ่านสำหรับล็อกเข้าสู่ Windows
- การจัดการ PIN ของโทเคน
- การจัดการตัวตน
- การล็อคคอมพิวเตอร์

หมายเหตุ: ตัวเลือกนี้จะนำมาใช้ได้เฉพาะเมื่อพรอมต์การล็อกออนแบบคลาสสิกของ Credential Manager ถูกเปิดใช้งาน โปรดดู “ตัวอย่างที่ 1–การใช้หน้า “Advanced Settings” เพื่ออนุญาตให้ล็อกออน Windows จาก Credential Manager ในหน้า 22”

การสร้างโทเคนเสมือนจริง

โทเคนเสมือนจริงทำงานเหมือนกับ Java Card หรือ USB eToken ค่อนข้างมาก โทเคนจะถูกบันทึกไว้บนฮาร์ดไดรฟ์ของคอมพิวเตอร์หรือในรีจิสทรีของ Windows เมื่อคุณล็อกเข้าด้วยโทเคนเสมือนจริง ระบบจะขอให้คุณป้อนรหัส PIN ของผู้ใช้เพื่อทำการตรวจสอบความถูกต้องให้เสร็จสมบูรณ์

ในการสร้างโทเคนเสมือนจริงใหม่:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวา ให้คลิก **Virtual Token** วิซาร์ดการลงทะเบียน Credential Manager จะเปิดออก

หมายเหตุ: หาก **Virtual Token** ไม่ใช่ตัวเลือก ให้ใช้ขั้นตอนสำหรับ “การลงทะเบียนใบรับรองอื่นๆ ในหน้า 13”

4. ทำตามคำแนะนำที่หน้าจอ

การเปลี่ยนแปลงรหัสผ่านสำหรับล็อกเข้าสู่ Windows

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวา ให้คลิก **Change Windows Password**
4. พิมพ์รหัสผ่านเดิมของคุณลงในช่อง **Old Password**
5. พิมพ์รหัสผ่านใหม่ของคุณลงในช่อง **New password** และ **Confirm password**
6. คลิก **Finish**

การเปลี่ยนรหัส PIN ของโทเคน

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวา ให้คลิก **Change Token PIN**
4. เลือกโทเคนที่คุณต้องการเปลี่ยนรหัส PIN และคลิก **Next**
5. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อเปลี่ยนรหัส PIN ให้เสร็จสมบูรณ์

การจัดการตัวตน

การล้างตัวตนออกจากระบบ

หมายเหตุ: สิ่งนี้จะไม่มีผลต่อบัญชีผู้ใช้ Windows ของคุณ

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวาให้คลิก **Clear Identity for this Account**
4. คลิก **Yes** ในไดอะล็อกบ็อกซ์การยืนยัน ตัวตนของคุณจะถูกล็อกออกและย้ายออกจากระบบ

การล็อคคอมพิวเตอร์

คุณสมบัตินี้จะนำมาใช้ได้หากคุณล็อกเข้าสู่ Windows ด้วย Credential Manager ในการสร้างความปลอดภัยให้กับคอมพิวเตอร์เมื่อคุณไม่ได้อยู่ที่โต๊ะทำงาน ให้ใช้คุณสมบัติล็อคเวิร์กสเตชัน คุณสมบัตินี้จะป้องกันผู้ใช้ที่ไม่ได้รับอนุญาตเข้าใช้คอมพิวเตอร์ของคุณ เฉพาะคุณและสมาชิกของกลุ่มผู้ดูแลระบบบนคอมพิวเตอร์ของคุณเท่านั้นที่สามารถปลดล็อค

หมายเหตุ: ตัวเลือกนี้จะนำมาใช้ได้เฉพาะเมื่อพรอมต์การล็อกออนแบบคลาสสิกของ Credential Manager ถูกเปิดใช้งาน โปรดดู “ตัวอย่างที่ 1–การใช้หน้า “Advanced Settings” เพื่ออนุญาตให้ล็อกออน Windows จาก Credential Manager ในหน้า 22”

สำหรับความปลอดภัยเพิ่มเติม คุณสามารถกำหนดค่าคุณสมบัติล็อคเวิร์กสเตชันให้ขอ Java Card โปรแกรมอ่านไบโอเมตริก หรือโทเคนเพื่อปลดล็อคคอมพิวเตอร์ สำหรับข้อมูลเพิ่มเติม ดูที่ “การกำหนดค่าการตั้งค่า Credential Manager ในหน้า 22”

ในการปลดล็อคคอมพิวเตอร์:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager**
3. ในแผงด้านขวา ให้คลิก **Lock Workstation** หน้าจอล็อกเข้าสู่ Windows จะปรากฏขึ้น คุณต้องใช้รหัสผ่านของ Windows หรือวิซาร์ดการล็อกออน Credential Manager เพื่อปลดล็อคคอมพิวเตอร์

การใช้การล็อกเข้าสู่ Windows

คุณสามารถใช้ Credential Manager เพื่อล็อกเข้าสู่ Windows ที่คอมพิวเตอร์ท้องถิ่นหรือบนโดเมนของเน็ตเวิร์ก เมื่อคุณล็อกเข้าสู่ Credential Manager เป็นครั้งแรก ระบบจะเพิ่มบัญชีผู้ใช้ Windows ในท้องที่ในฐานะที่เป็นบัญชีสำหรับบริการ Windows Logon ให้โดยอัตโนมัติ

การล็อกออน Windows ด้วย Credential Manager

คุณสามารถใช้ Credential Manager เพื่อล็อกเข้าสู่เน็ตเวิร์กของ Windows หรือบัญชีในท้องที่

1. หากคุณลงทะเบียนลายพิมพ์นิ้วมือเพื่อล็อกเข้าสู่ Windows ให้วางนิ้วมือของคุณเพื่อล็อกออน
2. หากคุณไม่ได้ลงทะเบียนลายพิมพ์นิ้วมือเพื่อล็อกออน Windows ให้คลิกที่ไอคอนบนแป้นพิมพ์ที่มุมซ้ายบนของหน้าจอที่อยู่ติดกับไอคอนลายพิมพ์นิ้วมือ วิซาร์ดการล็อกออน Credential Manager จะเปิดออก
3. คลิกลูกศร **User name** และคลิกชื่อของคุณ
4. พิมพ์รหัสผ่านของคุณลงในกล่อง **Password** และคลิก **Next**

5. เลือก **More** > **Wizard Options**

   a. หากคุณต้องการให้ข้อมูลนี้เป็นชื่อผู้ใช้เริ่มต้นของคุณในครั้งหน้าที่คุณล็อกเข้าสู่คอมพิวเตอร์ ให้เลือกกล่องตัวเลือก **Use last user name on next logon**

   b. หากคุณต้องการให้กฎเกณฑ์การล็อกออนนี้เป็นวิธีการเริ่มต้น ให้เลือกกล่องตัวเลือก **Use last policy on next logon**

6. ทำตามคำแนะนำที่หน้าจอ หากข้อมูลการตรวจสอบความถูกต้องของคุณถูกต้อง คุณจะถูกล็อกเข้าสู่บัญชี Windows ของคุณและเข้าสู่ Credential Manager

การเพิ่มบัญชี

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ให้คลิก **Windows Logon** จากนั้นคลิก **Add a Network Account** วิซาร์ดการเพิ่มบัญชีเน็ตเวิร์กจะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

การนำบัญชีออก

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ให้คลิก **Windows Logon** จากนั้นคลิก **Manage Network Accounts** ไดอะล็อกบ็อกซ์ **Manage Network Accounts** จะเปิดออก
4. คลิกบัญชีที่คุณต้องการนำออก และคลิก **Remove**
5. ในไดอะล็อกบ็อกซ์การยืนยัน คลิก **Yes**
6. คลิก **OK**

การใช้การลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On)

Credential Manager มีคุณสมบัติการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) ที่จัดเก็บชื่อผู้ใช้และรหัสผ่านสำหรับโปรแกรมอินเทอร์เน็ตและ Windows หลายๆ โปรแกรม และจะป้อนใบรับรองการล็อกออนให้โดยอัตโนมัติเมื่อคุณเข้าสู่โปรแกรมที่ลงทะเบียน

หมายเหตุ: ความปลอดภัยและความเป็นส่วนตัวเป็นคุณสมบัติที่สำคัญของการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) ใบรับรองทั้งหมดจะถูกเข้ารหัสและนำมาใช้ได้เฉพาะหลังจากล็อกเข้าสู่ Credential Manager ได้สำเร็จแล้ว

หมายเหตุ: คุณยังสามารถกำหนดค่าการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) เพื่อให้ตรวจสอบใบรับรองความถูกต้องของคุณด้วย Java Card โปรแกรมอ่านลายพิมพ์นิ้วมือ หรือโทเคนก่อนจะล็อกเข้าสู่ไซต์หรือโปรแกรมที่ต้องการความปลอดภัย ลักษณะนี้มีประโยชน์มากเป็นพิเศษเมื่อกำลังล็อกเข้าสู่โปรแกรมหรือเว็บไซต์ที่มีข้อมูลส่วนบุคคล เช่นหมายเลขบัญชีธนาคาร สำหรับข้อมูลเพิ่มเติม โปรดดูที่ “การกำหนดค่าการตั้งค่า Credential Manager ในหน้า 22”

การลงทะเบียนโปรแกรมประยุกต์ใหม่

Credential Manager พร้อมต์ให้คุณลงทะเบียนโปรแกรมประยุกต์ใดๆ ที่คุณเรียกใช้ในขณะที่กำลังล็อกเข้าสู่ Credential Manager คุณยังสามารถลงทะเบียนโปรแกรมประยุกต์ด้วยตัวคุณเอง

การใช้การลงทะเบียนอัตโนมัติ

1. เปิดโปรแกรมประยุกต์ที่ระบุว่าคุณต้องล็อกเข้าใช้
2. คลิกไอคอน Credential Manager SSO ในไดอะล็อกบ์อกซ์ของโปรแกรมหรือเว็บไซต์

3. พิมพ์รหัสผ่านของคุณสำหรับโปรแกรมหรือเว็บไซต์ และคลิก **OK** ไดอะล็อกบ็อกซ์ **Credential Manager Single Sign On** จะเปิดออก
4. คลิก **More** และเลือกจากตัวเลือกต่อไปนี้:
   - ห้ามใช้ SSO สำหรับไซต์นี้หรือโปรแกรมประยุกต์นี้
   - พรอมต์ให้เลือกบัญชีสำหรับโปรแกรมประยุกต์นี้
   - กรอกรายละเอียดใบรับรองแต่ไม่ต้องแสดง
   - ตรวจสอบความถูกต้องของผู้ใช้ก่อนแสดงใบรับรอง
   - แสดงทางลัด SSO สำหรับโปรแกรมประยุกต์นี้
5. คลิก **Yes** เพื่อกรอกรายละเอียดการลงทะเบียนให้ครบถ้วน

การใช้การลงทะเบียนด้วยตัวผู้ใช้เอง (ลากและวาง)

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ให้คลิก **Single Sign On** และคลิก **Register New Application** วิซาร์ดโปรแกรมประยุกต์ SSO จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

การจัดการโปรแกรมประยุกต์และใบรับรอง

การแก้ไขคุณสมบัติของโปรแกรมประยุกต์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Single Sign On** ให้คลิก **Manage Applications and Credentials**
4. คลิกรายการโปรแกรมประยุกต์ที่คุณต้องการแก้ไข และคลิก **Properties**
5. คลิกแท็บ **General** เพื่อแก้ไขชื่อและคำอธิบายของโปรแกรมประยุกต์ เปลี่ยนแปลงการตั้งค่าได้ด้วยการเลือกหรือล้างกล่องตัวเลือกที่อยู่ติดกับการตั้งค่าที่เหมาะสม
6. คลิกแท็บ **Script** เพื่อดูและแก้ไขสคริปต์โปรแกรมประยุกต์ SSO
7. คลิก **OK**

การนำโปรแกรมประยุกต์ออกจากการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On)

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Single Sign On** ให้คลิก **Manage Applications and Credentials**
4. คลิกรายการโปรแกรมประยุกต์ที่คุณต้องการนำออก และคลิก **Remove**
5. คลิก **Yes** ในไดอะล็อกบ็อกซ์การยืนยัน
6. คลิก **OK**

การส่งออกโปรแกรมประยุกต์

คุณสามารถส่งออกโปรแกรมประยุกต์เพื่อสร้างสำเนาของข้อมูลสำรองสำหรับสคริปต์โปรแกรมประยุกต์การลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) ไฟล์นี้สามารถนำมาใช้เพื่อเรียกคืนข้อมูลการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) สิ่งนี้เปรียบเสมือนการกระทำเสริมนอกเหนือจากไฟล์สำรองข้อมูลระบุตัวตน ที่ประกอบด้วยข้อมูลใบรับรองเพียงอย่างเดียว

ในการส่งออกโปรแกรมประยุกต์:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Single Sign On** ให้คลิก **Manage Applications and Credentials**
4. คลิกรายการโปรแกรมประยุกต์ที่คุณต้องการส่งออก แล้วคลิก **More** > **Applications** > **Export Script**
5. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อส่งออกให้เสร็จสมบูรณ์
6. คลิก **OK**

การนำเข้าโปรแกรมประยุกต์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Single Sign On** ให้คลิก **Manage Applications and Credentials**
4. คลิกรายการโปรแกรมประยุกต์ที่คุณต้องการนำเข้า แล้วเลือก **More** > **Applications** > **Import Script**
5. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อนำเข้าให้เสร็จสมบูรณ์
6. คลิก **OK**

การแก้ไขใบรับรอง

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Single Sign On** ให้คลิก **Manage Applications and Credentials**
4. คลิกรายการโปรแกรมประยุกต์ที่คุณต้องการแก้ไข และคลิก **More**
5. เลือกตัวเลือกใดตัวเลือกหนึ่งดังต่อไปนี้:
   - โปรแกรมประยุกต์
     - เพิ่มใหม่
     - นำออก
     - คุณสมบัติ
     - นำเข้าสคริปต์
     - ส่งออกสคริปต์
   - ใบรับรอง
     - สร้างใหม่
   - ดูรหัสผ่าน

     หมายเหตุ: คุณต้องตรวจสอบความถูกต้องของตัวตนของคุณก่อนดูรหัสผ่าน

6. ทำตามคำแนะนำที่หน้าจอ

7. คลิก **OK**

การใช้การป้องกันโปรแกรมประยุกต์

คุณสมบัตินี้จะอนุญาตให้คุณกำหนดค่าการเข้าใช้โปรแกรมประยุกต์ คุณสามารถจำกัดการเข้าใช้โดยอิงกับเกณฑ์ต่างๆ ดังต่อไปนี้:

- ประเภทของผู้ใช้
- เวลาใช้
- การไม่มีกิจกรรมของผู้ใช้

การจำกัดการเข้าถึงโปรแกรมประยุกต์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Application Protection** คลิก **Manage Protected Applications** ไดอะล็อกบ็อกซ์ **Application Protection Service** จะเปิดออก
4. เลือกประเภทของผู้ใช้ที่มีการเข้าถึงที่คุณต้องการจัดการ

หมายเหตุ: หากประเภทของผู้ใช้เป็น Everyone หรือทุกคน คุณอาจจำเป็นต้องเลือก **Override default settings** เพื่อแทนที่การตั้งค่าสำหรับประเภทผู้ใช้เป็น Everyone หรือทุกคน

5. คลิก **Add** วิซาร์ดการเพิ่มโปรแกรมจะเปิดออก
6. ทำตามคำแนะนำที่หน้าจอ

การนำการป้องกันออกจากโปรแกรมประยุกต์

ในการนำข้อจำกัดออกจากโปรแกรมประยุกต์:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Application Protection** คลิก **Manage Protected Applications** ไดอะล็อกบ็อกซ์ **Application Protection Service** จะเปิดออก
4. เลือกประเภทของผู้ใช้ที่มีการเข้าถึงที่คุณต้องการจัดการ

หมายเหตุ: หากประเภทของผู้ใช้เป็น Everyone หรือทุกคน คุณอาจจำเป็นต้องเลือก **Override default settings** เพื่อแทนที่การตั้งค่าสำหรับประเภทผู้ใช้เป็น Everyone หรือทุกคน

5. คลิกรายการโปรแกรมประยุกต์ที่คุณต้องการนำออก และคลิก **Remove**
6. คลิก **OK**

การเปลี่ยนแปลงการตั้งค่าข้อจำกัดสำหรับโปรแกรมประยุกต์ที่มีการป้องกัน

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Services and Applications**
3. ในแผงด้านขวา ใต้ **Application Protection** คลิก **Manage Protected Applications** ไดอะล็อกบ็อกซ์ **Application Protection Service** จะเปิดออก
4. เลือกประเภทของผู้ใช้ที่มีการเข้าถึงที่คุณต้องการจัดการ

หมายเหตุ: หากประเภทของผู้ใช้เป็น Everyone หรือทุกคน คุณอาจจำเป็นต้องเลือก **Override default settings** เพื่อแทนที่การตั้งค่าสำหรับประเภทผู้ใช้เป็น Everyone หรือทุกคน

5. คลิกโปรแกรมประยุกต์ที่คุณต้องการเปลี่ยน และคลิก **Properties** ไดอะล็อกบ็อกซ์ **Properties** สำหรับโปรแกรมประยุกต์นั้นจะเปิดออก
6. คลิกแท็บ **General** เลือกการตั้งค่าใดการตั้งค่าหนึ่งดังต่อไปนี้:
   - ปิดใช้งาน (ไม่สามารถนำมาใช้ได้)
   - เปิดใช้งาน (สามารถนำมาใช้ได้โดยไม่มีข้อจำกัด)
   - จำกัด (การใช้ขึ้นอยู่กับการตั้งค่า)
7. เมื่อคุณเลือก Restricted หรือจำกัด การตั้งค่าต่อไปนี้สามารถนำมาใช้ได้:
   a. หากคุณต้องการจำกัดการใช้โดยอิงกับเวลา วันหรือวันที่ ให้คลิกแท็บ **Schedule**และกำหนดค่าการตั้งค่า
   b. หากคุณต้องการจำกัดการใช้โดยอิงอยู่กับการไม่มีกิจกรรม ให้คลิกแท็บ **Advanced** และเลือกช่วงเวลาที่ไม่มีกิจกรรม
8. คลิก **OK** เพื่อเปิดไดอะล็อกบ็อกซ์ **Properties** ของโปรแกรมประยุกต์
9. คลิก **OK**

งานขั้นสูง (ผู้ดูแลระบบเท่านั้น)

หน้า “Authentication and Credentials” และหน้า “Advanced Settings” ของ Credential Manager จะนำมาใช้ได้เฉพาะกับผู้ใช้ที่มีสิทธิ์ของผู้ดูแลระบบ สำหรับหน้าต่างๆ เหล่านี้ คุณสามารถทำงานต่างๆ ดังต่อไปนี้:

- การระบุถึงวิธีการล็อกออนของผู้ใช้และผู้ดูแลระบบ
- การกำหนดค่าข้อกำหนดการตรวจสอบความถูกต้องแบบเลือกกำหนดเอง
- การกำหนดค่าคุณสมบัติใบรับรอง
- การกำหนดค่าการตั้งค่า Credential Manager

การระบุถึงวิธีการล็อกออนของผู้ใช้และผู้ดูแลระบบ

บนหน้า “Authentication and Credentials” คุณสามารถระบุประเภทของใบรับรองหรือใบรับรองประเภทต่างๆ ที่จำเป็นสำหรับผู้ใช้หรือผู้ดูแลระบบ

ในการระบุถึงวิธีการล็อกออนของผู้ใช้และผู้ดูแลระบบ:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** และคลิก **Authentication and Credentials**
3. ในแผงด้านขวา ให้คลิกแท็บ **Authentication**
4. คลิกประเภท (**Users** หรือ **Administrators**) จากรายการประเภท
5. คลิกวิธีการตรวจสอบความถูกต้องประเภทหนึ่งหรือหลายๆ ประเภทจากรายการ
6. คลิก **Apply** และคลิก **OK**

การกำหนดค่าข้อกำหนดการตรวจสอบความถูกต้องแบบเลือกกำหนดเอง

หากชุดของใบรับรองการตรวจสอบความถูกต้องที่คุณต้องการไม่ได้อยู่ในรายการบนแท็บการตรวจสอบความถูกต้องของหน้า “Authentication and Credentials” คุณสามารถระบุข้อกำหนดที่เลือกกำหนดเอง

ในการกำหนดค่าข้อกำหนดแบบเลือกกำหนดเอง:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** และคลิก **Authentication and Credentials**
3. ในแผงด้านขวา ให้คลิกแท็บ **Authentication**
4. คลิกประเภท (**Users** หรือ **Administrators**) จากรายการประเภท
5. คลิก **Custom** ในรายการวิธีการตรวจสอบความถูกต้อง
6. คลิก **Configure**
7. เลือกวิธีการตรวจสอบความถูกต้องที่คุณต้องการ
8. เลือกวิธีการต่างๆ รวมกันได้ด้วยการคลิกหนึ่งในตัวเลือกต่อไปนี้:
   - ใช้ AND เพื่อรวมวิธีการตรวจสอบความถูกต้อง

     (ผู้ใช้จะต้องตรวจสอบความถูกต้องกับวิธีการต่างๆ ที่คุณเลือกทุกครั้งที่ผู้ใช้ล็อกออน)
   - ใช้ OR เพื่อกำหนดให้ใช้วิธีการตรวจสอบความถูกต้องหนึ่งในสองวิธีหรือมากกว่านั้น

     (ผู้ใช้จะสามารถเลือกวิธีใดๆ ที่เลือกไว้แล้วทุกครั้งที่ผู้ใช้ล็อกออน)

9. คลิก **OK**
10. คลิก **Apply** และคลิก **OK**

การกำหนดค่าคุณสมบัติใบรับรอง

บนแท็บใบรับรองของหน้า “Authentication and Credentials” คุณสามารถดูรายการวิธีการตรวจสอบความถูกต้องที่นำมาใช้ได้ และแก้ไขการตั้งค่า

ในการกำหนดค่าใบรับรอง:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** และคลิก **Authentication and Credentials**
3. ในแผงด้านขวา ให้คลิกแท็บ **Credentials**
4. คลิกประเภทของใบรับรองที่คุณต้องการแก้ไข คุณสามารถแก้ไขใบรับรองโดยใช้หนึ่งในตัวเลือกต่างๆ ต่อไปนี้:
   - ในการลงทะเบียนใบรับรอง ให้คลิก **Register** และทำตามคำแนะนำบนหน้าจอ
   - ในการลบใบรับรอง ให้คลิก **Clear** และคลิก **Yes** ในไดอะล็อกบ็อกซ์การยืนยัน
   - ในการแก้ไขคุณสมบัติของใบรับรอง ให้คลิก **Properties** และคลิกจากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ
5. คลิก **Apply** และคลิก **OK**

การกำหนดค่าการตั้งค่า Credential Manager

จากหน้า “Settings” คุณสามารถเข้าถึงและแก้ไขการตั้งค่าต่างๆ โดยใช้แท็บต่างๆ ดังต่อไปนี้:

- ทั่วไป–อนุญาตให้คุณแก้ไขการตั้งค่าสำหรับการกำหนดค่าขั้นพื้นฐาน
- การลงชื่อเข้าใช้เพียงครั้งเดียว–อนุญาตให้คุณแก้ไขการตั้งค่าวิธีการทำงานของการลงชื่อเข้าใช้เพียงครั้งเดียวสำหรับผู้ใช้ปัจจุบัน เช่น วิธีการจัดการกับการตรวจหาหน้าจอการล็อกออน การล็อกออนอัตโนมัติไปยังไดอะล็อกการล็อกออนที่ลงทะเบียนแล้ว และหน้าจอรหัสผ่าน
- บริการและโปรแกรมประยุกต์–อนุญาตให้คุณดูบริการที่มีอยู่และแก้ไขการตั้งค่าสำหรับบริการเหล่านั้น
- ความปลอดภัย–อนุญาตให้คุณเลือกซอฟต์แวร์อ่านลายพิมพ์นิ้วมือ และปรับระดับความปลอดภัยของโปรแกรมอ่านลายพิมพ์นิ้วมือ
- สมาร์ทการ์ดและโทเคน–อนุญาตให้คุณดูและแก้ไขคุณสมบัติสำหรับ Java Cards และโทเคนที่มีอยู่ทั้งหมด

ในการแก้ไขการตั้งค่า Credential Manager:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Settings**
3. ในแผงด้านขวา ให้คลิกแท็บที่เหมาะสมสำหรับการตั้งค่าที่คุณต้องการแก้ไข
4. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อแก้ไขการตั้งค่า
5. คลิก **Apply** และคลิก **OK**

ตัวอย่างที่ 1–การใช้หน้า “Advanced Settings” เพื่ออนุญาตให้ล็อกออน Windows จาก Credential Manager

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Settings**
3. ในแผงด้านขวา ให้คลิกแท็บ **General**

4. ใต้ **Select the way users log on to Windows (requires restart)** ให้เลือกกล่องตัวเลือก **Use Credential Manager with classic logon prompt**
5. คลิก **Apply** และคลิก **OK**
6. เริ่มการทำงานของคอมพิวเตอร์ใหม่

หมายเหตุ: การเลือกกล่องตัวเลือก **Use Credential Manager with classic logon prompt** จะอนุญาตให้คุณล็อคคอมพิวเตอร์ ดูที่ “การล็อคคอมพิวเตอร์ ในหน้า 15”

ตัวอย่างที่ 2–การใช้หน้า “Advanced Settings” ระบุว่าต้องมีการตรวจสอบผู้ใช้ก่อนการลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On)

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Credential Manager** จากนั้นคลิก **Settings**
3. ในแผงด้านขวา ให้คลิกแท็บ **Single Sign On**
4. ใต้ **When registered logon dialog or Web page is visited** เลือกกล่องตัวเลือก **Authenticate user before submitting credentials**
5. คลิก **Apply** และคลิก **OK**
6. เริ่มการทำงานของคอมพิวเตอร์ใหม่

3 Embedded Security สำหรับ HP ProtectTools

หมายเหตุ: ต้องติดตั้งชิปความปลอดภัย Trusted Platform Module (TPM) แบบฝังตัวในคอมพิวเตอร์เพื่อใช้ Embedded Security สำหรับ HP ProtectTools

Embedded Security สำหรับ HP ProtectTools ช่วยป้องกันการลักลอบเข้าใช้ข้อมูลผู้ใช้หรือใบรับรอง:โมดูลซอฟต์แวร์นี้มีคุณสมบัติด้านความปลอดภัยดังต่อไปนี้:

- การเข้ารหัสไฟล์และโฟลเดอร์ด้วย Enhanced Microsoft® Encrypting File System (EFS)
- การสร้างไดรฟ์ความปลอดภัยส่วนบุคคล (PSD) สำหรับป้องกันข้อมูลผู้ใช้ในไดรฟ์ที่ซ่อน
- ฟังก์ชันการจัดการข้อมูล เช่น การสำรองข้อมูลและการเรียกคืนลำดับชั้นของคีย์
- สนับสนุนโปรแกรมประยุกต์ของบริษัทภายนอก (เช่น Microsoft Outlook และ Internet Explorer) สำหรับการดำเนินการด้วยใบรับรองดิจิตอลที่มีการป้องกันเมื่อใช้ซอฟต์แวร์ Embedded Security

ชิปความปลอดภัย TPM แบบภายในจะช่วยยกระดับและเปิดการทำงานของคุณสมบัติอื่นๆ ของ HP ProtectTools Security Manager ตัวอย่างเช่น Credential Manager สำหรับ HP ProtectTools สามารถใช้ชิปภายในเป็นวิธีการตรวจสอบความถูกต้องเมื่อผู้ใช้ล็อกเข้าสู่ Windows บนรุ่นที่เลือก ชิปความปลอดภัย TPM แบบภายในยังจะเปิดการทำงานของคุณสมบัติด้านความปลอดภัย BIOS ขั้นสูง ที่เข้าถึงได้ผ่านการกำหนดค่า BIOS สำหรับ HP ProtectTools

ขั้นตอนการติดตั้ง

△ **ข้อควรระวัง:** เพื่อลดความเสี่ยงด้านความปลอดภัย ขอแนะนำให้ผู้ดูแลระบบไอทีของคุณเริ่มต้นการทำงานของชิปความปลอดภัยภายในในทันที การไม่สามารถเริ่มต้นชิปความปลอดภัยภายในอาจทำให้ผู้ใช้อื่นลักลอบเข้ามาใช้เครื่อง เกิดเวิร์มคอมพิวเตอร์ หรือไวรัสแพร่ระบาดในคอมพิวเตอร์และควบคุมงานของเจ้าของ เช่น การจัดการแหล่งจัดเก็บการเรียกคืนฉุกเฉิน และการกำหนดค่าการตั้งค่าการเข้าถึงของผู้ใช้

ปฏิบัติตามขั้นตอนในส่วนที่ 2 ต่อไปนี้เพื่อเปิดใช้งานและเริ่มต้นชิปความปลอดภัยภายใน

การเปิดใช้งานชิปความปลอดภัยภายใน

ต้องเปิดใช้งานชิปความปลอดภัยภายในในยูทิลิตีการตั้งค่าคอมพิวเตอร์ ไม่สามารถทำขั้นตอนนี้ในการกำหนดค่า BIOS สำหรับ HP ProtectTools

ในการเปิดใช้งานชิปความปลอดภัยภายใน:

1. เข้าใช้การตั้งค่าคอมพิวเตอร์โดยการเปิดหรือรีสตาร์ทเครื่องคอมพิวเตอร์ แล้วจากนั้นกด F10 ในขณะที่ข้อความ “F10 = ROM Based Setup” แสดงอยู่ที่มุมด้านล่างซ้ายของหน้าจอ
2. หากคุณไม่ได้ตั้งรหัสผ่านสำหรับผู้ดูแลระบบ ให้ใช้ปุ่มลูกศรเพื่อเลือก **Security** > **Setup password** และกด enter
3. พิมพ์รหัสผ่านของคุณลงในช่อง **New password** และ **Verify new password** และกด F10
4. ในเมนู **Security** ให้ใช้ปุ่มลูกศรเพื่อเลือก **TPM Embedded Security** และกด enter
5. ใต้ **Embedded Security** หากอุปกรณ์ถูกซ่อนไว้ เลือก **Available**
6. เลือก **Embedded security device state** และเปลี่ยนเป็น **Enable**
7. กด F10 เพื่อยอมรับการเปลี่ยนแปลงการกำหนดค่า Embedded Security
8. ในการบันทึกการกำหนดลักษณะของคุณและออกจากการตั้งค่าคอมพิวเตอร์ ให้ใช้ปุ่มลูกศรเพื่อเลือก **File** > **Save Changes and Exit** แล้วปฏิบัติตามคำแนะนำบนหน้าจอ

การเริ่มต้นการทำงานของชิปความปลอดภัยภายใน

ในขั้นตอนการเริ่มต้นการทำงานสำหรับ Embedded Security คุณจะได้ทำงานต่างๆ ดังต่อไปนี้:

- ตั้งรหัสผ่านของผู้เป็นเจ้าของสำหรับชิปความปลอดภัยภายในที่ป้องกันการเข้าถึงฟังก์ชันทั้งหมดของผู้เป็นเจ้าของบนชิปความปลอดภัยภายใน
- ตั้งค่าแหล่งจัดเก็บการเรียกคืนฉุกเฉิน ซึ่งคือส่วนการจัดเก็บที่ได้รับการป้องกัน และอนุญาตให้มีการเข้ารหัสคีย์ผู้ใช้เบื้องต้นสำหรับผู้ใช้ทุกคนซ้ำอีกครั้ง

ในการเริ่มต้นการทำงานของชิปความปลอดภัยภายใน:

1. คลิกขวาที่ไอคอน HP ProtectTools Security Manager ในเนื้อที่ประกาศ ที่ด้านขวาสุดของแถบงาน และเลือก **Embedded Security Initialization**

   วิซาร์ดการเริ่มต้นการทำงานของ HP ProtectTools Embedded Security จะเปิดออก
2. ทำตามคำแนะนำที่หน้าจอ

การตั้งค่าบัญชีผู้ใช้เบื้องต้น

การตั้งค่าบัญชีผู้ใช้เบื้องต้นใน Embedded Security ประกอบด้วยการทำงานต่างๆ ดังต่อไปนี้:

- สร้างคีย์ผู้ใช้เบื้องต้นที่ป้องกันข้อมูลที่ถูกเข้ารหัสไว้ และตั้งรหัสผ่านของคีย์ผู้ใช้เบื้องต้นเพื่อป้องกันคีย์ผู้ใช้เบื้องต้น
- ตั้งค่าไดรฟ์ความปลอดภัยส่วนบุคคล (PSD) สำหรับจัดเก็บไฟล์และโฟลเดอร์ที่ถูกเข้ารหัส

△ **ข้อควรระวัง:** ปกป้องรหัสผ่านของคีย์ผู้ใช้เบื้องต้น ข้อมูลที่เข้ารหัสจะไม่สามารถเข้าถึงหรือกู้คืนได้หากไม่มีรหัสผ่านนี้

ในการตั้งค่าบัญชีผู้ใช้เบื้องต้นและเปิดใช้คุณสมบัติความปลอดภัยของผู้ใช้:

1. หากวิซาร์ดการเริ่มต้นการทำงานของ Embedded Security User ไม่เปิดออก ให้เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **User Settings**
3. ในแผงด้านขวา ใต้ **Embedded Security Features** คลิก **Configure**

   วิซาร์ดการเริ่มต้นการทำงานของ Embedded Security User จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

หมายเหตุ: ในการใช้อีเมลที่ปลอดภัย คุณจะต้องกำหนดค่าไคลเอนต์อีเมลให้ใช้ใบรับรองดิจิตอลที่สร้างด้วย Embedded Security เสียก่อน หากไม่มีใบรับรองดิจิตอล คุณก็สามารถขอรับใบรับรองได้จากหน่วยงานออกใบรับรอง (Certification Authority) สำหรับคำแนะนำเกี่ยวกับการกำหนดค่าอีเมลของคุณและการขอรับใบรับรองดิจิตอล โปรดดูวิธีใช้ออนไลน์ของไคลเอนต์อีเมล

งานทั่วไป

หลังจากตั้งค่าบัญชีผู้ใช้เบื้องต้นแล้ว คุณสามารถทำงานต่างๆ ดังต่อไปนี้:

- การเข้ารหัสไฟล์และโฟลเดอร์:
- การส่งและรับอีเมลที่เข้ารหัส

การใช้ไดรฟ์ความปลอดภัยส่วนบุคคล

หลังจากตั้งค่า PSD แล้ว คุณจะถูกพรอมต์ให้พิมพ์รหัสผ่านของคีย์ผู้ใช้เบื้องต้นเมื่อล็อกออนครั้งต่อไป หากป้อนรหัสผ่านของคีย์ผู้ใช้เบื้องต้นได้ถูกต้อง คุณจะสามารถเข้าสู่ PSD ได้โดยตรงจาก Windows Explorer

การเข้ารหัสไฟล์และโฟลเดอร์:

เมื่อทำงานกับไฟล์ที่ถูกเข้ารหัส ให้พิจารณากฎเกณฑ์ดังต่อไปนี้:

- สามารถเข้ารหัสได้เฉพาะไฟล์และโฟลเดอร์บนพาร์ติชัน Windows เท่านั้น ไม่สามารถเข้ารหัสไฟล์และโฟลเดอร์บนพาร์ติชัน MS-DOS
- ไม่สามารถเข้ารหัสไฟล์ระบบและไฟล์ที่ถูกบีบอัด และไฟล์ที่เข้ารหัสจะไม่สามารถบีบอัดได้
- ควรเข้ารหัสโฟลเดอร์ชั่วคราว เนื่องจากไฟล์ชั่วคราวมักจะเป็นตกเป็นเป้าของผู้โจมตี
- นโยบายการกู้คืนจะถูกตั้งค่าโดยอัตโนมัติ เมื่อคุณเข้ารหัสไฟล์หรือโฟลเดอร์เป็นครั้งแรก กฎเกณฑ์นี้จะช่วยให้แน่ใจว่าหากคุณสูญเสียใบรับรองการเข้ารหัสและคีย์ส่วนตัว คุณจะสามารถใช้เอเจนต์การกู้คืนเพื่อถอดรหัสข้อมูลของคุณ

ในการเข้ารหัสไฟล์และโฟลเดอร์:

1. คลิกขวาที่ไฟล์หรือโฟลเดอร์ที่คุณต้องการเข้ารหัส
2. คลิก **Encrypt**
3. คลิกเลือกตัวเลือกใดตัวเลือกหนึ่งดังต่อไปนี้:
   - **นำการเปลี่ยนแปลงมาใช้กับโฟลเดอร์นี้เท่านั้น**
   - **นำการเปลี่ยนแปลงมาใช้กับโฟลเดอร์นี้ โฟลเดอร์ย่อยนี้และไฟล์นี้**
4. คลิก **OK**

การส่งและรับอีเมลที่เข้ารหัส

Embedded Security ช่วยให้คุณส่งและรับอีเมลที่เข้ารหัสไว้ แต่ขั้นตอนอาจแตกต่างกันโดยขึ้นอยู่กับโปรแกรมที่คุณใช้เข้าสู่อีเมลของคุณ สำหรับข้อมูลเพิ่มเติม โปรดดูที่วิธีใช้ออนไลน์ของ Embedded Security และวิธีใช้ออนไลน์สำหรับอีเมลของคุณ

การเปลี่ยนแปลงรหัสผ่านของคีย์ผู้ใช้เบื้องต้น

ในการเปลี่ยนแปลงรหัสผ่านของคีย์ผู้ใช้เบื้องต้น:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **User Settings**
3. ในแผงด้านขวา ใต้ **Basic User Key password** คลิก **Change**
4. พิมพ์รหัสผ่านตัวเดิม ก่อนตั้งและยืนยันรหัสผ่านตัวใหม่
5. คลิก **OK**

การทำงานขั้นสูง

การสำรองข้อมูลและการเรียกคืน

คุณสมบัติการสำรองข้อมูลของ Embedded Security จะสร้างแหล่งจัดเก็บที่ประกอบด้วยข้อมูลการรับรองที่จะถูกเรียกคืนในกรณีที่เกิดเหตุฉุกเฉิน

การสร้างไฟล์สำรองข้อมูล

ในการสร้างไฟล์สำรองข้อมูล:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **Backup**
3. ในแผงด้านขวา ให้คลิก **Backup** วิซาร์ดการสำรองข้อมูลของ Embedded Security จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

การเรียกคืนข้อมูลการรับรองจากไฟล์สำรองข้อมูล

ในการเรียกคืนข้อมูลจากไฟล์สำรองข้อมูล:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **Backup**
3. ในแผงด้านขวา ให้คลิก **Restore** วิซาร์ดการสำรองข้อมูลของ Embedded Security จะเปิดออก
4. ทำตามคำแนะนำที่หน้าจอ

การเปลี่ยนรหัสผ่านของผู้เป็นเจ้าของ

ในการเปลี่ยนรหัสผ่านของผู้เป็นเจ้าของ:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **Advanced**
3. ในแผงด้านขวา ใต้ **Owner Password** คลิก **Change**
4. พิมพ์รหัสผ่านตัวเดิมของผู้เป็นเจ้าของ ก่อนตั้งและยืนยันรหัสผ่านตัวใหม่ของผู้เป็นเจ้าของ
5. คลิก **OK**

การรีเซ็ตรหัสผ่านผู้ใช้

ผู้ดูแลระบบสามารถช่วยผู้ใช้รีเซ็ตรหัสผ่านที่ผู้ใช้ลืม สำหรับข้อมูลเพิ่มเติม โปรดดูที่วิธีใช้แบบออนไลน์

การเปิดใช้งานและการปิดใช้งาน Embedded Security

มีความเป็นไปได้ที่จะปิดใช้งานคุณสมบัติ Embedded Security หากคุณต้องการทำงานโดยไม่ใช้ฟังก์ชันความปลอดภัย

คุณสมบัติของ Embedded Security สามารถเปิดใช้งานหรือปิดใช้งานได้ใน 2 ระดับที่แตกต่างกัน:

- การปิดใช้งานชั่วคราว–เมื่อใช้ตัวเลือกนี้ ความปลอดภัยภายในจะถูกเปิดใช้งานอีกครั้งโดยอัตโนมัติเมื่อรีสตาร์ท Windows ตัวเลือกนี้นำมาใช้ได้กับผู้ใช้ทุกคนตั้งแต่เริ่มต้น
- การปิดใช้งานถาวร–เมื่อใช้ตัวเลือกนี้ จำเป็นต้องใช้รหัสผ่านของผู้เป็นเจ้าของเพื่อเปิดใช้งาน Embedded Security อีกครั้ง ตัวเลือกนี้นำมาใช้ได้เฉพาะผู้ที่เป็นผู้ดูแลระบบ

การปิดใช้งาน Embedded Security เป็นการถาวร

ในการปิดใช้งาน Embedded Security เป็นการถาวร:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **Advanced**
3. ในแผงด้านขวา ใต้ **Embedded Security Features** คลิก **Disable**
4. พิมพ์รหัสผ่านของผู้เป็นเจ้าของเมื่อพรอมต์ และคลิก **OK**

การเปิดใช้งาน Embedded Security หลังจากปิดใช้งานอย่างถาวร

ในการเปิดใช้งาน Embedded Security หลังจากปิดใช้งานอย่างถาวร:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Embedded Security** และคลิก **Advanced**
3. ในแผงด้านขวา ใต้ **Embedded Security Features** คลิก **Enable**
4. พิมพ์รหัสผ่านของผู้เป็นเจ้าของเมื่อพรอมต์ และคลิก **OK**

การเปลี่ยนย้ายคีย์โดยใช้วิซาร์ดการเปลี่ยนย้าย

การเปลี่ยนย้ายเป็นงานขั้นสูงของผู้ดูแลระบบซึ่งช่วยให้สามารถจัดการ กู้คืน และถ่ายโอนคีย์และใบรับรอง สำหรับรายละเอียดเกี่ยวกับการเปลี่ยนย้าย โปรดดูวิธีใช้แบบออนไลน์ของ Embedded Security

4 Java Card Security สำหรับ HP ProtectTools

Java Card Security สำหรับ HP ProectTools จัดการการตั้งค่า Java Card และการกำหนดค่าสำหรับใช้งานร่วมกับแป้นพิมพ์ HP Smart Card ทั้งนี้ Java Card ของ HP เป็นอุปกรณ์ความปลอดภัยส่วนบุคคลที่ปกป้องข้อมูลการตรวจสอบความถูกต้อง ซึ่งต้องใช้ทั้งการ์ดและรหัส PIN เพื่อให้สามารถเข้าใช้งาน เหมือนกับการใช้บัตร ATM และรหัส PIN Java Card สามารถใช้ในการเข้าใช้งาน Credential Manager, Drive Encryption, HP BIOS หรือจุดเข้าใช้งานใดๆ ของผู้ผลิตรายอื่น

เมื่อใช้ความปลอดภัยของ Java Card คุณสามารถทำงานต่างๆ ต่อไปนี้:

- เข้าสู่คุณสมบัติด้านความปลอดภัยของ Java Card
- ทำงานกับยูทิลิตีการตั้งค่าคอมพิวเตอร์เพื่อเปิดใช้งานการตรวจสอบความถูกต้องของ Java Card ในขณะที่เปิดเครื่อง
- กำหนดค่า Java Cards เฉพาะสำหรับผู้ดูแลระบบและผู้ใช้ ผู้ใช้ต้องใส่ Java Card และพิมพ์รหัส PIN ก่อนที่ระบบปฏิบัติการจะโหลด
- ตั้งและเปลี่ยนรหัส PIN ที่นำมาใช้ตรวจสอบความถูกต้องของผู้ใช้ Java Card

งานทั่วไป

หน้า “General” อนุญาตให้คุณทำงานต่างๆ ดังต่อไปนี้:

- เปลี่ยนรหัส PIN ของ Java Card
- เลือกตัวอ่านการ์ดหรือแป้นพิมพ์ของสมาร์ทการ์ด

หมายเหตุ: ตัวอ่านการ์ดใช้ทั้ง Java Cards และสมาร์ทการ์ด คุณสมบัตินี้นำมาใช้ได้เฉพาะเมื่อคุณมีตัวอ่านการ์ดมากกว่าหนึ่งตัวอยู่บนคอมพิวเตอร์

การเปลี่ยนรหัส PIN ของ Java Card

ในการเปลี่ยนรหัส PIN ของ Java Card

หมายเหตุ: รหัส PIN ของ Java Card PIN ต้องมีอักขระที่เป็นตัวเลข 4 และ 8 ตัว

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **General**
3. ใส่ Java Card (พร้อมรหัส PIN ที่มีอยู่) ลงในตัวอ่านการ์ด
4. ในแผงด้านขวา ให้คลิก **Change**
5. ในไดอะล็อกบ็อกซ์ **Change PIN** ให้พิมพ์รหัส PIN ปัจจุบันลงในกล่อง **Current PIN**
6. พิมพ์รหัส PIN ใหม่ลงในกล่อง **New PIN** และพิมพ์รหัส PIN อีกครั้งลงในกล่อง **Confirm New PIN**
7. คลิก **OK**

การเลือกตัวอ่านการ์ด

ดูให้แน่ใจว่า ได้เลือกตัวอ่านการ์ดที่ถูกต้องในความปลอดภัยของ Java Card ก่อนใช้ Java Card หากไม่ได้เลือกตัวอ่านที่ถูกต้อง คุณสมบัติบางอย่างอาจไม่ทำงานหรือแสดงผลไม่ถูกต้อง นอกจากนั้น ไดรเวอร์ตัวอ่านการ์ดต้องได้รับการติดตั้งอย่างเหมาะสม เช่นที่แสดงไว้ในตัวจัดการอุปกรณ์ของ Windows

ในการเลือกตัวอ่านการ์ด:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **General**
3. ใส่ Java Card ลงในตัวอ่านการ์ด
4. ในแผงด้านขวา ใต้ **Selected card reader** ให้คลิกตัวอ่านที่ถูกต้อง

งานขั้นสูง (ผู้ดูแลระบบเท่านั้น)

หน้า “Advanced” อนุญาตให้คุณทำงานต่างๆ ดังต่อไปนี้:

- มอบหมายรหัส PIN ของ Java Card
- ตั้งชื่อให้กับ Java Card
- ตั้งการตรวจสอบความถูกต้องเมื่อเปิดเครื่องไว้
- การสำรองข้อมูลและการเรียกคืน Java Cards

หมายเหตุ: คุณต้องมีเอกสิทธิ์ของผู้ดูแลระบบ Windows เพื่อแสดงผลหน้า "Advanced"

การกำหนดรหัส PIN ของ Java Card:

คุณต้องกำหนดชื่อและรหัส PIN ให้กับ Java Card ก่อนที่จะนำการ์ดนั้นมาใช้ในความปลอดภัยของ Java Card

ในการกำหนดรหัส PIN ของ Java Card:

หมายเหตุ: รหัส PIN ของ Java Card PIN ต้องมีอักขระที่เป็นตัวเลข 4 และ 8 ตัว

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **Advanced**
3. ใส่ Java Card ใหม่ลงในตัวอ่านการ์ด
4. เมื่อไดอะล็อกบ็อกซ์ **New Card** เปิด ให้พิมพ์ชื่อใหม่ลงในกล่อง **New display name** พิมพ์รหัส PIN ใหม่ลงในกล่อง **New PIN** และพิมพ์รหัส PIN ใหม่ลงในกล่อง **Confirm New PIN** อีกครั้ง
5. คลิก **OK**

การตั้งชื่อให้กับ Java Card

คุณต้องตั้งชื่อให้กับ Java Card ก่อนที่จะนำการ์ดนั้นตรวจสอบความถูกต้องเมื่อเปิดเครื่อง

ในการตั้งชื่อให้กับ Java Card:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **Advanced**
3. ใส่ Java Card ลงในตัวอ่านการ์ด

   หมายเหตุ: หากคุณไม่ได้ตั้งรหัส PIN สำหรับการ์ดนี้ ไดอะล็อกบ็อกซ์ **New Card** จะเปิดออก เพื่อให้คุณพิมพ์ชื่อและรหัส PIN ใหม่
4. ในแผงด้านขวา ใต้ **Display name** คลิก **Change**
5. พิมพ์ชื่อสำหรับ Java Card ลงในกล่อง **Name**
6. พิมพ์รหัส PIN ปัจจุบันสำหรับ Java Card ลงในกล่อง **PIN**
7. คลิก **OK**

การตั้งการตรวจสอบความถูกต้องเมื่อเปิดเครื่องไว้

เมื่อเปิดใช้งาน การตรวจสอบความถูกต้องเมื่อเปิดเครื่องใช้จะระบุให้คุณใช้ Java Card เพื่อเริ่มต้นคอมพิวเตอร์

ขั้นตอนการเปิดใช้งานการตรวจสอบความถูกต้องเมื่อเปิดเครื่องด้วย Java Card เกี่ยวข้องกับขั้นตอนต่างๆ ดังต่อไปนี้:

1. เปิดใช้งานการสนับสนุนการตรวจสอบความถูกต้องเมื่อเปิดเครื่องด้วย Java Card ในการกำหนดค่า BIOs หรือการตั้งค่าคอมพิวเตอร์
2. เปิดใช้งานรองรับการตรวจสอบเมื่อเปิดเครื่องด้วย Java Card ในความปลอดภัย Java Card
3. สร้างและเปิดใช้งาน Java Card ของผู้ดูแลระบบ

การเปิดใช้งานการตรวจสอบความถูกต้องเมื่อเปิดเครื่องด้วย Java Card และการสร้าง Java Card สำหรับผู้ดูแลระบบ

ในการเปิดใช้งานการตรวจสอบความถูกต้องเมื่อเปิดเครื่องไว้ด้วย Java Card:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **Advanced**
3. ใส่ Java Card ลงในตัวอ่านการ์ด

หมายเหตุ: หากคุณไม่ได้ตั้งชื่อและรหัส PIN สำหรับการ์ดนี้ ไดอะล็อกบ็อกซ์ **New Card** จะเปิดออก เพื่อให้คุณพิมพ์ชื่อและรหัส PIN ใหม่

4. ในแผงด้านขวา ใต้ **Power-on authentication** เลือกกล่องตัวเลือก **Enable**
5. พิมพ์รหัสผ่านการตั้งค่าคอมพิวเตอร์ของคุณลงในไดอะล็อกบ็อกซ์ **Computer Setup Password** และคลิก **OK**
6. หากคุณไม่ได้เปิดใช้งาน DriveLock ไว้แล้ว ให้พิมพ์รหัส PIN ของ Java Card และคลิก **OK**

   - หรือ -

   หากคุณเปิดใช้งาน DriveLock ไว้แล้ว:

   a. คลิก **Make Java card identity unique**

      - หรือ -

      คลิก **Make the Java card identity the same as the DriveLock password**

   หมายเหตุ: หาก DriveLock เปิดใช้งานบนคอมพิวเตอร์ คุณสามารถตั้งตัวตนของ Java Card ให้เหมือนกับรหัสผ่านผู้ใช้ DriveLock ซึ่งจะอนุญาตให้คุณตรวจสอบความถูกต้องของทั้ง DriveLock และ Java Card ได้โดยใช้เฉพาะ Java Card เมื่อเริ่มต้นคอมพิวเตอร์

   b. หากเหมาะสม ให้พิมพ์รหัสผ่านผู้ใช้ DriveLock ลงในกล่อง **DriveLock password** และพิมพ์รหัสผ่านตัวเดียวกันนี้ลงในกล่อง **Confirm password**

   c. พิมพ์รหัส PIN ของ Java Card

   d. คลิก **OK**

7. เมื่อคุณถูกพรอมต์ให้สร้างไฟล์การกู้คืน ให้คลิก **Cancel** เพื่อสร้างไฟล์การกู้คืนในภายหลัง หรือคลิก **OK** และทำตามคำแนะนำบนหน้าจอในวิซาร์ดการสำรองข้อมูล HP ProtectTools เพื่อสร้างไฟล์การกู้คืนในตอนนี้

หมายเหตุ: สำหรับข้อมูลเพิ่มเติม ดูที่ “การสำรองข้อมูลและการเรียกคืน HP ProtectTools ในหน้า 8”

การสร้าง Java Card ของผู้ใช้

หมายเหตุ: การตรวจสอบความถูกต้องเมื่อเปิดเครื่องและการ์ดของผู้ดูแลระบบจะต้องถูกตั้งค่าเพื่อสร้าง Java Card ของผู้ใช้

ในการสร้าง Java Card ของผู้ใช้:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **Advanced**
3. ใส่ Java Card ที่จะนำมาใช้เป็นการ์ดของผู้ใช้
4. ในแผงด้านขวา ใต้ **Power-on authentication** คลิก **Create** ถัดจาก **User card identity**
5. พิมพ์รหัส PIN สำหรับผู้ใช้ Java Card และจากนั้นคลิก **OK**

การปิดใช้งานการตรวจสอบความถูกต้องเมื่อเปิดเครื่องไว้ด้วย Java Card

เมื่อคุณปิดใช้งานการตรวจสอบความถูกต้องเมื่อเปิดเครื่องด้วย Java Card คุณก็ไม่จำเป็นต้องใช้ Java Card เพื่อเข้าถึงคอมพิวเตอร์อีกต่อไป

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย คลิก **Java Card Security** และคลิก **Advanced**
3. ใส่ Java Card ของผู้ดูแลระบบ
4. ในแผงด้านขวา ใต้ **Power-on authentication** ให้ล้างกล่องตัวเลือก **Enable**
5. พิมพ์รหัส PIN สำหรับ Java Card และจากนั้นคลิก **OK**

5 การกำหนดค่า BIOS สำหรับ HP ProtectTools

การกำหนดค่า BIOS สำหรับ HP ProtectTools ช่วยให้คุณสามารถเข้าใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์และการกำหนดค่าความปลอดภัย ซึ่งให้ผู้ใช้ Windows สามารถเข้าใช้คุณลักษณะด้านความปลอดภัยของระบบที่ถูกจัดการด้วยยูทิลิตีการตั้งค่าคอมพิวเตอร์ ตัวเลือกภายในการกำหนดค่า BIOS สำหรับ HP ProtectTools ได้แก่:

- File
- Storage
- Security
- Power
- Advanced

หมายเหตุ: การสนับสนุนสำหรับตัวเลือกการตั้งค่าคอมพิวเตอร์โดยเฉพาะ อาจแตกต่างกันไปขึ้นอยู่กับข้อมูลการตั้งค่าของฮาร์ดแวร์เฉพาะ

การกำหนดค่า BIOS อนุญาตให้คุณจัดการกับการตั้งค่าต่างๆ ของคอมพิวเตอร์ที่อาจเข้าถึงได้เฉพาะด้วยการกด F10 เมื่อเริ่มต้นใช้งานหรือเข้าสู่การตั้งค่าคอมพิวเตอร์ เมื่อใช้การกำหนดค่า BIOS คุณสามารถตามวัตถุประสงค์ต่างๆ ต่อไปนี้:

- จัดการรหัสผ่านเมื่อเปิดเครื่องและรหัสผ่านของผู้ดูแลระบบ
- กำหนดค่าคุณสมบัติอื่นๆ ของการตรวจสอบความถูกต้องเมื่อเปิดเครื่อง เช่น การเปิดใช้งานการสนับสนุนการตรวจสอบความถูกต้องด้วยความปลอดภัยภายใน
- เปิดใช้งานและปิดใช้งานคุณสมบัติฮาร์ดแวร์ เช่น การบูตจากสื่อที่ถอดออกได้ หรือพอร์ตฮาร์ดแวร์อื่น
- กำหนดค่าตัวเลือกการบูต ซึ่งรวมถึงการเปิดใช้งาน MultiBoot และการเปลี่ยนลำดับการบูต

หมายเหตุ: คุณสมบัติทั้งหมดของการกำหนดค่า BIOS สำหรับ HP ProtectTools สามารถใช้ได้จากการตั้งค่า F10 สำหรับคำแนะนำโดยละเอียดเกี่ยวกับการใช้การตั้งค่า F10 โปรดดูที่ คู่มือยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) ซึ่งมาพร้อมกับเครื่องคอมพิวเตอร์หรืออัพเดต BIOS

File

ตัวเลือก File ภายในการกำหนดค่า BIOS สำหรับ HP ProtectTools จัดหาข้อมูลระบบ เช่น ชนิดของโปรเซสเซอร์, ชื่อและรุ่น BIOS ของระบบ, โครงเครื่อง, ซีเรียลนัมเบอร์ ฯลฯ ข้อมูล File ที่สามารถแก้ไขได้มีเพียงอย่างเดียว นั่นคือ หมายเลขการติดตามสินทรัพย์ ข้อมูลอื่นๆ ทั้งหมดใช้สำหรับอ่านเท่านั้น

Storage

ตัวเลือก Storage ภายในการกำหนดค่า BIOS สำหรับ HP ProtectTools จัดหาข้อมูลเกี่ยวกับอุปกรณ์บูตทั้งหมดที่กำหนดค่าไว้ในระบบคอมพิวเตอร์ และให้คุณสามารถระบุการตั้งค่าสำหรับอุปกรณ์เหล่านี้ การตั้งค่าที่เข้าใช้งานได้ใน Storage ได้แก่:

- Device Configuration
- Storage Options
- DPS Self-Test
- Boot Order

Security

ตัวเลือก Security ภายในการกำหนดค่า BIOS สำหรับ HP ProtectTools เป็นตำแหน่งศูนย์กลางสำหรับการตั้งค่าทั้งหมดที่เกี่ยวกับความปลอดภัยและรหัสผ่าน การตั้งค่าที่มีอยู่ได้แก่:

- Setup Password
- Power-On Password
- Password Options
- Smart Cover (บางรุ่น)
- Device Security
- Network Service Boot
- System IDs
- DriveLock Security
- System Security (บางรุ่น)
- Setup Security Level

Power

ตัวเลือก Power ภายในการกำหนดค่า BIOS สำหรับ HP ProtectTools จัดหาการตั้งค่าสำหรับควบคุมการจัดการพลังงานที่ระดับฮาร์ดแวร์ การตั้งค่าที่มีอยู่ได้แก่:

- OS Power Management
- Hardware Power Management
- Thermal

Advanced

การตั้งค่าภายในการกำหนดค่า BIOS สำหรับ HP ProtectTools ใช้สำหรับผู้ใช้ขั้นสูง การตั้งค่าเหล่านี้ได้แก่:

- Power-On Options
- Execute Memory Test (บางรุ่น)
- BIOS Power-On
- Onboard Devices
- PCI Devices
- PCI VGA Configuration
- Bus Options
- Device Options
- ตัวเลือก AMT

6 Device Access Manager สำหรับ HP ProtectTools

เครื่องมือความปลอดภัยนี้นำมาใช้ได้เฉพาะผู้ที่เป็นผู้ดูแลระบบ Device Access Manager จัดหาการควบคุมที่ปรับแต่งได้สำหรับอุปกรณ์จัดเก็บและรับส่งข้อมูล (พอร์ต USB, COM & LPT, ไดรฟ์ซีดี, การ์ดอินเตอร์เฟซเน็ตเวิร์ก, เครื่องเล่นเพลงส่วนบุคคล ฯลฯ) นอกจากนี้ Device Access Manager ยังสามารถจัดการผู้ใช้และกลุ่มผู้ใช้เพื่อจัดหาสิทธิ์ในการอ่าน เขียน อนุญาต หรือปฏิเสธข้อมูลบนฮาร์ดแวร์

การเริ่มบริการส่วนหลัง

สำหรับการใช้โปรไฟล์อุปกรณ์ บริการส่วนหลัง HP ProtectTools Device Locking/Auditing จะต้องทำงานอยู่ เมื่อคุณพยายามที่จะใช้โปรไฟล์อุปกรณ์ในครั้งแรก HP ProtectTools Security Manager จะเปิดกล่องโต้ตอบเพื่อถามว่าคุณต้องการเริ่มบริการดังกล่าวหรือไม่ คลิก **Yes** เพื่อเริ่มบริการนั้น และตั้งค่าให้เริ่มทำงานโดยอัตโนมัติทุกครั้งที่บูตระบบ

Simple configuration

คุณสมบัตินี้จะอนุญาตให้คุณปฏิเสธการเข้าใช้ประเภทของอุปกรณ์ต่อไปนี้:

- สื่อที่ถอดออกได้ทั้งหมด (ฟลอปปีดิสก์, ไดรฟ์แบบปากกา, USB เป็นต้น) สำหรับผู้ใช้ทุกคนที่ไม่ใช่ผู้ดูแลระบบ
- ไดรฟ์ดีวีดี/ซีดีรอมทั้งหมดสำหรับผู้ใช้ทุกคนที่ไม่ใช่ผู้ดูแลระบบ
- พอร์ตอนุกรมและพอร์ตขนานทั้งหมดสำหรับผู้ใช้ทุกคนที่ไม่ใช่ผู้ดูแลระบบ
- อุปกรณ์ Bluetooth, อินฟราเรด, โมเด็ม, PCMCIA, เครื่องเล่นเพลงส่วนบุคคล และอุปกรณ์ 1394 (FireWire) ทั้งหมดสำหรับผู้ใช้ทุกคนที่ไม่ใช่ผู้ดูแลระบบ

การปฏิเสธการเข้าใช้ประเภทของอุปกรณ์สำหรับผู้ใช้ทุกคนที่ไม่ใช่ผู้ดูแลระบบ:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Device Acces Manager** จากนั้นคลิก **Simple Configuration**
3. ในแผงด้านขวา ให้เลือกกล่องตัวเลือกของอุปกรณ์เพื่อปฏิเสธการเข้าใช้
4. คลิก **Apply**

หมายเหตุ: หากบริการส่วนหลังไม่ได้ทำงานอยู่ บริการนั้นก็จะพยายามเริ่มต้นในตอนนี้ คลิก **Yes** เพื่ออนุญาต

5. คลิก **OK**

Device class configuration (ขั้นสูง)

สามารถทำการเลือกเพิ่มเติมเพื่ออนุญาตให้ยอมรับหรือปฏิเสธผู้ใช้หรือกลุ่มผู้ใช้สำหรับการเข้าใช้อุปกรณ์บางชนิด อุปกรณ์บางประเภทอนุญาตให้ตัวเลือกนี้สามารถกำหนดค่า Read Only หรือ Write

การเพิ่มผู้ใช้หรือกลุ่ม

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Device Acces Manager** จากนั้นคลิก **Device Class Configuration**
3. ในรายการอุปกรณ์ ให้คลิกประเภทของอุปกรณ์ที่คุณต้องการกำหนดค่า
4. คลิก **Add** กล่องโต้ตอบ **Select Users or Groups** จะเปิดขึ้น
5. เลือก **Advanced** > **Find Now** เพื่อค้นหาผู้ใช้หรือกลุ่มที่จะเพิ่ม
6. คลิกผู้ใช้หรือกลุ่มที่จะเพิ่มลงในรายการผู้ใช้และกลุ่มที่มีอยู่ จากนั้นคลิก **OK**
7. คลิก **OK**

การลบผู้ใช้หรือกลุ่ม

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Device Acces Manager** จากนั้นคลิก **Device Class Configuration**
3. ในรายการอุปกรณ์ ให้คลิกประเภทของอุปกรณ์ที่คุณต้องการกำหนดค่า
4. คลิกผู้ใช้หรือกลุ่มที่คุณต้องการลบออก และคลิก **Remove**
5. คลิก **Apply** แล้วคลิก **OK**

การปฏิเสธการเข้าใช้สำหรับผู้ใช้หรือกลุ่ม

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Device Acces Manager** จากนั้นคลิก **Device Class Configuration**
3. ในรายการอุปกรณ์ ให้คลิกประเภทของอุปกรณ์ที่คุณต้องการกำหนดค่า
4. ภายใต้ **User/Groups** ให้คลิกผู้ใช้หรือกลุ่มที่จะปฏิเสธการเข้าใช้
5. คลิก **Deny** ที่อยู่ข้างๆ ผู้ใช้หรือกลุ่มที่จะปฏิเสธการเข้าใช้
6. คลิก **Apply** และคลิก **OK**

การอนุญาตการเข้าใช้ประเภทของอุปกรณ์สำหรับผู้ใช้หนึ่งคนภายในกลุ่ม

คุณสามารถอนุญาตให้ผู้ใช้หนึ่งคนเข้าใช้อุปกรณ์ประเภทหนึ่ง ในขณะที่ปฏิเสธการเข้าใช้สำหรับผู้ใช้คนอื่นๆ ทั้งหมดภายในกลุ่ม

การอนุญาตการเข้าใช้สำหรับผู้ใช้หนึ่งคน แต่ไม่ได้อนุญาตให้แก่กลุ่ม:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Device Acces Manager** จากนั้นคลิก **Device Class Configuration**
3. คลิกประเภทของอุปกรณ์ที่คุณต้องการกำหนดค่าในรายการอุปกรณ์
4. ภายใต้ **User/Groups** ให้เพิ่มกลุ่มที่จะปฏิเสธการเข้าใช้
5. คลิก **Deny** ที่อยู่ข้างๆ กลุ่มที่จะปฏิเสธการเข้าใช้

6. ไปยังโฟลเดอร์ที่อยู่ด้านล่างประเภทที่ต้องการ และเพิ่มผู้ใช้ที่เฉพาะเจาะจง คลิก **Allow** เพื่อให้สิทธิ์เข้าใช้งาน
7. คลิก **Apply** และคลิก **OK**

การอนุญาตการเข้าใช้อุปกรณ์ตัวใดตัวหนึ่งสำหรับผู้ใช้หนึ่งคนภายในกลุ่ม

คุณสามารถอนุญาตให้ผู้ใช้หนึ่งคนเข้าใช้อุปกรณ์ตัวใดตัวหนึ่ง ในขณะที่ปฏิเสธการเข้าใช้สำหรับผู้ใช้คนอื่นๆ ทั้งหมดภายในกลุ่มสำหรับอุปกรณ์ทั้งหมดในประเภทนั้น

การอนุญาตการเข้าใช้อุปกรณ์ตัวใดตัวหนึ่งสำหรับผู้ใช้หนึ่งคนภายในกลุ่ม แต่ไม่อนุญาตให้แก่กลุ่ม:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Device Acces Manager** จากนั้นคลิก **Device Class Configuration**
3. ในรายการอุปกรณ์ ให้คลิกประเภทของอุปกรณ์ที่คุณต้องการกำหนดค่า แล้วไปยังโฟลเดอร์ที่อยู่ด้านล่าง
4. ภายใต้ **User/Groups** ให้เพิ่มกลุ่มที่จะปฏิเสธการเข้าใช้
5. คลิก **Deny** ที่อยู่ข้างๆ กลุ่มที่จะปฏิเสธการเข้าใช้
6. ไปยังอุปกรณ์ที่เฉพาะเจาะจงที่จะอนุญาตให้แก่ผู้ใช้ในรายการอุปกรณ์
7. คลิก **Add** กล่องโต้ตอบ **Select Users or Groups** จะเปิดขึ้น
8. เลือก **Advanced** > **Find Now** เพื่อค้นหาผู้ใช้หรือกลุ่มที่จะเพิ่ม
9. คลิกผู้ใช้ที่จะอนุญาตให้เข้าใช้ แล้วคลิก **OK**
10. คลิก **Allow** เพื่อให้สิทธิ์เข้าใช้งาน
11. คลิก **Apply** และคลิก **OK**

7 การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools

การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools สามารถเข้ารหัสข้อมูลทุกบิตบนฮาร์ดไดรฟ์ตัวเดียว, พาร์ติชัน หรือฮาร์ดไดรฟ์หลายตัว เพื่อป้องกันไม่ให้บุคคลที่ไม่ได้รับอนุญาตสามารถอ่านข้อมูลดังกล่าวได้

△ **ข้อควรระวัง:** หากคุณตัดสินใจจะถอนการติดตั้งโมดูลการเข้ารหัสไดรฟ์ คุณต้องถอดรหัสของไดรฟ์ที่ถูกเข้ารหัสทั้งหมดก่อน หากคุณไม่ทำ คุณจะไม่สามารถเข้าใช้ข้อมูลบนไดรฟ์ที่เข้ารหัสได้ เว้นแต่คุณได้ลงทะเบียนด้วยการเรียกคืนข้อมูลการเข้ารหัสไดรฟ์ (โปรดดู “การเรียกคืน ในหน้า 49”) การติดตั้งโมดูลการเข้ารหัสไดรฟ์อีกครั้งจะไม่เปิดการใช้งานที่คุณเข้าใช้งานไดรฟ์ที่เข้ารหัส

การจัดการการเข้ารหัส

การเข้ารหัสไดรฟ์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **Encryption Management**
3. ในแผงด้านขวา ให้คลิก **Activate** การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools Wizard เปิดอยู่
4. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อใช้การเข้ารหัส

หมายเหตุ: คุณจำเป็นต้องระบุแผ่นดิสก์ อุปกรณ์จัดเก็บแบบแฟลช หรือบางสื่อการจัดเก็บอื่นๆ ที่เชื่อมต่อด้วย USB ที่ข้อมูลการเรียกคืนที่จะถูกจัดเก็บ

เปลี่ยนการเข้ารหัสลับ

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **Encryption Management**
3. ในแผงด้านขวา ให้คลิก **Change encryption** เลือกดิสก์เพื่อเข้ารหัสในกล่องโต้ตอบ **Change Encryption** แล้วคลิก **OK**
4. คลิก **OK** อีกครั้งเพื่อเริ่มต้นการเข้ารหัสลับ

การถอดรหัสไดรฟ์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **Encryption Management**
3. ในแผงด้านขวา ให้คลิก **Deactivate**

จัดการผู้ใช้

เพิ่มผู้ใช้

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **User Management**
3. ในแผงด้านขวา ให้คลิก **Add** คลิกชื่อผู้ใช้ในรายการ **User Name** หรือพิมพ์ชื่อผู้ใช้ในช่อง **Username** คลิก **Next**
4. พิมพ์รหัสผ่าน Windows สำหรับผู้ใช้ที่เลือก และจากนั้นคลิก **Next**
5. เลือกวิธีการตรวจสอบความถูกต้องสำหรับผู้ใช้ใหม่ และจากนั้นคลิก **Finish**

ลบผู้ใช้ออก

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **User Management**
3. ในแผงด้านขวา ให้คลิกชื่อผู้ใช้เพื่อลบในรายการ **User Name** คลิก **Remove**
4. คลิก **Yes** เพื่อยืนยันว่าคุณต้องการลบผู้ใช้ที่เลือกนี้

เปลี่ยนโทเคน

เปลี่ยนวิธีการตรวจสอบความถูกต้องสำหรับผู้ใช้ได้ดังนี้:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **User Management**
3. ในแผงด้านขวา ให้เลือกชื่อผู้ใช้จากรายการ **User Name** และจากนั้นคลิก **Change Token**
4. พิมพ์รหัสผ่าน Windows ของผู้ใช้ และจากนั้นคลิก **Next**
5. เลือกวิธีการตรวจสอบความถูกต้องใหม่ และจากนั้นคลิก **Finish**
6. หากคุณเลือก Java Card เป็นวิธีการตรวจสอบความถูกต้อง ให้คุณพิมพ์รหัสผ่าน Java Card เมื่อได้รับการแจ้ง และจากนั้นคลิก **OK**

ตั้งรหัสผ่าน

ตั้งค่ารหัสผ่านหรือเปลี่ยนวิธีการตรวจสอบความถูกต้องสำหรับผู้ใช้ได้ดังนี้:

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **User Management**
3. ในแผงด้านขวา ให้เลือกผู้ใช้จากรายการ **User Name** และจากนั้นคลิก **Set Password**
4. พิมพ์รหัสผ่าน Windows ของผู้ใช้ และจากนั้นคลิก **Next**
5. เลือกวิธีการตรวจสอบความถูกต้องใหม่ และจากนั้นคลิก **Finish**
6. หากคุณเลือก Java Card เป็นวิธีการตรวจสอบความถูกต้อง ให้คุณพิมพ์รหัสผ่าน Java Card เมื่อได้รับการแจ้ง และจากนั้นคลิก **OK**

การเรียกคืน

สองมาตรการการรักษาความปลอดภัยที่มีให้คุณดังต่อไปนี้:

- หากคุณลืมรหัสผ่าน คุณจะไม่สามารถเข้าใช้ไดรฟ์ที่เข้ารหัสของคุณได้ อย่างไรก็ตาม คุณอาจจะลงทะเบียนกับบริการการเรียกคืนข้อมูลการเข้ารหัสไดรฟ์เพื่อเปิดใช้งานให้คุณเข้าใช้คอมพิวเตอร์หากคุณลืมรหัสผ่าน
- คุณอาจจะต้องสำรองข้อมูลคีย์การเข้ารหัสไดรฟ์บนแผ่นดิสก์ อุปกรณ์จัดเก็บแบบแฟลช หรือบางสื่อการจัดเก็บอื่นๆ ที่เชื่อมต่อด้วย USB

การลงทะเบียนกับบริการการเรียกคืนข้อมูลการเข้ารหัสไดรฟ์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **Recovery**
3. ในแผงด้านขวา ให้คลิก **Click here to register** พิมพ์ข้อมูลที่ร้องขอเพื่อให้ขั้นตอนการสำรองข้อมูลความปลอดภัยเสร็จสมบูรณ์

การสำรองข้อมูลคีย์การเข้ารหัสไดรฟ์

1. เลือก **Start** > **All Programs** > **HP ProtectTools Security Manager**
2. ในแผงด้านซ้าย ให้คลิก **Drive Encryption** และจากนั้นคลิก **Recovery**
3. ในแผงด้านขวาให้คลิก **Click here to backup your keys**
4. เลือกแผ่นดิสก์ อุปกรณ์จัดเก็บแบบแฟลช หรือบางสื่อการจัดเก็บอื่นๆ ที่เชื่อมต่อด้วย USB ที่บันทึกข้อมูลการเรียกคืน และจากนั้นคลิก **Next** การเข้ารหัสไดรฟ์สำหรับ HP ProtectTools Wizard เปิดอยู่
5. ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อสำรองข้อมูลคีย์การเข้ารหัสไดรฟ์

หมายเหตุ: คุณจำเป็นต้องระบุแผ่นดิสก์ อุปกรณ์จัดเก็บแบบแฟลช หรือบางสื่อการจัดเก็บอื่นๆ ที่เชื่อมต่อด้วย USB ที่ข้อมูลการเรียกคืนที่จะถูกจัดเก็บ

8 การแก้ไขปัญหา

Credential Manager สำหรับ HP ProtectTools

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
การใช้ตัวเลือก Credential Manager Network Accounts ผู้ใช้สามารถเลือกบัญชีโดเมนเพื่อบันทึกลง เมื่อใช้การตรวจสอบความถูกต้อง TPM แล้ว ตัวเลือกนี้จะไม่สามารถทำงาน วิธีการตรวจสอบความถูกต้องอื่นๆ ทั้งหมดทำงานอย่างถูกต้อง	การใช้การตรวจสอบความถูกต้อง TPM ผู้ใช้ที่ได้ล็อกเข้าสู่คอมพิวเตอร์โลคัลเท่านั้น	การใช้เครื่องมือ Credential Manager Single Sign On อนุญาตให้ตรวจสอบความถูกต้องบัญชีอื่นๆ
ใบรับรองโทเคน USB ไม่สามารถใช้งานได้กับการล็อกเข้า Windows XP Service Pack 1	หลังจากการติดตั้งซอฟต์แวร์โทเคน USB การลงทะเบียนใบรับรองโทเคน USB token และการตั้งค่า Credential Manager เป็นการล็อกเข้าหลักแล้ว USB Token จะไม่มีอยู่ในรายการหรือไม่มีอยู่ใน Credential Manager/gina logon เมื่อทำการล็อกกลับเข้า Windows ล็อกออฟ Credential Manager ล็อกกลับเข้า Credential Manager ใหม่และเลือกโทเคนเป็นล็อกเข้าหลักอีกครั้ง การล็อกเข้าโทเคนจะดำเนินการการทำงานเป็นปกติ	ปัญหานี้เกิดขึ้นเฉพาะกับ Windows XP Service Pack 1 ให้อัพเดตเวอร์ชันของ Windows version เป็น Service Pack 2 ผ่าน Windows Update อย่างถูกต้อง ในการทำงานรอบๆ หากยังมี Service Pack 1 อยู่ ให้ล็อกกลับเข้าไป Windows อีกครั้งโดยการใช้ใบรับรองอื่นๆ (รหัสผ่าน Windows) เพื่อที่จะล็อกออฟและล็อกกลับเข้า Credential Manager อีกครั้ง
บางเว็บเพจแอปพลิเคชั่นสร้างข้อผิดพลาดที่กีดขวางผู้ใช้จากการกระทำหรือการทำงานอย่างสมบูรณ์	บางแอปพลิเคชั่นแบบเว็บหยุดการทำงานและรายงานข้อผิดพลาดระหว่างการยกเลิกรูปแบบฟังก์ชันการทำงานของ Single Sign On ตัวอย่างเช่น **!** ในรูปสามเหลี่ยมสีเหลืองที่พบใน Internet Explorer เป็นเครื่องหมายแสดงข้อผิดพลาดที่เกิดขึ้น	Credential Manager Single Sign On ไม่สนับสนุนกับอินเทอร์เฟซเว็บซอฟต์แวร์ทั้งหมด ยกเลิกการใช้งานการสนับสนุน Single Sign On สำหรับเว็บเพจที่ระบุด้วยการปิดการสนับสนุน Single Sign On โปรดดูเอกสารประกอบแบบเต็มที่ Single Sign On ซึ่งมีอยู่ในไฟล์วิธีใช้ของ Credential Manager หาก Single Sign On ที่ระบุไม่สามารถยกเลิกแอปพลิเคชั่นที่ให้ได้ โปรดติดต่อฝ่ายบริการและฝ่ายสนับสนุนของ HP และร้องขอการสนับสนุนลำดับที่ 3 ผ่านการติดต่อฝ่ายบริการของ HP
ไม่มีตัวเลือกไปยัง **Browse for Virtual Token** ระหว่างขั้นตอนการล็อกเข้า	ผู้ใช้ไม่สามารถย้ายตำแหน่งของโทเคนเสมือนจริงที่ลงทะเบียนไว้ใน Credential Manager เนื่องจากตัวเลือกนี้ไปยังการเรียกดูที่ถูกลบระหว่างความเสี่ยงด้านความปลอดภัย	ตัวเลือกการเรียกดูที่ถูกลบจากการนำเสนอผลิตภัณฑ์ปัจจุบันเนื่องจากอนุญาตให้ผู้ที่ไม่ใช่ผู้ใช้ลบและเปลี่ยนชื่อไฟล์ได้รวมทั้งทำการควบคุม Windows
ล็อกเข้าด้วยการตรวจสอบความถูกต้อง TPM ที่ไม่ให้ตัวเลือก **Network Accounts**	การใช้ตัวเลือก **Network Accounts** ผู้ใช้สามารถเลือกบัญชีโดเมนเพื่อบันทึกลง เมื่อใช้การตรวจสอบความถูกต้อง TPM แล้ว ตัวเลือกนี้จะไม่สามารถทำงาน	HP ทำการศึกษาแนวทางแก้ไขเพื่อให้ผลิตภัณฑ์มีประสิทธิภาพดียิ่งขึ้นในอนาคต
ผู้ดูแลระบบโดเมนไม่สามารถเปลี่ยนรหัสผ่านของ Windows แม้จะได้รับการตรวจสอบความถูกต้อง	การกระทำนี้เกิดขึ้นหลังจากผู้ดูแลระบบโดเมนล็อกออนไปที่โดเมนและลงทะเบียนการระบุโดเมนด้วย Credential Manager โดยการใช้บัญชีสิทธิ์ของผู้ดูแลระบบบนโดเมนและคอมพิวเตอร์โลคัล เมื่อผู้ดูแลระบบโดเมนพยายามทำการเปลี่ยนแปลงรหัสผ่าน Windows จาก Credential Manager ผู้ดูแลระบบจะได้	Credential Manager ไม่สามารถเปลี่ยนรหัสผ่านบัญชีของผู้ใช้โดเมนผ่าน **Change Windows password** Credential Manager สามารถเปลี่ยนรหัสผ่านของคอมพิวเตอร์โลคัลได้เท่านั้น ผู้ใช้โดเมนสามารถเปลี่ยนรหัสผ่านของเขา/เธอผ่านตัวเลือก **Windows security** > **Change password** แต่ เนื่องจากผู้ใช้โดเมนไม่มีบัญชีทางกายภาพบนคอมพิวเตอร์โลคัล Credential Manager สามารถเปลี่ยนรหัสผ่านที่ใช้แล้วเพื่อล็อกเข้าได้เท่านั้น

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
	รับข้อผิดพลาดการล็อกออนดังนี้: **User account restriction**.	
การตั้งค่าเริ่มต้นของ Credential Manager Single Sign ควรจะตั้งเป็นการแจ้งเตือนข้อความเพื่อป้องกันการวน	ค่าเริ่มต้นของ Single Sign On ตั้งค่าเพื่อบันทึกผู้ใช้โดยอัตโนมัติ อย่างไรก็ตาม เมื่อการสร้างที่สองของสองเอกสารที่ถูกป้องกันด้วยรหัสผ่านอื่น Credential Manager จะใช้รหัสผ่านที่บันทึกไว้ล่าสุดจากเอกสารแรก	HP ทำการศึกษาแนวทางแก้ไขเพื่อให้ผลิตภัณฑ์มีประสิทธิภาพดียิ่งขึ้นในอนาคต
ปัญหาของความไม่สามารถเข้ากันได้ด้วย Corel WordPerfect 12 password gina	หากผู้ใช้ล็อกเข้าไปที่ Credential Manager ให้สร้างเอกสารใน WordPerfect และบันทึกด้วยการป้องกันด้วยรหัสผ่าน Credential Manager จะไม่สามารถตรวจสอบหรือยอมรับแบบด้วยตนเองหรือแบบอัตโนมัติ gina รหัสผ่าน	HP ทำการศึกษาแนวทางแก้ไขเพื่อให้ผลิตภัณฑ์มีประสิทธิภาพดียิ่งขึ้นในอนาคต
Credential Manager ไม่รู้จักปุ่ม **Connect** บนหน้าจอ	หากใบรับรองของ Single Sign On สำหรับ Remote Desktop Connection (RDP) ตั้งค่าที่ **Connect** Single Sign On เมื่อเปิดอีกครั้งป้อน **Save As** เสมอ แทนที่ **Connect**	HP ทำการศึกษาแนวทางแก้ไขเพื่อให้ผลิตภัณฑ์มีประสิทธิภาพดียิ่งขึ้นในอนาคต
ตัวช่วยการกำหนดค่า ATI Catalyst ไม่สามารถใช้กับ Credential Manager	Credential Manager Single Sign On ขัดแย้งกับตัวช่วยกำหนดค่า ATI Catalyst	ยกเลิกการใช้งาน Credential Manager Single Sign On
เมื่อทำการล็อกเข้าโดยการใช้การตรวจสอบความถูกต้อง TPM ปุ่ม **Back** บนหน้าจอจะข้ามตัวเลือกนี้เพื่อเลือกวิธีการตรวจสอบความถูกต้องอื่นๆ	หากผู้ใช้ใช้การตรวจสอบความถูกต้องล็อกเข้า TPM สำหรับ Credential Manager จะป้อนรหัสผ่าน ปุ่ม **Back** จะไม่สามารถทำงานได้ แต่จะแทนที่การแสดงหน้าจอล็อกเข้าของ Windows โดยทันที	HP ทำการศึกษาแนวทางแก้ไขเพื่อให้ผลิตภัณฑ์มีประสิทธิภาพดียิ่งขึ้นในอนาคต
Credential Manager จะเปิดออกจากโหมดสแตนด์บายเมื่อถูกกำหนดค่า	เมื่อ **use Credential Manager log on to Windows** ไม่เลือกเป็นตัวเลือก การอนุญาตให้ระบบเข้าไปที่การพักการทำงาน S3 และจากนั้นออกจากสาเหตุของระบบของ Credential Manager ล็อกออนไปที่ Windows เพื่อเปิด	โดยที่ไม่มีการตั้งค่ารหัสผ่านผู้ดูแลระบบ ผู้ใช้จะไม่สามารถล็อกออนไปที่ Windows ผ่าน Credential Manager เนื่องจากข้อจำกัดของบัญชีที่ถูกร้องขอโดย Credential Manager • หากไม่มี Java Card/โทเคน ผู้ใช้สามารถยกเลิกการล็อกเข้าของ Credential Manager และผู้ใช้จะพบการล็อกเข้าของ Microsoft Windows ผู้ใช้สามารถล็อกเข้าได้ที่จุดนี้ • หากมี Java Card/โทเคน ให้ปฏิบัติตามแนวทางการแก้ไขต่อไปนี้ที่ให้คุณใช้งาน/ยกเลิกการใช้งานการเปิดของ Credential Manager เมื่อทำการใส่ Java Card 1. คลิก **Advanced Settings** 2. คลิก **Service & Applications** 3. คลิก **Java Cards and Tokens** 4. คลิกเมื่อได้ใส่ Java Card/โทเคนแล้ว 5. ทำเครื่องหมายเลือกที่ **Advise to log-on**
ผู้ใช้จะสูญเสียใบรับรองของ Credential Manager ทั้งหมดที่ถูกป้องกันด้วย TPM หากโมดูล TPM ถูกนำออกหรือเสียหาย	หากโมดูล TPM ถูกนำออกหรือเสียหาย ผู้ใช้จะสูญเสียใบรับรองทั้งหมดที่ถูกป้องกันด้วย TPM	สิ่งนี้ได้รับการออกแบบมาแล้ว โมดูล TPM ที่ได้รับการออกแบบเพื่อปกป้องใบรับรองของ Credential Manager HP ขอแนะนำว่าให้ผู้ใช้สำรองข้อมูลที่ระบุจาก Credential Manager ก่อนเพื่อนำออกจากโมดูล TPM
Credential Manager ไม่ได้ตั้งค่าเป็นการล็อกเข้าหลักใน Windows 2000	ระหว่างที่ติดตั้ง Windows 2000 นโยบายการล็อกออนจะตั้งค่าสำหรับผู้ดูแลระบบล็อกออนแบบด้วยตนเองหรือแบบโดยอัตโนมัติ หากเลือกการล็อกออนอัตโนมัติ จากนั้นการตั้งค่ารีจิสทรีเริ่มต้นของ Windows จะตั้งค่าล็อกออนของผู้ดูแลระบบอัตโนมัติไว้ที่ 1 และ Credential Manager จะไม่ยกเลิกค่านี้	สิ่งนี้ได้รับการออกแบบไว้แล้ว หากผู้ใช้ต้องการแก้ไขการตั้งค่าระดับของระบบปฏิบัติการสำหรับค่าการล็อกออนของผู้ดูแลระบบโดยอัตโนมัติเพื่อข้ามพาธการแก้ไขคือ `HKEY_LOCAL_MACHINE/Software/Microsoft/ WindowsNT/CurrentVersion/WinLogon`

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
		ข้อควรระวัง: ใช้ Registry Editor ตามใจคุณ! การใช้ Registry Editor (regedit) ที่ไม่ถูกต้องสามารถทำให้เกิดปัญหาที่ร้ายแรงได้ซึ่งอาจจะทำให้คุณต้องติดตั้งระบบปฏิบัติการใหม่อีกครั้ง ไม่มีการรับรองว่าการเกิดปัญหาจากการใช้ที่ไม่ถูกต้องของ Registry Editor สามารถแก้ไขได้
ข้อความการล็อกออนด้วยลายนิ้วมือจะปรากฏขึ้นหรือไม่ตัวอ่านลายนิ้วมือจะต้องได้ติดตั้งหรือลงทะเบียนไว้แล้ว	หากผู้ใช้เลือกการล็อกออนของ Windows ให้ปฏิบัติตามการแจ้งเตือนของเดสก์ทอปที่ปรากฏอยู่ในทาสก์บาร์ Credential Manager ดังต่อไปนี้: **คุณสามารถวางนิ้วของคุณบนตัวอ่านลายพิมพ์นิ้วมือเพื่อล็อกออนเข้าไปที่ Credential Manager**	จุดประสงค์ของการแจ้งเตือนของเดสก์ท็อปคือเพื่อแจ้งเตือนให้ผู้ใช้ว่าการตรวจสอบความถูกต้องด้วยลายนิ้วมือสามารถใช้งานได้หากได้กำหนดค่าไว้
หน้าต่างการล็อกออน Credential Manager สำหรับสถานะของ Windows 2000 **insert card** เมื่อไม่ได้ติดตั้งตัวอ่าน	หน้าจอ Windows Credential Manager Welcome จะแนะนำให้ผู้ใช้สามารถล็อกออนด้วย **insert card** เมื่อไม่ได้ติดตั้งตัวอ่าน Java Card	จุดประสงค์ของการแจ้งเตือนคือเพื่อแจ้งเตือนให้ผู้ใช้ว่าการตรวจสอบความถูกต้อง Java Card สามารถใช้งานได้ หากได้กำหนดค่าไว้
ไม่สามารถล็อกเข้า Credential Manager หลังจากการเปลี่ยนจากโหมดพักชั่วคราวไปยังไฮเบอร์เนชั่นบน Windows XP Service Pack 1 เท่านั้น	หลังจากอนุญาตให้ระบบทำการเปลี่ยนไปเป็นโหมดไฮเบอร์เนชั่นและโหมดพักชั่วคราว ผู้ดูแลระบบหรือผู้ใช้จะไม่สามารถทำการล็อกเข้า Credential Manager และหน้าจอล็อกออนของ Windows ที่ปรากฏขึ้นไม่ว่าจะล็อกออกใบรับรอง (รหัสผ่าน ลายพิมพ์นิ้วมือ หรือ Java Card) ที่เลือกไว้	ปัญหาที่ปรากฏนี้ถูกแก้ไขใน Service Pack 2 จาก Microsoft โปรดดูที่บทความพื้นฐานความรู้ของ Microsoft 813301 ที่ http://www.microsoft.com สำหรับข้อมูลเพิ่มเติมของสาเหตุปัญหานี้ เพื่อที่จะล็อกออน ผู้ใช้ต้องเลือก Credential Manager และล็อกเข้า หลังจากทำการล็อกเข้า Credential Manager ผู้ใช้จะได้รับการแจ้งเตือนให้ล็อกเข้า Windows (ผู้ใช้อาจเลือกตัวเลือกการล็อกเข้าของ Windows) เพื่อให้ขั้นตอนการล็อกเข้าเสร็จสมบูรณ์ หากผู้ใช้ล็อกเข้าสู่ Windows ก่อน แล้วจากนั้นผู้ใช้ต้องล็อกเข้าสู่ Credential Manager ด้วยตนเอง
Restoring Embedded Security ทำให้ Credential Manager ไม่ทำงาน	ข้อผิดพลาดของ Credential Manager ในการลงทะเบียนใบรับรองใดๆ หลังจากที่ ROM ได้ถูกเรียกคืนเป็นการตั้งค่าจากโรงงาน	HP Credential Manager สำหรับข้อผิดพลาดของ ProtectTools เพื่อเข้าใช้ TPM หาก ROM ได้รีเซ็ตเป็นการตั้งค่าจากโรงงานหลังจากการติดตั้ง Credential Manager ชิปความปลอดภัย TPM แบบฝังตัวสามารถใช้งานได้ในยูทิลิตีการตั้งค่าคอมพิวเตอร์ของ BIOS, การกำหนดค่า BIOS สำหรับ ProtectTools หรือ HP Client Manager ในการใช้งานชิปความปลอดภัย TPM แบบฝังตัว: 1. เปิดการตั้งค่าคอมพิวเตอร์โดยการเปิดหรือรีสตาร์ทเครื่องคอมพิวเตอร์ แล้วจากนั้นกด F10 ในขณะที่ข้อความ **F10 = ROM Based Setup** ปรากฏอยู่ในมุมซ้ายล่างของหน้าจอ 2. ใช้ปุ่มลูกศรเพื่อเลือก **Security** > **Setup Password** ตั้งรหัสผ่าน 3. เลือก **Embedded Security Device** 4. ใช้ปุ่มลูกศรเพื่อเลือก **Embedded Security Device—Disable** ใช้ปุ่มลูกศรเพื่อเปลี่ยนเป็น **Embedded Security Device—Enable** 5. เลือก **Enable** > **Save changes and exit** HP ทำการตรวจสอบการแก้ไขตัวเลือกความละเอียดสำหรับการปล่อยซอฟต์แวร์ของลูกค้าในอนาคต
ขั้นตอน **Restore Identity** ของความปลอดภัยที่สูญเสียการรวมกันด้วยโทเคนเสมือนจริง	เมื่อผู้ใช้คืนค่าการระบุ Credential Manager อาจสูญเสียการรวมกันด้วยตำแหน่งของโทเคนเสมือนจริงที่หน้าจอล็อกเข้า แม้ว่า Credential Manager จะมีโทเคนเสมือนจริงที่ลงทะเบียนไว้แล้ว ผู้ใช้ก็ต้องลงทะเบียนโทเคนอีกครั้งเพื่อคืนค่าการรวมกัน	สิ่งนี้ได้รับการออกแบบไว้แล้ว เมื่อทำการถอนการติดตั้ง Credential Manager โดยที่ไม่ทำการเก็บการระบุ ส่วนของระบบ (เซิร์ฟเวอร์) โทเคนจะถูกทำลาย ดังนั้นโทเคนจึงไม่สามารถถูกใช้ล็อกเข้าได้อีก แม้ว่าหากส่วนของไคลเอนต์ของโทเคนจะถูกคืนค่าผ่านการคืนค่าการระบุ HP ทำการตรวจสอบการแก้ไขตัวเลือกระยะยาวสำหรับความละเอียด

Embedded Security สำหรับ HP ProtectTools

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
การเข้ารหัสโฟลเดอร์โฟลเดอร์ย่อย และไฟล์บน PSD ทำให้เกิดข้อความแสดงข้อผิดพลาด	หากผู้ใช้คัดลอกไฟล์และโฟลเดอร์ไปยัง PSD และพยายามเข้ารหัสโฟลเดอร์/ไฟล์ หรือโฟลเดอร์/โฟลเดอร์ย่อย ข้อความ **Error Applying Attributes** จะปรากฏขึ้น ผู้ใช้สามารถเข้ารหัสไฟล์เดียวกันบน C:\ drive บนฮาร์ดไดรฟ์ที่ติดตั้งไว้พิเศษ	สิ่งนี้ได้รับการออกแบบไว้แล้ว การย้ายไฟล์/โฟลเดอร์ไปยัง PSD ที่เข้ารหัสไฟล์โฟลเดอร์โดยอัตโนมัติ ไม่จำเป็นต้อง “เข้ารหัสคู่” ที่ไฟล์/โฟลเดอร์ กำลังพยายามเข้ารหัสคู่โดยใช้บน PSD โดยการใช้ EFS จะทำให้เกิดข้อความการแสดงข้อผิดพลาดนี้
ไม่สามารถแสดงความเป็นเจ้าของกับระบบปฏิบัติการอื่นในแพล็ตฟอร์ม MultiBoot	หากไดรฟ์ได้ตั้งค่าสำหรับการบูตหลายระบบปฏิบัติการ เจ้าของสามารถถูกนำด้วยตัวช่วยการเริ่มต้นของแพล็ตฟอร์มในหนึ่งระบบปฏิบัติการเท่านั้น	สิ่งนี้ได้รับการออกแบบไว้แล้ว เพื่อเหตุผลทางด้านความปลอดภัย
ผู้ดูแลระบบสามารถดู ลบ เปลี่ยนชื่อ หรือย้ายเนื้อหาของโฟลเดอร์ EFS ที่เข้ารหัส	การเข้ารหัสโฟลเดอร์จะไม่หยุดผู้ใช้ที่ไม่ได้ตรวจสอบความถูกต้องด้วยสิทธิ์ของผู้ดูแลระบบเพื่อดู ลบ หรือย้ายเนื้อหาของโฟลเดอร์	สิ่งนี้ได้รับการออกแบบไว้แล้ว เป็นคุณสมบัติของ EFS ไม่ใช่ Embedded Security TPM Embedded Security ใช้ซอฟต์แวร์ของ Microsoft EFS และ EFS เก็บไฟล์/โฟลเดอร์สิทธิ์การเข้าใช้สำหรับผู้ดูแลระบบทั้งหมด
โฟลเดอร์ที่เข้ารหัสด้วย EFS ใน Windows 2000 จะไม่แสดงที่ถูกไฮไลต์เป็นสีเขียว	โฟลเดอร์ที่เข้ารหัสด้วย EFS ใน Windows 2000 จะไม่แสดงที่ถูกไฮไลต์เป็นสีเขียว	สิ่งนี้ได้รับการออกแบบไว้แล้ว เป็นคุณสมบัติของ EFS ที่ไม่ไฮไลต์โฟลเดอร์ที่เข้ารหัสใน Windows 2000 แต่มีใน Windows XP จริงหรือไม่ที่ Embedded Security TPM ได้ติดตั้งแล้ว
EFS ไม่จำเป็นต้องใช้รหัสผ่านเพื่อดูไฟล์ที่เข้ารหัสใน Windows 2000	หากผู้ใช้ติดตั้ง Embedded Security ให้ล็อกออกเป็นผู้ดูแลระบบ แล้วล็อกออฟแล้วกลับเข้าเป็นผู้ดูแลระบบ ผู้ใช้สามารถดูไฟล์/โฟลเดอร์ตามลำดับใน Windows 2000 โดยที่ไม่มีรหัสผ่าน กรณีนี้เกิดเฉพาะในบัญชีผู้ดูแลระบบแรกบน Windows 2000 หากบัญชีผู้ดูแลระบบที่สองได้ล็อกเข้าแล้ว จะไม่เกิดกรณีนี้ขึ้น	สิ่งนี้ได้รับการออกแบบไว้แล้ว เป็นคุณสมบัติของ EFS ใน Windows 2000 EFS ใน Windows XP ตามค่าเริ่มต้นจะไม่ให้ผู้ใช้เปิดไฟล์/โฟลเดอร์โดยที่ไม่มีรหัสผ่าน
ซอฟต์แวร์ไม่ควรติดตั้งไว้ก่อนบนการเรียกคืนด้วยพาร์ทิชัน FAT32	หากผู้ใช้พยายามทำการเรียกคืนฮาร์ดไดรฟ์โดยการใช้ FAT32 จะไม่มีการเข้ารหัสตัวเลือกสำหรับไฟล์/โฟลเดอร์ใดๆ โดยการใช้ EFS	สิ่งนี้ได้รับการออกแบบไว้แล้ว Microsoft EFS สนับสนุนเฉพาะบน NTFS และจะไม่ทำงานบน FAT32 คุณสมบัตินี้เป็นของ EFS ของ Microsoft และไม่เกี่ยวข้องกับซอฟต์แวร์ของ HP ProtectTools
Windows 2000 User สามารถแชร์ไปยังเครือข่าย PSD ด้วยการแชร์ที่ซ่อน ($)	Windows 2000 User สามารถแชร์ไปยังเครือข่าย PSD ด้วยการแชร์ที่ซ่อน ($) การแชร์ที่ซ่อนสามารถเข้าใช้ผ่านเครือข่ายโดยการใช้การแชร์ที่ซ่อน ($)	PSD ไม่ได้แชร์บนเครือข่ายอย่างปกติ แต่สามารถแชร์ผ่านการแชร์ที่ซ่อน ($) ใน Windows 2000 เท่านั้น HP ขอแนะนำให้มีรหัสผ่านที่ป้องกันบัญชีผู้ดูแลระบบภายในเสมอ
ผู้ใช้สามารถเข้ารหัสหรือลบไฟล์ XML แหล่งจัดเก็บสำหรับการเรียกคืน	โดยออก ACL สำหรับโฟลเดอร์ที่ไม่ได้ตั้งค่า ดังนั้น ผู้ใช้สามารถเข้ารหัสหรือลบไฟล์โดยไม่ได้ตั้งใจหรือตั้งใจ ทำให้ไม่สามารถเข้าถึงได้ เมื่อได้เข้ารหัสหรือลบไฟล์นี้แล้ว จะไม่มีใครสามารถใช้ซอฟต์แวร์ TPM ได้	สิ่งนี้ได้รับการออกแบบไว้แล้ว ผู้ใช้มีสิทธิ์เข้าใช้แหล่งจัดเก็บฉุกเฉินเพื่อที่จะบันทึก/อัพเดตการคัดลอกการสำรองข้อมูลของ Basic User Key ลูกค้าควรจะนำวิธีการรักษาความปลอดภัยของแนวทางที่เหมาะสมและแนะนำผู้ใช้ที่ไม่เคยเข้ารหัสหรือลบไฟล์ของแหล่งจัดเก็บการเรียกคืน
HP ProtectTools Embedded Security EFS ทำงานร่วมกับ Symantec Antivirus หรือ Norton Antivirus ทำการเข้ารหัส/ถอดรหัสและเวลาที่สแกนได้นานกว่า	ไฟล์ที่เข้ารหัสแย้งกันกับ Symantec Antivirus หรือสแกนไวรัสของ Norton Antivirus 2005 ระหว่างขั้นตอนการสแกน รหัสผ่านของ Basic User จะแจ้งเตือนผู้ใช้รหัสผ่านทุกๆ 10 ไฟล์โดยประมาณ หากผู้ใช้ไม่ป้อนรหัสผ่าน รหัสผ่านของ Basic User จะแจ้งเตือนว่าหมดเวลา การอนุญาตให้ NAV2005 ดำเนินการด้วยการสแกนต่อไป การเข้ารหัสไฟล์โดยการใช้ HP ProtectTools Embedded Security EFS จะนานขึ้นเมื่อ Symantec Antivirus หรือ Norton Antivirus ทำงานอยู่	ในการลดเวลาที่จำเป็นในการสแกนไฟล์ของ HP ProtectTools Embedded Security EFS ผู้ใช้สามารถป้อนรหัสผ่านการเข้ารหัสก่อนการสแกนหรือการถอดรหัสก่อนการสแกน ในการลดเวลาที่จำเป็นในการเข้ารหัส/ถอดรหัสข้อมูลโดยการใช้ HP ProtectTools Embedded Security EFS ผู้ใช้ไม่ควรยกเลิกการใช้งาน Auto-Protect บน Symantec Antivirus หรือ Norton Antivirus
ไม่สามารถบันทึกแหล่งจัดเก็บการเรียกคืนฉุกเฉินลงสื่อที่ถอดเข้าออกได้	หากผู้ใส่ MMC หรือการ์ด SD เมื่อกำลังสร้างพาธของแหล่งจัดเก็บการเรียกคืนฉุกเฉินระหว่าง Embedded Security Initialization ข้อความแสดงข้อผิดพลาดจะปรากฏขึ้น	สิ่งนี้ได้รับการออกแบบไว้แล้ว

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
		ไม่สนับสนุนการจัดเก็บของแหล่งจัดเก็บการเรียกคืนบนลงสื่อที่ถอดเข้าออกได้ แหล่งจัดเก็บการเรียกคืนสามารถจัดเก็บบนไดรฟ์เครือข่ายหรือไดรฟ์โลคัลอื่นๆ นอกจากไดรฟ์ C
ไม่สามารถเข้ารหัสข้อมูลใดๆ ในสภาพแวดล้อม Windows 2000 French (ฝรั่งเศส)	ไม่มีการเลือก **Encrypt** เมื่อคลิกขวาที่ไอคอนไฟล์	นี่คือการจำกัดของระบบปฏิบัติการของไมโครซอฟต์ หากเปลี่ยนพื้นเป็นอย่างอื่น (เช่น ฝรั่งเศส (แคนาดา)) แล้วการเลือก **Encrypt** จะปรากฏ ในการแก้ไขปัญหา ให้เข้ารหัสไฟล์ดังต่อไปนี้: คลิกขวาที่ไอคอนไฟล์และเลือก **Properties** > **Advanced** > **Encrypt Contents**
ข้อผิดพลาดที่เกิดขึ้นหลังจากเกิดไฟล์ดับขณะกำลังทำการควบคุมระหว่าง Embedded Security Initialization	หากไฟดับขณะทำการเริ่มต้นชิป Embedded Security ให้ทำตามปัญหาที่จะเกิดขึ้นต่อไปนี้: • เมื่อกำลังพยายามเพื่อเปิด Embedded Security Initialization Wizard ให้ปฏิบัติตามข้อผิดพลาดที่แสดงต่อไปนี้: **The Embedded security cannot be initialized since the Embedded Security chip has already an Embedded Security owner.** • เมื่อกำลังพยายามเพื่อเปิด User Initialization Wizard ให้ปฏิบัติตามข้อผิดพลาดที่แสดงต่อไปนี้: **The Embedded security is not initialized. To use the wizard, the Embedded Security must be initialized first.**	ปฏิบัติตามขั้นตอนในการกู้คืนจากการไฟดับต่อไปนี้: **หมายเหตุ:** ใช้ปุ่มลูกศรเพื่อเลือกหลายเมนู รายการเมนู และเพื่อเปลี่ยนค่า (ยกเว้นในกรณีที่ระบุเป็นอย่างอื่น) 1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ 2. กด F10 เมื่อข้อม **F10=Setup** ปรากฏบนหน้าจอ (หรือทันทีที่ไฟสัญญาณมอนิเตอร์สีเขียวติดสว่าง) 3. เลือกตัวเลือกภาษาที่เหมาะสม 4. กด Enter 5. เลือก **Security** > **Embedded Security** 6. ตั้งค่าตัวเลือก **Embedded Security Device** เป็น **Enable** 7. กด F10 เพื่อยอมรับการเปลี่ยนแปลง 8. เลือก **File** > **Save Changes and Exit** 9. กด ENTER 10. กด F10 เพื่อบันทึกการเปลี่ยนแปลงและออกจากยูทิลิตี F10 Setup
รหัสผ่านของ Computer Setup (F10) Utility สามารถถูกลบออกหลังจากการเปิดใช้งาน TPM Module	Enabling the TPM module requires a Computer Setup (F10) Utility password. เมื่อเปิดใช้งานโมดูลแล้ว ผู้ใช้สามารถนำรหัสผ่านออกได้ ซึ่งทำให้บุคคลใดก็ตามด้วยการเข้าใช้โดยตรงไปยังระบบเพื่อรีเซ็ตโมดูล TPM และทำให้เกิดการสูญเสียของข้อมูลที่เป็นไปได้	สิ่งนี้ได้รับการออกแบบไว้แล้ว รหัสผ่านของ Computer Setup (F10) Utility สามารถถูกนำออกโดยผู้ใช้ผู้ที่รู้รหัสผ่าน อย่างไรก็ตาม HP ขอแนะนำอย่างจริงจังให้มีรหัสผ่านของ Computer Setup (F10) Utility ป้องกันตลอดเวลา
ช่องใส่รหัสผ่านของ PSD ยุติการแสดงเมื่อระบบจะมีสถานะสแตนด์บาย	เมื่อผู้ใช้ล็อกออนระบบหลังจากทำการสร้าง PSD TPM จะแจ้งให้คุณใส่รหัสผ่านของ Basic User หากผู้ใช้ไม่ใส่รหัสผ่านและระบบเข้าสู่สแตนด์บาย กล่องโต้ตอบรหัสผ่านจะไม่มีอยู่อีกเมื่อผู้ใช้ดำเนินการต่อไป	สิ่งนี้ได้รับการออกแบบแล้ว ผู้ใช้ล็อกออฟแล้วกลับมาเพื่อดูช่องใส่รหัสผ่านของ PSD อีกครั้ง
ไม่จำเป็นต้องใช้รหัสผ่านเพื่อเปลี่ยนแปลง Security Platform Policies	เข้าใช้ Security Platform Policies (ทั้ง Machine และ User) โดยไม่จำเป็นต้องใช้รหัสผ่านของ TPM สำหรับผู้ใช้ที่มีสิทธิ์ของผู้ดูแลระบบบนระบบ	สิ่งนี้ได้รับการออกแบบ. ผู้ดูแลระบบใดๆ สามารถแก้ไข Security Platform Policies โดยที่มีหรือไม่มีการเริ่มต้นของผู้ใช้ TPM
Microsoft EFS จะไม่ทำงานได้อย่างสมบรูณ์ใน Windows 2000	ผู้ดูแลระบบสามารถเข้าใช้ข้อมูลที่เข้ารหัสบนระบบโดยที่ไม่รู้รหัสผ่านที่ถูกต้อง หากผู้ดูแลระบบป้อนรหัสผ่านไม่ถูกต้องหรือยกเลิกกล่องโต้ตอบรหัสผ่าน ไฟล์ที่เข้ารหัสจะเปิดเป็นหากผู้ดูแลระบบได้ใส่รหัสผ่านที่ถูกต้อง กรณีนี้ทั้งๆ ที่การตั้งค่าความปลอดภัยที่ใช้เมื่อทำการเข้ารหัสข้อมูลกรณีนี้ในบัญชีผู้ดูแลระบบแรกบน Windows 2000 เท่านั้น	กำหนดค่า Data Recovery Policy โดยอัตโนมัติเพื่อกำหนดผู้ดูแลระบบเป็นเอเจนต์การกู้คืน เมื่อคีย์ผู้ใช้ไม่สามารถนำกลับมาใช้ได้ (ในกรณีที่ใส่รหัสผ่านผิดหรือยกเลิกกล่องโต้ตอบ Enter Password) ไฟล์นี้จะถูกถอดรหัสโดยอัตโนมัติด้วยคีย์การเรียกคืน เนื่องจาก Microsoft EFS. สำหรับข้อมูลเพิ่มเติม โปรดดูที่บทความทางเทคนิคพื้นฐานความรู้ของ Microsoft Q257705 ที่ http://www.microsoft.com เอกสารไม่สามารถถูกเปิดโดยผู้ใช้ที่ไม่ใช่ผู้ดูแลระบบ

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
เมื่อดูใบรับรอง จะแสดงว่าไม่น่าเชื่อถือ	หลังจากการตั้งค่า HP ProtectTools และทำการรัน User Initialization Wizard ผู้ใช้สามารถดูใบรับรองที่ออก อย่างไรก็ตาม เมื่อดูใบรับรอว จะแสดงว่าไม่น่าเชื่อถือ ขณะที่ใบรับรองสามารถถูกติดตั้งที่จุดนี้โดยการคลิกที่ปุ่มติดตั้งการติดตั้งไม่ทำให้เชื่อถือได้	ใบรับรองที่ลงนามด้วยตัวเองไม่น่าเชื่อถือ ในสภาพแวดล้อมระดับองค์กรที่ถูกกำหนดค่าอย่างเหมาะสม ใบรับรอง EFS ที่ออกโดยหน่วยงานออกใบรับรองและน่าเชื่อถือทางออนไลน์
ข้อผิดพลาดที่เกิดของการเข้ารหัสและถอดรหัสเป็นระยะๆ: **ขั้นตอนนี้ไม่สามารถเข้าใช้ไฟล์ได้เพราะเป็นการถูกใช้โดยขั้นตอนอื่นๆ**	ข้อผิดพลาดที่เป็นระยะๆ อย่างยิ่งระหว่างการเกิดการเข้ารหัสหรือการถอดรหัสไฟล์ในระหว่างไฟล์ที่ถูกใช้โดยขั้นตอนอื่นๆ แม้ว่าไฟล์หรือโฟลเดอร์ที่ประมวลผลด้วยระบบปฏิบัติการหรือแอปพลิเคชั่นอื่นๆ	ในการแก้ไขการขัดข้อง: 1. เริ่มการทำงานของระบบใหม่ 2. ล็อกออฟ 3. ล็อกเข้ากลับ
การสูญเสียข้อมูลในแหล่งจัดเก็บที่ถอดเข้าออกได้ที่เกิดขึ้นหากแหล่งจัดเก็บที่ถูกถอดออกก่อนไปยังการสร้างหรือการโอนย้ายข้อมูลใหม่	การถอดแหล่งจัดเก็บขนาดกลางเช่น ฮาร์ดไดรฟ์ MultiBay ยังคงแสดง PSD ที่มีและไม่สร้างข้อผิดพลาดขณะที่กำลังเพิ่ม/แก้ไขข้อมูลไปยัง PSD หลังจากที่ระบบรีสตาร์ท PSD จะไม่แสดงให้เห็นการเปลี่ยนแปลงของไฟล์ที่เกิดขึ้นในขณะแหล่งจัดเก็บที่ถอดออกได้ที่ไม่มีอยู่	ปัญหานี้จะพบได้เฉพาะหากผู้ใช้เข้าใช้ PSD แล้วถอดฮาร์ดไดรฟ์ก่อนทำการสร้างหรือโอนย้ายข้อมูลใหม่เสร็จสมบูรณ์ หากผู้ใช้พยายามเข้าใช้ PSD เมื่อฮาร์ดไดรฟ์ที่ถอดเข้าออกได้ไม่มีอยู่ในปัจจุบัน ข้อความแสดงข้อผิดพลาดที่แสดงสถานะว่า **the device is not ready**
ระหว่างทำการถอนการติดตั้ง หากผู้ใช้ไม่เริ่มต้นผู้ใช้ทั่วไป และเปิดเครื่องมือการจัดการ ตัวเลือก **Disable** จะไม่มีอยู่ โปรแกรมลบการติดตั้งจะไม่ดำเนินการต่อไปจนกระทั่งเครื่องมือการจัดการจะถูกปิดลง	ผู้ใช้มีตัวเลือกของการถอนการติดตั้งโดยที่ไม่มีการยกเลิกการใช้งาน TPM หรือโดยการยกเลิกการใช้งาน TPM ก่อน (ผ่านเครื่องมือการจัดการ) จากนั้นทำการถอนการติดตั้ง การเข้าใช้เครื่องมือการจัดการจำเป็นต้องมีการเริ่มต้นคีย์ผู้ใช้ทั่วไป หากการเริ่มต้นพื้นฐานไม่เกิดขึ้น ตัวเลือกทั้งหมดไม่สามารถเข้าถึงผู้ใช้ได้ เนื่องจากผู้ใช้ได้เลือกเพื่อเปิดเครื่องมือการจัดการอย่างชัดเจน (โดยการคลิก **Yes** ในกล่องโต้ตอบการแจ้งเตือน **Click Yes to open Embedded Security Administration tool**) ให้ยกเลิกการติดตั้งรอจนกระทั่งเครื่องมือการจัดการถูกปิด หากผู้ใช้คลิก **No** ในกล่องโต้ตอบ จากนั้นเครื่องมือการจัดการจะไม่เปิดแน่นอนและขั้นตอนการถอนการติดตั้ง	เครื่องมือการจัดการที่ใช้สำหรับการยกเลิกการใช้งานชิป TPM แต่ตัวเลือกจะไม่สามารถใช้งานได้ยกเว้นคีย์ผู้ใช้ทั่วไปที่เริ่มต้นแล้ว หากไม่มี แล้วจากนั้นเลือก **OK** หรือ **Cancel** เพื่อที่จะดำเนินการต่อไปด้วยขั้นตอนการถอนการติดตั้ง
ระบบค้างเป็นระยะๆ เกิดขึ้นหลังจากการสร้าง PSD บน 2 บัญชีผู้ใช้และการใช้การสลับผู้ใช้แบบเร็วในการกำหนดค่าของระบบ 128-MB	ระบบอาจจะค้างโดยที่มีหน้าจอมืดรวมทั้งไม่มีการตอบสนองของแป้นพิมพ์และเมาส์แทนการแสดงของหน้ายินดีต้อนรับ (ล็อกออน) เมื่อการใช้การสลับแบบเร็วด้วย RAM ที่น้อยที่สุด	ข้อสงสัยของ Root Cause เป็นปัญหาไทม์มิ่งในการกำหนดค่าหน่วยความจำต่ำ กราฟิกภายในที่ใช้สถาปัตยกรรม UMA การนำเอา 8 MB ของหน่วยความจำ และเหลือ 120 เท่านั้นให้กับผู้ใช้ 120 MB นี้ถูกแชร์ด้วยทั้งผู้ใช้ที่ได้ล็อกเข้าแล้วและการสลับผู้ใช้แบบเร็วเมื่อเกิดข้อผิดพลาด แนวทางการแก้ไขเพื่อรีบูตระบบและสนับสนุนลูกค้าให้เพิ่มการกำหนดค่าหน่วยความจำ (HP ไม่จัดจำหน่ายการกำหนดค่า 128-MB โดยค่าเริ่มต้นด้วยโมดูลความปลอดภัย)
EFS User Authentication (การร้องขอรหัสผ่าน) หมดเวลาด้วย **access denied**	รหัสผ่านของ EFS User Authentication เปิดหลังจากการคลิก **OK** อีกครั้งหรือกลับจากสถานะสแตนด์บายหลังจากหมดเวลา	วัตถุประสงค์นี้ออกแบบมาเพื่อให้หลีกเลี่ยงปัญหากับ Microsoft EFS เมื่อสร้าง 30-second watchdog timer เพื่อสร้างข้อความแสดงข้อผิดพลาด)
การย่อรองระหว่างการตั้งค่าของ Japanese ที่พบได้ในคำอธิบายการทำงาน	คำอธิบานการทำงานระหว่างกำหนดตัวเลือกการตั้งค่าด้วยตัวเองระหว่างตัวช่วยการติดตั้งที่ถูกย่อ	HP จะแก้ไขให้ถูกต้องในการออกในภายหน้า
EFS Encryption ทำงานได้โดยที่ไม่ต้องมีการใส่รหัสผ่านในการแจ้งเตือน	โดยการอนุญาตให้แจ้งเตือนสำหรับรหัสผ่านของผู้ใช้หมดเวลา การถอดรหัสยังคงสามารถทำได้บนไฟล์หรือโฟลเดอร์	ความสามารถในการเข้ารหัสไม่จำเป็นต้องทำการตรวจสอบความถูกต้องของรหัสผ่าน เนื่องคุณสมบัตินี้เป็นของการเข้ารหัสของ Microsoft EFS การถอดรหัสจำเป็นต้องใช้รหัสผ่านของผู้ใช้เพื่อป้อนลงไป
สนับสนุนอีเมลเพื่อความปลอดภัย แม้ว่าจะไม่ได้เลือกใน User Initialization Wizard หรือหากการกำหนดค่าอีเมลเพื่อความปลอดภัยถูกยก	ซอฟต์แวร์ความปลอดภัยแบบฝังตัวและตัวช่วยไม่ควบคุมการตั้งค่าของไคลเอนต์อีเมล (Outlook, Outlook Express หรือ Netscape)	ลักษณะแบบนี้ได้รับการออกแบบไว้แล้ว การกำหนดค่าของการตั้งค่าอีเมล TPM ไม่ได้ห้ามการตั้งค่าการเข้ารหัสการแก้ไขในอไคลเอนต์อีเมลโดยตรง การใช้ของอีเมลเพื่อความปลอดภัยได้ตั้งค่าและถูกควบคุมโดยแอปพลิเคชั่นของผู้ผลิตรายอื่น ตัวช่วย HP

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
เลิกการใช้งานในนโยบายสำหรับผู้ใช้		อนุญาตให้การเชื่อมต่อไปยังสามแอปพลิเคชั่นที่อ้างอิงกำหนดได้ด้วยตัวเองโดยทันที
การรันการใช้งานขนาดใหญ่ครั้งที่สองบนเครื่องคอมพิวเตอร์เครื่องเดียวกันหรือบนเครื่องคอมพิวเตอร์ที่เริ่มต้นก่อนหน้านี้เขียนทับการกู้คืนฉุกเฉินและไฟล์โทเคนฉุกเฉิน ไฟล์ใหม่จะไม่มีผลสำหรับการกู้คืน	การรันการใช้งานขนาดใหญ่บนระบบของ HP ProtectTools Embedded Security ที่ได้เริ่มต้นก่อนหน้านี้จะทำการเรนเดอร์แหล่งจัดเก็บสำหรับการกู้คืนที่มีอยู่และโทเคนการกู้คืนซึ่งจะไม่มีผลกับการเขียนทับของไฟล์ xml	HP ทำงานเพื่อแก้ไขปัญหาการเขียนทับไฟล์ xml และจะจัดเตรียมโซลูชันไว้ใน SoftPaq ในอนาคต
สคริปต์ล็อกออนโดยอัตโนมัติจะไม่ทำงานระหว่างผู้ใช้ทำการเรียกคืนใน Embedded Security	ข้อผิดพลาดเกิดขึ้นหลังจากผู้ใช้ • เจ้าของและผู้ใช้เริ่มต้นใน Embedded Security (การใช้ตำแหน่งเริ่ม–**My Documents**) • รีเซ็ตชิปให้เป็นการตั้งค่าจากโรงงานใน BIOS • รีบูตคอมพิวเตอร์ • เริ่มต้นเพื่อเรียกคืน Embedded Security ในระหว่างขั้นตอนการเรียกคืน Credential Manager จะแจ้งให้ผู้ใช้หากระบบสามารถล็อกออนไปยัง Infineon TPM User Authentication โดยอัตโนมัติ หากผู้ใช้เลือก **Yes** จากนั้นตำแหน่งของ SPEmRecToken จะปรากฏขึ้นในกล่องข้อความโดยอัตโนมัติ แม้ว่าตำแหน่งนี้จะถูกต้อง ข้อความแสดงข้อผิดพลาดต่อไปนี้จะปรากฏขึ้น: **No Emergency Recovery Token is provided. Select the token location the Emergency Recovery Token should be retrieved from.**	คลิกที่ปุ่ม **Browse** บนหน้าจอเพื่อเลือกตำแหน่ง และขั้นตอนการประมวลการเรียกคืน
Multiple User PSD ไม่ทำงานในสภาพแวดล้อมการสลับผู้ใช้แบบเร็ว	ข้อผิดพลาดนี้เกิดขึ้นเมื่อผู้ใช้หลายคนได้สร้างและใช้ PSD ด้วยชื่อไดรฟ์เดียวกัน หากพยายามสร้างการสลับผู้ใช้แบบเร็วระหว่างผู้ใช้เมื่อโหลด PSD แล้ว PSD ของผู้ใช้ที่สองจะไม่สามารถใช้งานได้	PSD ของผู้ใช้ที่สองจะสามารถใช้งานได้ หากไ ดักำหนดค่าเพื่อใช้ตัวอักษรไดรฟ์อื่นๆ หรือหากผู้ใช้คนแรกได้ล็อกออฟแล้ว
PSD ถูกยกเลิกการใช้งานและไม่สามารถตรวจสอบได้หลังทำการฟอร์แมตฮาร์ดไดรฟ์บนที่สร้าง PSD ขึ้น	The PSD is disabled and cannot be deleted after formatting the secondary hard drive on which the PSD was generated. ไอคอน PSD ยังสามารถมองเห็นได้ แต่ข้อความแสดงข้อผิดพลาด **drive is not accessible** จะปรากฏขึ้นเมื่อผู้ใช้พยายามเข้าใช้ PSD ผู้ใช้ไม่สามารถลบ PSD และข้อความที่ปรากฏที่สถานะ: **Your PSD is still in use, please ensure that your PSD contains no open files and is not accessed by another process**. ผู้ใช้ต้องรีบูตระบบเพื่อที่จะลบ PSD และไม่โหลดหลังจากรีบูต	ตามที่ออกแบบ: หากลูกค้าลบหรือยกเลิกการเชื่อมต่อตำแหน่งการจัดเก็บของข้อมูล PSD การจำลองไดรฟ์ Embedded Security PSD ให้ดำเนินการทำงานต่อไป รวมทั้งจะสร้างข้อผิดพลาดขาดการติดต่อสื่อสารที่ไม่พบข้อมูล ความละเอียด: หลังจากรีบูตครั้งต่อไป การจำลองจะไม่โหลดและผู้ใช้สามารถลบการจำลอง PSD เดิมและสร้าง PSD ใหม่
ข้อผิดพลาดภายในที่ได้ตรวจสอบการเรียกคืนจากแหล่งจัดเก็บการสำรองข้อมูลโดยอัตโนมัติ	หากผู้ใช้ • คลิกตัวเลือก **Restore under Backup** ของ Embedded Security ใน HPPTSM เพื่อเรียกคืนจากแหล่งจัดเก็บการสำรองข้อมูลโดยอัตโนมัติ • เลือก **SPSystemBackup .xml**	หากผู้ใช้เลือก **SpSystemBackup.xml** เมื่อจำเป็นต้องใช้ SpBackupArchive.xml Embedded Security Wizard จะไม่ทำงานโดยมี: **An internal Embedded Security error has been detected.** ผู้ใช้ต้องเลือกไฟล์ .xml ที่ถูกต้องเพื่อให้เข้ากับเหตุผลที่ต้องการ ขั้นตอนนี้ทำงานโดยได้รับการออกแบบและทำงานอย่างถูกต้อง อย่างไรก็ตาม ข้อความแสดงข้อผิดพลาด Embedded Security

คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
	ตัวช่วยการเรียกคืนไม่ทำงานและข้อความแสดงข้อผิดพลาดต่อไปนี้จะปรากฏขึ้น: **The selected Backup Archive does not match the restore reason. Please select another archive and continue.**	ภายในไม่ได้ลบและควรกำหนดข้อความที่เหมาะสมเพิ่มเติม HP ทำงานเพื่อเพิ่มประสิทธิภาพให้ผลิตภัณฑ์นี้ดียิ่งขึ้นในอนาคต
ระบบความปลอดภัยแสดงข้อผิดพลาดการเรียกคืนที่มีผู้ใช้หลายคน	ระหว่างขั้นตอนการเรียกคืน หากผู้ดูแลระบบเลือกผู้ใช้เพื่อเรียกคืน ผู้ใช้ที่ไม่ได้รับเลือกจะไม่สามารถเรียกคืนคีย์เมื่อพยายามเรียกคืนในภายหลังได้ ข้อความแสดงข้อผิดผลาด **decryption process failed** จะปรากฏขึ้น	ผู้ใช้ที่ไม่ได้รับเลือกสามารถได้รับการเรียกคืนโดยการรีเซ็ต TPM การรันขั้นตอนการเรียกคืน และการเลือกผู้ใช้ทั้งหมดก่อนค่าเริ่มต้นประจำวันครั้งต่อไปกลับทำงาน หากการรันการสำรองข้อมูลโดยอัตโนมัติ จะเขียนทับผู้ใช้ที่ไม่ได้เรียกคืนและข้อมูลเหล่านั้นสูญหาย หากการสำรองข้อมูลระบบใหม่ถูกจัดเก็บ ผู้ใช้ที่ไม่ได้รับเลือกก่อนหน้านี้ไม่สามารถจัดเก็บได้ นอกจากนี้ ผู้ใช้ต้องเรียกคืนการสำรองข้อมูลระบบทั้งหมด การสำรองข้อมูลของแหล่งจัดเก็บสามารถสามารถเรียกคืนทีละอย่างได้
การรีเซ็ต ROM ระบบเป็นค่าเริ่มต้นที่ซ่อน TPM	การรีเซ็ต ROM ระบบเป็นค่าเริ่มต้นที่ซ่อน TPM ไปยัง WindowsResetting the system ROM to default hides the TPM to Windows. กรณีนี้ไม่อนุญาตให้ซอฟต์แวร์ความปลอดภัยเพื่อดำเนินการอย่างถูกต้องและสร้าง ข้อมูล TPM ที่เข้ารหัสที่ไม่สามารถเข้าถึงได้	ไม่ซ่อน TPM ใน BIOS: เปิดยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) ให้นำทางไปยัง **Security** > **Device security** แก้ไขช่องข้อมูลจาก **Hidden** เป็น **Available**
การสำรองข้อมูลโดยอัตโนมัติจะไม่ทำงานร่วมกับการใช้ไดรฟ์ของผู้อื่น	เมื่อผู้ดูแลระบบตั้งค่าการสำรองข้อมูลโดยอัตโนมัติใน Embedded Security จะสร้างรายการใน **Windows** > **Tasks** > **Scheduled Task** Windows Scheduled Task ตั้งค่าเพื่อใช้ NT AUTHORITY\SYSTEM สำหรับสิทธิ์ในการทำการสำรองข้อมูล การทำงานได้อย่างถูกต้องนี้ที่ไดรฟ์โลคัลใดๆ เมื่อผู้ดูแลระบบกำหนดค่าแทนที่การสำรองข้อมูลโดยอัตโนมัติเพื่อบันทึกการใช้ไดรฟ์ของผู้อื่น ข้อผิดพลาดการประมวลผลเนื่องจาก NT AUTHORITY\SYSTEM ไม่มีสิทธิ์ในการใช้ไดรฟ์ของผู้อื่น หากการสำรองข้อมูลโดยอัตโนมัติได้กำหนดการในการเกิดขึ้นเมื่อล็อกเข้า Embedded Security TNA Icon จะแสดงข้อความดังต่อไปนี้: **The Backup Archive location is currently not accessible. Click here if you want to backup to a temporary archive until the Backup Archive is accessible again.** หากการสำรองข้อมูลโดยอัตโนมัติสำหรับเวลาที่ระบุ อย่างไรก็ตาม ข้อผิดพลาดการสำรองข้อมูลจะไม่มีการแสดงการแจ้งข้อผิดพลาด	แนวทางการแก้ไขในการเปลี่ยน NT AUTHORITY\SYSTEM เป็น (ชื่อคอมพิวเตอร์)\(ชื่อผู้ดูแล) นี่เป็นการตั้งค่าเริ่มต้นหากได้สร้าง Scheduled Task ด้วยตัวเอง HP ทำงานเพื่อจัดเตรียมการออกผลิตภัณฑ์ในอนาคตด้วยการตั้งค่าเริ่มต้นที่มีชื่อคอมพิวเตอร์\ชื่อผู้ดูแลระบบ
ไม่สามารถยกเลิกการใช้งาน Embedded Security State ชั่วคราวใน Embedded Security GUI	ซอฟต์แวร์ 4.0 ปัจจุบันได้รับการออกแบบเพื่อมาตรฐาน HP Notebook 1.1B รวมทั้งการสนับสนุนมาตรฐาน HP Desktop 1.2 ตัวเลือกที่ยกเลิกการใช้งานนี้ยังคงสนับสนุนในอินเตอร์เฟซซอฟต์แวร์สำหรับแพล็ตฟอร์ม TPM 1.1	HP จะจัดการปัญหานี้ในการออกในภายหน้า

เบ็ดเตล็ด

Software Impacted—คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
HP ProtectTools Security Manager—ได้รับคำเตือน: **The security application can not be installed until the HP Protect Tools Security Manager is installed**.	แอปพลิเคชั่นความปลอดภัยทั้งหมด เช่น Embedded Security, Java Card และไบโอเมตริกเป็นปลั๊กอินที่ขยายอินเทอร์เฟซของ HP Security Manager Security Manager ต้องถูกติดตั้งก่อนที่ปลั๊กอินความปลอดภัย HP ที่อนุมัติสามารถโหลด	ซอฟต์แวร์ HP ProtectTools Security Manager ต้องถูกติดตั้งก่อนการติดตั้งปลั๊กอินความปลอดภัยใดๆ
HP ProtectTools TPM Firmware Update Utility สำหรับ dc7600 และรุ่นที่มี Broadcom เปิดใช้งาน TPMs—เครื่องมือที่จัดเตรียมผ่านรายงานเว็บไซต์การสนับสนุนของ HP **ownership required**	นี่เป็นลักษณะที่คาดไว้ของยูทิลิตีเฟิร์มแวร์ TPM สำหรับ dc7600 และรุ่นที่มี Broadcom ที่เปิดใช้งาน TPM เครื่องมือการอัพเกรดเฟิร์มแวร์อนุญาตให้ผู้ใช้อัพเกรดเฟิร์มแวร์ โดยที่มีหรือไม่มีคีย์การรับรอง (EK) เมื่อไม่มี EK ไม่จำเป็นต้องมีการตรวจสอบความถูกต้องเพื่อให้การอัพเกรดเฟิร์มแวร์สมบรูณ์ เมื่อมี EK เจ้าของ TPM ต้องมีอยู่ เนื่องจากการอัพเกรดต้องการการตรวจสอบความถูกต้องของเจ้าของ หลังจากทำการอัพเกรดเสร็จสมบรูณ์ แพล็ตฟอร์มต้องถูกรีสตาร์ทเพื่อให้เฟิร์มแวร์ใหม่นี้มีผลใช้ หาก BIOS TPM ได้รีเซ็ตเป็นค่าจากโรงงาน ความเป็นเจ้าของจะถูกลบและความสามารถในการอัพเดตเฟิร์มแวร์จะถูกป้องกันจนกระทั่งได้กำหนดค่าแพล็ตฟอร์ม Embedded Security Software และ User Initialization Wizard แล้ว *ขอแนะนำให้ทำการรีบูตหลังจากทำการอัพเดตเฟิร์มแวร์เสมอ เวอร์ชันของเฟิร์มแวร์จะไม่ถูกระบุอย่างถูกต้องจนกระทั่งหลังจากทำการรีบูต	1. ติดตั้ง HP ProtectTools Embedded Security Software ใหม่ 2. เปิดแพล็ตฟอร์มและตัวช่วยการกำหนดค่าผู้ใช้ 3. ตรวจดูให้แน่ใจว่าระบบได้มีการติดตั้ง Microsoft .NET framework 1.1 : a. คลิก **Start** b. คลิก **Control Panel** c. คลิก **Add or remove programs** d. ตรวจดูว่า **Microsoft .NET Framework 1.1** อยู่ในรายการ 4. ตรวจสอบการกำหนดค่าฮาร์ดแวร์และซอฟต์แวร์: a. คลิก **Start** b. คลิก **All Programs** c. คลิก **HP ProtectTools Security Manager** d. เลือก **Embedded Security** จากเมนูย่อย e. คลิก **More Details** ระบบควรมีการกำหนดค่าต่อไปนี้: • เวอร์ชันของผลิตภัณฑ์ = V4.0.1 • Embedded Security State: Chip State = เปิดใช้งานแล้ว, Owner State = เริ่มต้นแล้ว, User State = เริ่มต้นแล้ว • ข้อมูลส่วนประกอบ: TCG Spec. เวอร์ชัน = 1.2 • ผู้จำหน่าย = Broadcom Corporation • เวอร์ชันของ FW = 2.18 (หรือสูงกว่า) • เวอร์ชันไลบรารีไดรเวอร์ TPM Device 2.0.0.9 (หรือสูงกว่า) 5. หากเวอร์ชันของ FW ไม่ตรงกับ 2.18 ให้ดาวน์โหลดและอัพเดตเฟิร์มแวร์ TPM TPM Firmware SoftPaq มีให้ดาวน์โหลดการสนับสนุนที่ http://www.hp.com
HP ProtectTools Security Manager—บางครั้งข้อผิดพลาดอาจเกิดขึ้นอีกเมื่อปิดอินเทอร์เฟซ Security Manager	บางครั้ง (1 ใน 12 กรณี) ข้อผิดพลาดที่เกิดขึ้นโดยการใช้ปุ่มปิดที่อยู่ด้านขวาบนของหน้าจอเพื่อปิด Security Manager ก่อนแอปพลิเคชั่นปลั๊กอินทั้งหมดได้ทำการโหลดเสร็จสิ้น	ซึ่งเกี่ยวข้องกับไทม์มิงเฉพาะตัวบนเวลาการโหลดบริการปลั๊กอิน เมื่อการปิดและรีสตาร์ท Security Manager เนื่องจาก PTHOST.exe เป็นการเฮาส์ซิ่งเชลล์ของแอปพลิเคชั่นอื่น (ปลั๊กอิน) ซึ่งขึ้นอยู่กับความสามารถของปลั๊กอินเพื่อให้เวลาโหลดเสร็จสมบรูณ์ (บริการ) การปิดเชลล์ก่อนที่ปลั๊กอินมีเวลาในการให้การโหลดเป็น root cause เสร็จสมบรูณ์

Software Impacted—คำอธิบายย่อ	รายละเอียด	วิธีแก้ไข
		อนุญาตให้ Security Manager เพื่อให้บริการการโหลดข้อความเสร็จสมบรูณ์ (สามารถพบได้ที่ด้านบนของหน้าต่าง Security Manager) และปลั๊กอินที่อยู่ในรายการทางคอลัมน์ด้านซ้าย ในการหลีกเลี่ยงข้อผิดพลาด ให้ระยะเวลาอันเหมาะสมสำหรับปลั๊กอินเหล่านี้เพื่อโหลด
HP ProtectTools * General —Unrestricted เข้าใช้หรือไม่ควบคุมสิทธิ์ผู้ดูแลระบบความเสี่ยงด้านความปลอดภัย	ความเสี่ยงต่างๆ ที่อาจเกิดขึ้นได้กับเข้าใช้ที่ไม่บังคับไปที่คอมพิวเตอร์ไคลเอนต์: • การลบของ PSD • การแก้ไขการประสงค์ร้ายของการตั้งค่าผู้ใช้ • การยกเลิกของนโยบายด้านความปลอดภัยและการทำงาน	ผู้ดูแลระบบสนับสนุนให้ปฏิบัติตาม “แนวทางที่เหมาะสม” ในการจำกัดสิทธิ์ของผู้ใช้ทั่วไปและการจำกัดการเข้าใช้ของผู้ใช้ ผู้ใช้ที่ไม่ได้รับการตรวจสอบความถูกต้องไม่ควรได้สิทธิ์การจัดการที่อนุมัติ
BIOS และรหัสผ่านของ OS Embedded Security ออกจากซิงค์	หากผู้ใช้ไม่ตรวจสอบความถูกต้องรหัสผ่านที่เป็นรหัสผ่านของ BIOS Embedded Security รหัสผ่านของ BIOS Embedded Security จะย้อนกลับไปเป็นรหัสผ่านด้านความปลอดภัยแบบฝังตัวผ่าน F10 BIOS	นี่เป็นการทำงานที่ได้รับการออกแบบแล้ว รหัสผ่านเหล่านี้สามารถซิงโครไนส์ได้อีกโดยการเปลี่ยนรหัสผ่านของ OS Basic User และตรวจสอบความถูกต้องที่การแจ้งเตือนรหัสผ่านของ BIOS Embedded Security
เฉพาะผู้ใช้สามารถล็อกออนไปที่ระบบหลังจากการตรวจความถูกต้องการบูตล่วงหน้าของ TPM ที่เปิดใช้งานใน BIOS	TPM BIOS PIN ที่เกี่ยวข้องกับผู้ใช้แรกที่เริ่มต้นการตั้งค่าผู้ใช้ หากคอมพิวเตอร์หนึ่งเครื่องมีผู้ใช้หลายคน ผู้ใช้แรกที่สำคัญ คือผู้ดูแลระบบ ผู้ใช้แรกจะให้รหัส PIN ผู้ใช้ของ TPM กับผู้ใช้อื่นเพื่อใช้ในการล็อกเข้า	นี่เป็นการทำงานที่ได้รับการออกแบบแล้ว HP ขอแนะนำให้แผนกไอทีของลูกค้าให้ทำตามนโยบายความปลอดภัยที่ดีสำหรับการสร้างโซลูชันรักษาความปลอดภัยและตรวจดูให้รหัสผ่านของผู้ดูแลระบบ BIOS ที่ถูกกำหนดค่าโดยผู้ดูแลระบบไอทีสำหรับการป้องกันระดับของระบบ
ผู้ใช้ได้เปลี่ยนรหัส PIN เพื่อสร้างการทำงานการบูต TPM ล่วงหน้าหลังจากการรีเซ็ตค่าจากโรงงานของ TPM	ผู้ใช้ได้เปลี่ยนรหัส PIN หรือสร้างผู้ใช้อื่นๆ เพื่อเริ่มต้นการตั้งค่าเพื่อสร้างการทำงานการตรวจสอบความถูกต้อง BIOS ของ TPM หลังจากรีเซ็ต ไม่มีตัวเลือกเพื่อสร้างการทำงานการตรวจสอบความถูกต้อง BIOS ของ TPM	สิ่งนี้ได้รับการออกแบบไว้แล้ว การรีเซ็ตเป็นค่าจากโรงงานจะลบคีย์ผู้ใช้เบื้องต้น ผู้ใช้ต้องเปลี่ยนรหัส PIN ผู้ใช้หรือสร้างผู้ใช้ของเขาเพื่อเริ่มต้นคีย์ผู้ใช้เบื้องต้น
Power-on authentication support ไม่ได้ตั้งค่าเริ่มต้นโดยการใช้ Embedded Security **Reset to Factory Settings**	ในการตั้งค่าคอมพิวเตอร์ ตัวเลือก **Power-on authentication support** จะไม่ได้รีเซ็ตเป็นการตั้งค่าจากโรงงานเมื่อใช้ตัวเลือก Embedded Security Device **Reset to Factory Settings** โดยค่าเริ่มต้น **Power-on authentication support** ตั้งค่าเป็น **Disable**	ตัวเลือก **Reset to Factory Settings** ยกเลิกใช้งาน Embedded Security Device ซึ่งซ่อนตัวเลือก Embedded Security อื่น (รวมถึง **Power-on authentication support**) อย่างไรก็ตาม หลังจากเปิดการใช้งาน Embedded Security Device ใหม่ เปิดการใช้งาน **Power-on authentication support** ที่มีอยู่แล้ว HP ทำงานเพื่อการแก้ไขปัญหา ที่จะจัดเตรียมไว้ในข้อเสนอของ ROM SoftPaq บนเว็บในอนาคต
การตรวจสอบเมื่อเปิดระบบรักษาความปลอดภัยไว้ซ้อนทับรหัสผ่าน BIOS ระหว่างลำดับการบูต	การตรวจสอบเมื่อเปิดเครื่องจะแจ้งเตือนผู้ใช้ให้ล็อกออนไปยังระบบโดยการใช้รหัสผ่านของ TPM แต่หากผู้ใช้กด F10 เพื่อเข้าใช้ BIOS อ่านสิทธิ์การเข้าใช้ที่ได้รับการอนุมัติเท่านั้น	ความสามารถในการเขียน BIOS ผู้ใช้ต้องใส่รหัสผ่าน BIOS แทนที่รหัสผ่านของ TPM ที่หน้าต่างการตรวจสอบเมื่อเปิดเครื่อง
BIOS จะแจ้งให้คุณใส่รหัสผ่านทั้งเก่าและใหม่ผ่านการตั้งค่าคอมพิวเตอร์หลังจากการเปลี่ยนรหัสผ่านของเจ้าของในซอฟต์แวร์ Embedded Security Windows	BIOS จะแจ้งให้คุณใส่รหัสผ่านทั้งเก่าและใหม่ผ่านการตั้งค่าคอมพิวเตอร์หลังจากการเปลี่ยนรหัสผ่านของเจ้าของในซอฟต์แวร์ Embedded Security Windows	สิ่งนี้ได้รับการออกแบบไว้แล้ว เนื่องจากไม่มีความสามารถของ BIOS ในการติดต่อสื่อสารด้วย TPM เมื่อระบบปฏิบัติการเริ่มขึ้นและกำลังทำงาน รวมทั้งเพื่อตรวจสอบ TPM ผ่านวิธีที่ขัดแย้งกับ blob คีย์ของ TPM

ประมวลคำศัพท์

DriveLock คุณสมบัติด้านความปลอดภัยที่เชื่อมโยงฮาร์ดไดรฟ์ไปยังผู้ใช้และผู้ใช้จำเป็นต้องพิมพ์รหัสผ่าน DriveLock ให้ถูกต้องเมื่อเริ่มคอมพิวเตอร์

Encryption File System (EFS) ระบบที่เข้ารหัสไฟล์และโฟลเดอร์ย่อยทั้งหมดภายในโฟลเดอร์ที่เลือก

Java Card ชิ้นส่วนเล็กๆ ของฮาร์ดแวร์ คล้ายกับขนาดและรูปร่างของบัตรเครดิต ซึ่งจัดเก็บข้อมูลการระบุที่เกี่ยวกับเจ้าของ ใช้เพื่อตรวจสอบความถูกต้องเจ้าของไปที่คอมพิวเตอร์

Public Key Infrastructure (PKI) มาตรฐานที่กำหนดอินเตอร์เฟซสำหรับการสร้าง ใช้งาน และจัดการใบรับรองและคีย์สำหรับการเข้ารหัส

การตรวจสอบความถูกต้อง ขั้นตอนของการตรวจสอบว่าผู้ใช้ได้รับการตรวจสอบแล้วเพื่อทำงาน การเข้าใช้คอมพิวเตอร์ การแก้ไขการตั้งสำหรับโปรแกรมโดยเฉพาะ หรือการดูข้อมูลที่ปลอดภัย

การตรวจสอบความถูกต้องเมื่อเปิดเครื่องไว้ คุณสมบัติด้านความปลอดภัยที่จำเป็นต้องมีบางแบบฟอร์มของการตรวจสอบความถูกต้อง เช่น Java Card ชิปความปลอดภัย หรือ รหัสผ่าน เมื่อเปิดคอมพิวเตอร์แล้ว

การถอดรหัสลับ กระบวนการที่ใช้ในการเข้ารหัสเพื่อแปลงข้อมูลที่เข้ารหัสให้กลายเป็นข้อความล้วน

การลงชื่อเข้าใช้เพียงครั้งเดียว (Single Sign On) คุณสมบัติที่จัดเก็บข้อมูลการตรวจสอบความถูกต้องและให้คุณใช้ Credential Manager เพื่อเข้าใช้แอปพลิเคชั่นอินเทอร์เน็ตและ Windows ที่จำเป็นต้องใช้การตรวจสอบความถูกต้องรหัสผ่า

การเข้ารหัสลับ แนวทางของการเข้ารหัสและการถอดรหัสข้อมูลเพื่อให้บุคคลใดบุคคลหนึ่งสามารถถอดรหัสข้อมูลดังกล่าว

การเข้ารหัสลับ ขั้นตอน เช่นการใช้ของอัลกอริธึม ใช้เพื่อเข้ารหัสเพื่อแปลงข้อความล้วนให้กลายเป็นข้อความรหัส เพื่อป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุาตสามารถอ่านข้อมูลนั้นๆ การเข้ารหัสข้อมูลมีหลายชนิด และเป็นพื้นฐานสำหรับระบบรักษาความปลอดภัยบนเน็ตเวิร์ก ชนิดที่ใช้ทั่วไปคือ มาตรฐานการเข้ารหัสข้อมูล (Data Encryption Standard) และการเข้ารหัสโดยใช้คีย์สาธารณะ

การเปลี่ยนย้าย งานที่ช่วยให้สามารถจัดการ กู้คืน และถ่ายโอนคีย์และใบรับรอง

ชิปความปลอดภับ Trusted Platform Module (TPM) แบบฝังตัว (เฉพาะบางรุ่น) ชิปความปลอดภัยภายในที่สามารถป้องกัยข้อมูลของผู้ใช้ที่มีความละเอียดอ่อนสูงจากผู้ประสงค์ร้าย เป็น root-of-trust ในแพล็ตฟอร์มที่ให้ TPM จัดเตรียมอัลกอริที่มการเข้ารหัสและดำเนินการที่ตรงกับข้อกำหนดของ Trusted Computing Group (TCG)

ตัวตน ใน HP ProtectTools Credential Manager กลุ่มของใบรับรองและการตั้งค่าที่จัดการเหมือนบัญชีหรือโปรไฟล์สำหรับผู้ใช้เฉพาะ

บัญชีผู้ใช้ของ Windows โปรไฟล์ที่ได้รับอนุญาตส่วนตัวเพื่อล็อกออนไปที่เครือข่ายหรือไปคอมพิวเตอร์ส่วนบุคคล

บัญชีเน็ตเวิร์ก ผู้ใช้หรือบัญชีผู้ดูแลระบบของ Windows บนคอมพิวเตอร์โลคัลในเวิร์กกรุ๊ป หรือบนโดเมน

ผู้ให้บริการเข้ารหัส (CSP) ผู้จัดหาหรือไลบรารีของอัลกอริธึมการเข้ารหัสที่สามารถใช้ในอินเตอร์เฟซที่ได้รับการกำหนดอย่างแน่ชัดเพื่อดำเนินฟังก์ชันการเข้ารหัสเฉพาะ

พาร์ติชัน FAT ตารางการแบ่งส่วนไฟล์ หนึ่งวิธีของสื่อการจัดเก็บการทำดัชนี

พาร์ติชัน NTFS ระบบไฟล์ NT หนึ่งวิธีของสื่อการจัดเก็บการทำดัชนี วิธีนี้เป็นมาตรฐานใน Windows Vista และ Windows XP

ระบบรักษาความปลอดภัยที่เข้มงวด คุณสมบัติความปลอดภัยใน BIOS ที่จัดเตรียมการป้องกันที่เพิ่มขึ้นสำหรับรหัสผ่านการป้องกันการเปิดเครื่องและรหัสผ่านผู้ดูแลระบบและฟอร์มอื่นของการตรวจสอบความถูกต้องการเปิดเครื่อง

รีบูต ขั้นตอนของการรีสตาร์ทคอมพิวเตอร์

ลายเซ็นดิจิตอล ข้อมูลที่ส่งกับไฟล์ที่ตรวจสอบผู้ส่งของวัสดุ และที่ไฟล์ที่ไม่ได้รับการแก้ไขหลังจากที่ลงนาม

สมาร์ทการ์ด ชิ้นส่วนเล็กๆ ของฮาร์ดแวร์ คล้ายกับขนาดและรูปร่างของบัตรเครดิต ซึ่งจัดเก็บข้อมูลการระบุที่เกี่ยวกับเจ้าของ ใช้เพื่อตรวจสอบความถูกต้องเจ้าของไปที่คอมพิวเตอร์

หน่วยงานออกใบรับรอง บริการออกใบรับรองที่จำเป็นสำหรับการใช้ Public Key Infrastructure

แหล่งจัดเก็บการกู้คืนฉุกเฉิน พื้นที่จัดเก็บข้อมูลที่ได้รับการคุ้มครอง ซึ่งช่วยให้สามารถทำการเข้ารหัสซ้ำสำหรับคีย์ผู้ใช้ทั่วไปจากคีย์เจ้าของแพลตฟอร์มหนึ่งไปยังคีย์อื่น

โดเมน กลุ่มของคอมพิวเตอร์ที่เป็นส่วนของเครือข่ายและเซิร์ฐานข้อมูลไดเรกทอรีทั่วไป โดเมนที่มีชื่อเฉพาะ และแต่ละชุดของหน้าที่ทั่วไปและขั้นตอน

โทเคน USB อุปกรณ์ความปลอดภัยที่จัดเก็บข้อมูลการระบุที่เกี่ยวกับผู้ใช้ คล้ายกับตัวอ่าน Java Card หรือไบโอเมตริก ที่ใช้ในการตรวจสอบความถูกต้องของเจ้าของไปที่คอมพิวเตอร์

โทเคนเสมือนจริง คุณสมบัติด้านความปลอดภัยที่ทำงานเหมือนกับ Java Card และตัวอ่านการ์ด โทเคนจะถูกบันทึกไว้บนฮาร์ดไดรฟ์ของคอมพิวเตอร์หรือในรีจิสทรีของ Windows เมื่อคุณล็อกเข้าด้วยโทเคนเสมือนจริง ระบบจะขอให้คุณป้อนรหัส PIN ของผู้ใช้เพื่อทำการตรวจสอบความถูกต้องให้เสร็จสมบูรณ์

โปรไฟล์ของ BIOS กลุ่มของการตั้งค่าการกำหนดค่าของ BIOS ที่สามารถบันทึกและนำไปใช้ได้กับบัญชีอื่น

โหมดการรักษาความปลอดภัยของ BIOS การตั้งค่าใน Java Card Security นั้น เมื่อเปิดใช้งานแล้ว จำเป็นต้องใช้ Java Card และรหัส PIN ที่ถูกต้องสำหรับการตรวจสอบความถูกต้องของผู้ใช้

ใบรับรอง วิธีที่ผู้ใช้ตรวจสอบความเหมาะสมสำหรับงานเฉพาะในขั้นตอนการตรวจสอบความถูกต้อง

ใบรับรองดิจิตอล ใบรับรองอิเล็กทรอนิกส์ที่ยืนยันตัวตนของบุคคลหรือบริษัท โดยเชื่อมโยงตัวตนของเจ้าของใบรับรองดิจิตอลเข้ากับชุดคีย์อิเล็กทรอนิกส์ที่ใช้สำหรับเซ็นชื่อในข้อมูลดิจิตอล

ไดรฟ์ความปลอดภัยส่วนบุคคล (PSD) จะจัดเตรียมให้พื้นที่จัดเก็บที่ได้รับการคุ้มครองสำหรับข้อมูลสำคัญๆ

ไบโอเมตริก ประเภทของใบรับรองการตรวจสอบที่ใช้คุณสมบัติทางกายภาพ เช่น การพิมพ์ลายนิ้วมือเพื่อระบุผู้ใช้

ดัชนี