HP Client Security

การเริ่มต้นใช้งาน

ข้อมูลที่ระบุในที่นี้อาจมีการเปลี่ยนแปลงโดยไม่จำเป็นต้องแจ้งให้ทราบล่วงหน้า การรับประกันสำหรับผลิตภัณฑ์และบริการของ HP ระบุไว้อย่างชัดเจนในใบรับประกันที่ให้มาพร้อมกับผลิตภัณฑ์และบริการดังกล่าวเท่านั้น ข้อความในที่นี้ไม่ถือเป็นการรับประกันเพิ่มเติมแต่อย่างใด HP จะไม่รับผิดชอบต่อข้อผิดพลาดทางเทคนิคหรือภาษาหรือการละเว้นข้อความในที่นี้

พิมพ์ครั้งที่หนึ่ง: สิงหาคม 2013

หมายเลขเอกสาร: 735339-281

สารบัญ

1 การแนะนำสำหรับ HP Client Security Manager

HP Client Security ช่วยให้คุณป้องกันข้อมูล อุปกรณ์ และข้อมูลระบุตัวตน ซึ่งเป็นการเพิ่มความปลอดภัยของเครื่องคอมพิวเตอร์ของคุณ

โมดูลซอฟต์แวร์ที่มีสำหรับคอมพิวเตอร์ของคุณอาจจะแตกต่างกันไปขึ้นอยู่กับรุ่นของโมเดลของคุณ

โมดูลซอฟต์แวร์ HP Client Security อาจติดตั้งไว้ล่วงหน้า โหลดไว้ล่วงหน้า หรือมีให้ดาวน์โหลดจากเว็บไซต์ของ HP สำหรับข้อมูลเพิ่มเติม โปรดไปที่ http://www.hp.com

หมายเหตุ: คำแนะนำในคู่มือนี้จะถูกเขียนเป็นลายลักษณ์อักษรด้วยสมมุติฐานที่ว่าคุณได้ติดตั้งโมดูลซอฟต์แวร์ HP Client Security ที่ต้องการไว้อยู่แล้ว

คุณสมบัติของ HP Client Security

ตารางต่อไปนี้จะแสดงรายละเอียดสำหรับคุณสมบัติที่สำคัญของโมดูลซอฟต์แวร์ HP Client Security

โมดูล	คุณสมบัติหลัก
HP Client Security Manager	ผู้ดูแลระบบสามารถดำเนินการดังต่อไปนี้: • ปกป้องคอมพิวเตอร์ของคุณก่อน Windows® จะเริ่มทำงาน • ปกป้องบัญชี Windows ของคุณโดยใช้การรับรองความถูกต้องที่มีประสิทธิภาพ • จัดการข้อมูลล็อกออนและรหัสผ่านของคุณสำหรับเว็บไซต์และโปรแกรม • เปลี่ยนรหัสผ่านระบบปฏิบัติการ Windows อย่างง่ายดาย • ใช้ลายนิ้วมือเพื่อเพิ่มความปลอดภัยและความสะดวก • ตั้งค่าสมาร์ทการ์ด การ์ดแบบไร้สัมผัส หรือการ์ดระยะใกล้สำหรับการรับรองความถูกต้อง • ใช้โทรศัพท์ Bluetooth ของคุณเป็นวิธีการยืนยันตัวตน • ตั้ง PIN เพื่อขยายทางเลือกการรับรองความถูกต้องของคุณ • กำหนดค่านโยบายล็อกออนและเซสชัน • สำรองข้อมูลและกู้คืนข้อมูลโปรแกรมของคุณ • เพิ่มโปรแกรมต่างๆ มากขึ้นเช่น HP Drive Encryption, HP File Sanitizer, HP Trust Circles, HP Device Access Manager และ HP Computrace ผู้ใช้ทั่วไปสามารถดำเนินฟังก์ชันต่อไปนี้ได้: • ดูการตั้งค่าสำหรับสถานะการเข้ารหัสและ Device Access Manager • เปิดใช้งาน Computrace • กำหนดตัวเลือกค่าลักษณะส่วนบุคคลและสำรองข้อมูลและการคืนค่า

โมดูล	คุณสมบัติหลัก
Password Manager	ผู้ใช้ทั่วไปสามารถดำเนินฟังก์ชันต่อไปนี้ได้: • จัดตั้ง และตั้งค่าชื่อผู้ใช้และรหัสผ่าน • สร้างรหัสผ่านที่แข็งแกร่งเพื่อเสริมสร้างการรักษาความปลอดภัยของบัญชีสำหรับบัญชีอีเมลและเว็บ Password Manager จะกรอกและส่งข้อมูลโดยอัตโนมัติ • สร้างความคล่องตัวให้กับกระบวนการล็อกออนด้วยคุณสมบัติการลงชื่อเข้าใช้แค่ครั้งเดียว ซึ่งจะจดจำและใช้การตรวจสอบข้อมูลประจำตัวผู้ใช้โดยอัตโนมัติ • ทำการกาเครื่องหมายบัญชีว่าเป็นบัญชีอันตราย เพื่อที่คุณจะสามารถแจ้งบัญชีอื่นที่ใช้ข้อมูลประจำตัวที่คล้าย ๆ กันได้ • นำเข้าข้อมูลล็อกออนจากเบราว์เซอร์ที่ได้รับการสนับสนุน
HP Drive Encryption (มีเฉพาะบางรุ่นเท่านั้น)	• ให้บริการเข้ารหัสที่สมบูรณ์ และสำหรับฮาร์ดไดร์ฟทั้งไดร์ฟ • บังคับการรับรองความถูกต้องก่อนบูตเพื่อเลิกเข้ารหัสและเข้าถึงข้อมูล • เสนอตัวเลือกเพื่อเรียกใช้งานการเข้ารหัสไดรฟ์เอง (มีเฉพาะบางรุ่นเท่านั้น)
HP Device Access Manager	• ช่วยผู้จัดการฝ่ายไอทีในการควบคุมการเข้าใช้อุปกรณ์โดยขึ้นอยู่กับโปรไฟล์ผู้ใช้ • ช่วยป้องกันไม่ให้ผู้ใช้ที่ไม่ได้รับอนุญาตจากการถอนข้อมูลโดยใช้สื่อเก็บข้อมูลภายนอก และจากการแนะนำไวรัสลงในระบบจากสื่อภายนอก • อนุญาตให้ผู้ดูแลระบบปิดใช้งานการเข้าถึงอุปกรณ์สื่อสารสำหรับบุคคลหรือกลุ่มผู้ใช้เฉพาะ
HP Trust Circles	• ให้บริการรักษาความปลอดภัยแก่ไฟล์และเอกสาร • เข้ารหัสไฟล์ที่อยู่ในโฟลเดอร์ที่ผู้ใช้ระบุไว้ และปกป้องไฟล์ภายใน trust circle • อนุญาตให้ใช้และแบ่งปันไฟล์ระหว่างสมาชิกใน trust circle
การกู้คืนในกรณีที่ถูกโจรกรรม (Computrace ต้องซื้อแยกต่างหาก)	• จะขอให้ทำการสั่งซื้อการสมัครรับการติดตามและตามรอยแยกต่างหากเพื่อเปิดใช้งาน • ให้บริการติดตามสินทรัพย์ที่ปลอดภัย • ตรวจสอบกิจกรรมผู้ใช้ รวมถึงการเปลี่ยนแปลงด้านฮาร์ดแวร์และซอฟต์แวร์ • จะยังคงมีผลแม้เมื่อฮาร์ดไดร์ฟถูกจัดรูปแบบใหม่หรือถูกแทนที่

คำอธิบายสินค้า HP Client Security และตัวอย่างที่ใช้เป็นประจำ

สินค้า HP Client Security ส่วนใหญ่มีทั้งการรับรองความถูกต้องของผู้ใช้ (ปกติแล้วจะเป็นรหัสผ่าน) และการสำรองของผู้ดูแลระบบเพื่อการเข้าถึงหากรหัสผ่านสูญหาย ไม่มีให้ใช้งาน หรือถูกลืม หรือในเวลาใดก็ตามที่ฝ่ายรักษาความปลอดภัยขององค์กรต้องการเข้าถึง

หมายเหตุ: สินค้า HP Client Security บางชนิดได้รับการออกแบบมาเพื่อห้ามการเข้าถึงข้อมูล ควรมีการเข้ารหัสข้อมูลเมื่อผู้ใช้ยอมที่จะสูญเสียข้อมูลมากกว่าการให้ข้อมูลถูกลักขโมยไป ขอแนะนำว่าข้อมูลทั้งหมดได้รับการสำรองในตำแหน่งที่ปลอดภัยแล้ว

Password Manager

Password Manager จะเก็บชื่อผู้ใช้และรหัสผ่าน และสามารถใช้ในการ:

- บันทึกชื่อล็อกอินและรหัสผ่านสำหรับการเข้าสู่อินเทอร์เน็ตหรือส่งอีเมล
- ลงชื่อผู้ใช้เข้าสู่เว็บไซต์หรือส่งอีเมลโดยอัตโนมัติ

- จัดการและบริหารการรับรองความถูกต้อง
- เลือกสินทรัพย์ทางเว็บหรือเครือข่าย และเข้าถึงลิงค์โดยตรง
- ดูชื่อและรหัสผ่านเมื่อจำเป็น
- ทำการกาเครื่องหมายบัญชีว่าเป็นบัญชีอันตราย เพื่อที่คุณจะสามารถแจ้งบัญชีอื่นที่ใช้ข้อมูลประจำตัวที่คล้าย ๆ กันได้
- นำเข้าข้อมูลล็อกออนจากเบราวเซอร์ที่ได้รับการสนับสนุน

ตัวอย่างที่ 1 : ตัวแทนการซื้อสำหรับผู้ผลิตรายใหญ่ได้ทำการค้าขายของเธอผ่านอินเทอร์เน็ตซะส่วนใหญ่ เธอยังได้เยี่ยมชมเว็บไซต์ที่นิยมหลาย ๆ เว็บ ซึ่งต้องการข้อมูลการล็อกอิน เธอเป็นคนระมัดระวังเรื่องความปลอดภัยและจะไม่ใช้รหัสผ่านเดียวกันบนทุกบัญชี ตัวแทนฝ่ายสั่งซื้อได้ติดสินใจที่จะใช้ Password Manager ในการจับคู่เว็บลิงค์ต่าง ๆ กับชื่อผู้ใช้และรหัสผ่านต่าง ๆ เมื่อเธอเข้าสู่เว็บไซต์เพื่อล็อกออน Password Manager จะให้ข้อมูลส่วนตัวโดยอัตโนมัติ หากเธอต้องการดูชื่อผู้ใช้และรหัสผ่าน Password Manager ก็จะถูกกำหนดค่าให้แสดงผลให้ดูได้

Password Manager ยังสามารถถูกใช้สำหรับการจัดการและบริหารการรับรองความถูกต้องต่าง ๆ เครื่องมือนี้จะอนุญาตให้ผู้ใช้เลือกสินทรัพย์ทางเว็บหรือเครือข่าย และเข้าถึงลิงค์นั้นโดยตรง นอกจากนี้ผู้ใช้ยังสามารถดูชื่อผู้ใช้และรหัสผ่านเมื่อจำเป็น

ตัวอย่างที่ 2 : พนักงานที่ทำงานหนักรายหนึ่งได้รับการเลื่อนตำแหน่งและตอนนี้จะจัดการแผนกบัญชีทั้งแผนก ทีมงานจะต้องล็อกออนสู่บัญชีทางเว็บไคลเอ็นต์จำนวนมาก แต่ละทีมจะใช้ข้อมูลการล็อกอินที่แตกต่างกัน ข้อมูลล็อกอินนี้จะต้องถูกแบ่งปันกับพนักงานท่านอื่น เพราะฉะนั้นการรักษาความลับจึงเป็นปัญหาใหญ่ พนักงานคนนี้ตัดสินใจว่า จะจัดการเว็บลิงค์ต่าง ๆ ชื่อผู้ใช้บริษัท และรหัสผ่านใน Password Manager เมื่อเสร็จสิ้น พนักงานก็ได้เปิดใช้งาน Password Manager ให้กับพนักงานท่านอื่น ๆ เพื่อให้พวกเขาสามารถทำงานบนบัญชีเว็บและไม่มีทางรู้เกี่ยวกับข้อมูลการล็อกอินที่เป็นความลับที่พวกเขาใช้อยู่

HP Drive Encryption (มีเฉพาะบางรุ่นเท่านั้น)

HP Drive Encryption ถูกใช้ในการจำกัดการเข้าถึงข้อมูลบนฮาร์ดไดร์ฟคอมพิวเตอร์ทั้งไดร์ฟ หรือไดร์ฟรอง การเข้ารหัสไดรฟ์ยังสามารถจัดการไดรฟ์ที่เข้ารหัสเอง

ตัวอย่างที่ 1 : นายแพทย์ท่านหนึ่งต้องการยืนยันว่าเขาสามารถเข้าถึงข้อมูลใด ๆ ก็ได้บนฮาร์ดไดร์ฟของเขา เขาจึงได้เปิดใช้งาน Drive Encryption ซึ่งจำเป็นต้องบูตการรับรองความถูกต้องก่อนล็อกอินสู่ Windows เมื่อตั้งค่า คุณจึงไม่สามารถเข้าถึงฮาร์ดไดร์ฟได้โดยไม่มีรหัสผ่าน ก่อนระบบปฏิบัติการจะเริ่มทำงาน นายแพทย์ท่านนี้ยังได้เสริมการรักษาความปลอดภัยของไดร์ฟเพิ่มเติมโดยการเลือกเข้ารหัสข้อมูลด้วยตัวเลือกไดร์ฟแบบเข้ารหัสเอง

ตัวอย่างที่ 2 : ผู้ดูแลระบบโรงพยาบาลแห่งหนึ่งต้องการยืนยันว่ามีเฉพาะแพทย์และบุคลากรที่ได้รับการอนุญาตเท่านั้นที่จะสามารถเข้าถึงข้อมูลบนคอมพิวเตอร์ประจำท้องถิ่นของพวกเขาได้โดยไม่ต้องแบ่งปันรหัสผ่านส่วนตัว แผนกไอทีจึงได้เพิ่มผู้ดูแลระบบ นายแพทย์ และบุคลากรที่ได้รับอนุญาตทั้งหมดเป็นผู้ใช้ของ Drive Encryption ตอนนี้ มีเฉพาะบุคลากรที่ได้รับอนุญาตเท่านั้นที่สามารถบูตเครื่องคอมพิวเตอร์หรือโดเมนโดยใช้ชื่อผู้ใช้และรหัสผ่านของผู้ใช้ส่วนตัวของพวกเขา

HP Device Access Manager (มีเฉพาะบางรุ่นเท่านั้น)

HP Device Access Manager อนุญาตให้ผู้ดูแลระบบห้ามและจัดการการเข้าถึงฮาร์ดแวร์ คุณสามารถใช้ Device Access Manager ในการบล็อกการเข้าถึงแฟลชไดร์ฟ USB ที่ไม่ได้รับอนุญาต ซึ่งอาจสามารถคัดลอกข้อมูลได้ โปรแกรมนี้ยังห้ามการเข้าถึงไดร์ฟ CD/DVD ควบคุมอุปกรณ์ USB การเชื่อมต่อทางเครือข่าย และอื่น ๆ ตัวอย่างควรเป็นสถานการณ์ที่ผู้จัดจำหน่ายภายนอกต้องการเข้าถึงคอมพิวเตอร์ของบริษัทแต่ไม่ควรคัดลอกข้อมูลลงในไดร์ฟ USB

ตัวอย่างที่ 1 : ผู้จัดการของบริษัทวัตถุดิบด้านการแพทย์มักจะทำงานกับบันทึกทางการแพทย์ส่วนตัว พร้อมกับข้อมูลบริษัทของเขา พนักงานจำเป็นต้องใช้ข้อมูลนี้ อย่างไรก็ตาม จึงสำคัญอย่างยิ่งว่าข้อมูลจะไม่ถูกลบออกจากคอมพิวเตอร์โดยไดรฟ์ USB หรือสื่อหน่วยจัดเก็บภายนอกอื่น ๆ ใด เครือข่ายนั้นปลอดภัย แต่คอมพิวเตอร์มีไดร์ฟเขียน CD และพอร์ต USB ที่อาจจะอนุญาตให้ข้อมูลถูกคัดลอกหรือลักขโมยได้ ผู้ใช้การจึงใช้ Device Access Manager เพื่อปิดใช้งานพอร์ต USB และไดร์ฟเขียน CD เพื่อให้พวกเขาไม่ถูกใช้ แม้ว่าพอร์ต USB จะถูกบล็อก เมาส์และแป้นพิมพ์ก็จะทำงานต่อ

ตัวอย่างที่ 2 : บริษัทประกันไม่ต้องการให้พนักงานติดตั้งหรือโหลดซอฟต์แวร์หรือข้อมูลส่วนตัวจากที่บ้าน พนักงานบางคนต้องการเข้าถึงพอร์ต USB บนคอมพิวเตอร์ทุกเครื่อง ผู้จัดการฝ่ายไอดีใช้ Device Access Manager ในการจัดการการเข้าถึงสำหรับพนักงานบางคน ในขณะที่ได้บล็อกการเข้าถึงภายนอกจากผู้อื่นด้วย

Computrace (ซื้อแยกต่างหาก)

computrace (ซื้อแยกต่างหาก) เป็นบริการที่สามารถติดตามตำแหน่งของคอมพิวเตอร์ที่ถูกขโมยเมื่อใดก็ตามที่ผู้ใช้เชื่อมต่อกับอินเทอร์เน็ต Computrace ยังสามารถจัดการและจับตำแหน่งคอมพิวเตอร์จากระยะไกล โดยรวมถึงการใช้งานหน้าจอคอมพิวเตอร์

ตัวอย่างที่ 1 : อาจารย์ใหญ่ของโรงเรียนแห่งหนึ่งสั่งให้แผนกไอดีติดตามคอมพิวเตอร์ที่โรงเรียนของเขา หลังจากได้สร้างคลังข้อมูลคอมพิวเตอร์แล้ว แผนกไอทีก็ได้ลงทะเบียนคอมพิวเตอร์ทั้งหมดกับ Computrace เพื่อให้พวกเขาสามารถติดตามเครื่องได้ในกรณีที่ถูกขโมย และเมื่อไม่นานมานี้ ทางโรงเรียนก็พบว่ามีเครื่องคอมพิวเตอร์หายไปหลายเครื่อง เพราะฉะนั้นผู้ดูแลระบบไอดีจึงได้ทำการแจ้งเตือนกับหน่วยงานต่าง ๆ และเจ้าหน้าที่ของ Computrace จากนั้น เจ้าหน้าที่ก็สามารถจับตำแหน่งคอมพิวเตอร์ได้และได้คืนคอมพิวเตอร์ให้กับโรงเรียน

ตัวอย่างที่ 2 : บริษัทอสังหาริมทรัพย์แห่งหนึ่งต้องการจัดการและอัพเดทคอมพิวเตอร์ทุกเครื่องทั่วโลก พวกเขาใช้ Computrace ในการตรวจสอบและอัพเดทคอมพิวเตอร์ต่าง ๆ โดยไม่ต้องส่งพนักงานไอดีให้กับคอมพิวเตอร์แต่ละเครื่อง

การบรรลุเป้าหมายด้านการรักษาความปลอดภัยหลัก

โมดูล HP Client Security สามารถทำงานร่วมกันเพื่อให้โซลูชั่นสำหรับปัญหาด้านการรักษาความปลอดภัยหลายอย่าง โดยรวมถึงเป้าหมายด้านการรักษาความปลอดภัยหลักดังต่อไปนี้:

- การปกป้องจากการตกเป็นเป้าหมายของการโจรกรรม
- การจำกัดการเข้าถึงข้อมูลที่เป็นความลับ
- การป้องกันไม่ให้สามารถเข้าถึงได้จากตำแหน่งที่ตั้งภายในหรือภายนอกโดยไม่ได้รับอนุญาต
- การสร้างนโยบายรหัสผ่านที่แข็งแรง

การปกป้องจากการตกเป็นเป้าหมายของการโจรกรรม

ตัวอย่างของการโจรกรรมที่เป็นเป้าหมายก็จะเป็นการขโมยคอมพิวเตอร์ที่มีข้อมูลที่เป็นความลับ และข้อมูลลูกค้าที่จุดตรวจสอบความปลอดภัยของสนามบิน คุณสมบัติต่อไปนี้จะช่วยป้องกันมิให้เครื่องตกเป็นเป้าหมายของการโจรกรรม:

- คุณสมบัติการรับรองความถูกต้องก่อนบูต หากเปิดใช้งาน จะช่วยป้องกันการเข้าถึงระบบปฏิบัติการได้
  - HP Client Security–โปรดดู HP Client Security ในหน้า 11
  - HP Drive Encryption–โปรดดู HP Drive Encryption (มีเฉพาะบางรุ่นเท่านั้น) ในหน้า 26
- การเข้ารหัสช่วยยืนยันว่าข้อมูลจะเข้าถึงไม่ได้แม้เมื่อได้ลบฮาร์ดไดร์ฟออกและติดตั้งไว้ในระบบที่ไม่ปลอดภัยแล้ว
- Computrace สามารถติดตามตำแหน่งของคอมพิวเตอร์หลังจากที่ถูกขโมยไป
  - Computrace–โปรดดู การกู้คืนในกรณีที่ถูกโจรกรรม (เฉพาะบางรุ่นเท่านั้น) ในหน้า 47

การจำกัดการเข้าถึงข้อมูลที่เป็นความลับ

สมมุติว่าผู้ตรวจสอบสัญญากำลังทำงานนอกสถานที่ และได้ให้การเข้าถึงสู่คอมพิวเตอร์เพื่อทบทวนข้อมูลทางการเงินที่เป็นความลับ คุณไม่ต้องการให้ผู้ตรวจสอบสามารถพิมพ์ไฟล์หรือบันทึกไฟล์เหล่านี้ลงในอุปกรณ์ที่เขียนได้ เช่นซีดี คุณสมบัติต่อไปนี้จะช่วยจำกัดการเข้าใช้ข้อมูล:

- HP Device Access Manager จะอนุญาตให้ผู้จัดการฝ่ายไอทีทำการจำกัดการเข้าถึงอุปกรณ์สื่อสารเพื่อมิให้ข้อมูลที่เป็นความลับถูกคัดลอกจากฮาร์ดไดร์ฟ โปรดดู มุมมองระบบ ในหน้า 38

การป้องกันไม่ให้สามารถเข้าถึงได้จากตำแหน่งที่ตั้งภายในหรือภายนอกโดยไม่ได้รับอนุญาต

การเข้าถึงที่ไม่ได้รับอนุญาตสู่คอมพิวเตอร์ธุรกิจที่ไม่ปลอดภัยเป็นความเสี่ยงที่แท้จริงสำหรับแหล่งทรัพยากรเครือข่ายองค์กรเช่นข้อมูลจากบริการทางการเงิน ผู้บริหาร หรือทีมการวิจัยและพัฒนา และสำหรับข้อมูลส่วนตัวเช่นบันทึกของผู้ป่วยหรือบันทึกทางการเงินส่วนตัว คุณสมบัติดังต่อไปนี้จะช่วยป้องกันการเข้าถึงที่ไม่ได้รับอนุญาต:

- คุณสมบัติการรับรองความถูกต้องก่อนบูต หากเปิดใช้งาน จะช่วยป้องกันการเข้าถึงระบบปฏิบัติการได้ (โปรดดู HP Drive Encryption (มีเฉพาะบางรุ่นเท่านั้น) ในหน้า 26
- HP Client Security ช่วยยืนยันว่าผู้ใช้ที่ไม่ได้รับอนุญาตจะไม่สามารถได้รับรหัสผ่านและสามารถเข้าถึงโปรแกรมที่ปกป้องไว้ด้วยรหัสผ่าน โปรดดู HP Client Security ในหน้า 11
- HP Device Access Manager จะอนุญาตให้ผู้จัดการฝ่ายไอทีทำการจำกัดการเข้าถึงอุปกรณ์ที่เขียนได้เพื่อมิให้ข้อมูลที่เป็นความลับถูกคัดลอกจากฮาร์ดไดร์ฟ โปรดดู HP Device Access Manager (มีเฉพาะบางรุ่นเท่านั้น) ในหน้า 37

การสร้างนโยบายรหัสผ่านที่แข็งแรง

หากนโยบายบริษัทมีข้อบังคับที่กำหนดให้ใช้นโยบายรหัสผ่านที่แข็งแรงสำหรับโปรแกรมและฐานข้อมูลบนเว็บหลาย ๆ รายการ Password Manager ก็จะสามารถสร้างคลังข้อมูลที่ได้รับการปกป้องสำหรับรหัสผ่านและสร้างความสะดวกสบายในการ Single Sign On โปรดดู Password Manager ในหน้า 16

องค์ประกอบด้านการรักษาปลอดภัยเพิ่มเติม

การกำหนดบทบาทการรักษาความปลอดภัย

ในการจัดการด้านการรักษาความปลอดภัยของคอมพิวเตอร์ (โดยเฉพาะในองค์กรใหญ่ ๆ) การกระทำอย่างหนึ่งที่สำคัญมากก็คือการแบ่งแยกความรับผิดชอบและสิทธิในหมู่ผู้ดูแลระบบและผู้ใช้ที่แตกต่างกัน

หมายเหตุ: ในองค์กรเล็ก ๆ หรือสำหรับการใช้งานส่วนตัว หน้าที่เหล่านี้อาจจะเป็นของบุคคลเดียวกัน

สำหรับ HP Client Security หน้าที่การรักษาความปลอดภัยและสิทธิ์ที่ถูกแบ่งแยกไว้ตามหน้าที่ต่าง ๆ ดังต่อไปนี้:

- เจ้าหน้าที่รักษาความปลอดภัย–ระบุระดับการรักษาความปลอดภัยสำหรับบริษัทหรือเครือข่าย และระบุคุณสมบัติด้านความปลอดภัยในการใช้งาน เช่น Drive Encryption.

  หมายเหตุ: คุณสมบัติหลายอย่างใน HP Client Security จะสามารถถูกกำหนดค่าโดยเจ้าหน้าที่การรักษาความปลอดภัยที่ทำงานกับ HP สำหรับข้อมูลเพิ่มเติม โปรดไปที่ http://www.hp.com

- ผู้ดูแลระบบไอที–ใช้งานและจัดการโดยคุณสมบัติด้านความปลอดภัยที่ระบุโดยเจ้าหน้าด้านความปลอดภัย ยังสามารถเปิดใช้งานและปิดใช้งานคุณสมบัติบางอย่าง ตัวอย่างเช่น หากเจ้าหน้ารักษาความปลอดภัยได้ตัดสินใจว่าจะใช้สมาร์ทการ์ด ผู้ดูแลระบบไอทีสามารถเปิดใช้งานทั้งโหมดรหัสผ่านและสมาร์ทการ์ด
- ผู้ใช้–ใช้คุณสมบัติในการรักษาความปลอดภัย ตัวอย่างเช่น เจ้าหน้าที่รักษาความปลอดภัยและผู้ดูแลระบบไอดีได้เปิดใช้งานสมาร์ทการ์ดสำหรับระบบ ผู้ใช้สามารถตั้ง PIN สมาร์ทการ์ดและใช้การ์ดใบนั้นสำหรับการรับรองความถูกต้อง

ข้อควรระวัง: เราขอแนะนำให้ผู้ดูแลระบบปฏิบัติตาม "การปฏิบัติที่ดีที่สุด" ในการจำกัดสิทธิ์ผู้ใช้และการจำกัดการเข้าถึงของผู้ใช้

ผู้ใช้ที่ไม่ได้รับรองความถูกต้องไม่ควรได้รับสิทธิ์ผู้ดูแลระบบ

การจัดการรหัสผ่านของ HP Client Security

คุณสมบัติของ HP Client Security ส่วนใหญ่จะถูกรักษาความปลอดภัยไว้ด้วยรหัสผ่าน ตารางในรายการต่อไปนี้เป็นรหัสผ่านที่ใช้บ่อยมากที่สุด โมดูลซอฟต์แวร์ที่รหัสผ่านถูกตั้งไว้ และฟังก์ชันรหัสผ่าน

รหัสผ่านที่ถูกตั้งและใช้โดยผู้ดูแลระบบไอทีอย่างเดียวก็ถูกระบุไว้ในตารางนี้ด้วย รหัสผ่านอื่น ๆ ทั้งหมดจะถูกตั้งไว้โดยผู้ใช้หรือผู้ดูแลระบบอื่น ๆ

รหัสผ่าน HP Client Security	ตั้งไว้ในการโมดูลต่อไปนี้	ฟังก์ชั่น
รหัสผ่านสำหรับการลงชื่อเข้าสู่ Windows	แผงควบคุมของ Windows หรือ HP Client Security	สามารถใช้ในการล็อกออนด้วยตัวเองและสำหรับการรับรองความถูกต้องในการเข้าถึงคุณสมบัติของ HP Client Security หลาย ๆ รายการ
การสำรองและการกู้คืนรหัสผ่านของ HP Client Security	HP Client Security โดยผู้ใช้แต่ละราย	ป้องกันการเข้าถึงไฟล์ที่สำรองและการกู้คืน HP Client Security
PIN สมาร์ทการ์ด	Credential Manager	สามารถนำมาใช้สำหรับการรับรองความถูกต้องในหลาย ๆ ปัจจัย สามารถนำมาใช้สำหรับการรับรองความถูกต้องของ Windows ผู้ใช้ที่ผ่านการรับรองความถูกต้องของ Drive Encryption หากเลือกสมาร์ทการ์ด

การสร้างรหัสผ่านรักษาความปลอดภัย

เมื่อสร้างรหัสผ่าน คุณจะต้องติดตามข้อกำหนดเฉพาะใด ๆ ที่ตั้งไว้โดยโปรแกรม โดยทั่วไปแล้ว อย่างไรก็ตาม ลองคำนึงถึงคู่มือเหล่านี้ในการช่วยให้คุณสร้างรหัสผ่านที่แข็งแรงและลดโอกาสที่รหัสผ่านของคุณจะตกอยู่ในอันตราย:

- ใช้รหัสผ่านด้วยตัวอักษรมากกว่า 6 ตัว และควรจะมีความยาวมากกว่า 8
- ผสมตัวอักษรพิมพ์ใหญ่เล็กไว้ด้วยกันในรหัสผ่านของคุณ
- เมื่อเป็นไปได้ ผสมตัวอักษรไว้ด้วยกันและรวมเครื่องหมายพิเศษและเครื่องหมายวรรคตอนไว้ด้วย
- ทดแทนตัวอักษรพิเศษหรือตัวเลขสำหรับตัวอักษรในคำสำคัญ ตัวอย่างเช่น คุณสามารถใช้หมายเลข 1 แทนตัวอักษร L
- ผสมถ้อยคำจากภาษา 2 ภาษาหรือมากกว่า
- แยกคำหรือถ้อยคำพร้อมหมายเลขหรือตัวอักษรพิเศษตรงกลาง ตัวอย่างเช่น “Mary2-2Cat45.”
- อย่าใช้รหัสผ่านที่จะปรากฏในพจนานุกรม
- อย่าใช้ชื่อของคุณเป็นรหัสผ่าน หรือข้อมูลส่วนตัวอื่น ๆ เช่นวันเกิด ชื่อสัตว์เลี้ยง หรือนามสกุลเดิมของมารดา แม้ว่าคุณจะสะกดกลับหลังก็ตาม
- เปลี่ยนรหัสผ่านเป็นประจำ คุณสามารถเปลี่ยนเฉพาะตัวอักษรเพียงไม่กี่ตัว
- หากคุณเขียนรหัสผ่านลง อย่าเก็บไว้ในสถานที่ที่มองเห็นได้ชัดเจนใกล้ ๆ กับคอมพิวเตอร์
- อย่าบันทึกรหัสผ่านในไฟล์ เช่นอีเมล บนคอมพิวเตอร์
- อย่าแบ่งปันบัญชีหรือบอกรหัสผ่านของคุณให้ใคร

การสำรองข้อมูลส่วนตัวและการตั้งค่า

คุณสามารถใช้เครื่องมือสำรองและกู้คืนใน HP Client Security เป็นตำแหน่งศูนย์กลางที่คุณสามารถสำรองและกู้คืนข้อมูลส่วนตัวสำหรับการรักษาความปลอดภัยจากโมดูล HP Client Security บางรายการที่ติดตั้งไว้

2 การเริ่มต้นใช้งาน

ในการกำหนดค่า HP Client Security สำหรับการใช้กับข้อมูลประจำตัว ให้เปิดใช้งาน HP Client Security ด้วยวิธีการต่อไปนี้ เมื่อผู้ใช้ดำเนินการตามตัวช่วยสร้างเสร็จสมบูรณ์แล้ว ผู้ใช้ดังกล่าวจะไม่สามารถเปิดใช้งานโปรแกรมนี้ได้อีก

1. จากหน้าจอเริ่มต้นหรือหน้าจอแอพ ให้คลิกหรือแตะแอพ **HP Client Security** (Windows 8)

   - หรือ -

   จากเดสก์ท็อป Windows ให้คลิกหรือแตะ **แกดเจ็ต HP Client Security** (Windows 7)

   - หรือ -

   จากเดสก์ท็อป Wondows ให้ดับเบิลคลิกหรือแตะสองครั้งที่ไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ประมาณขวาสุดของแถบงาน

   - หรือ -

   จากเดสก์ท็อป Wondows ให้คลิกหรือแตะไอคอน **HP Client Security** ในพื้นที่แจ้งเตือน จากนั้นเลือก **เปิด HP Client Security**

2. ตัวช่วยการติดตั้ง HP Client Security จะเปิดใช้งานพร้อมกับแสดงหน้ายินดีต้อนรับขึ้นมา

3. ให้อ่านหน้าจอยินดีต้อนรับ และตรวจสอบข้อมูลระบุตัวตนของคุณโดยพิมพ์รหัสผ่าน Windows จากนั้นคลิกหรือแตะ **ถัดไป**

   หากคุณยังไม่ได้สร้างรหัสผ่าน Windows คุณจะได้รับการแจ้งให้สร้างรหัสผ่าน รหัสผ่าน Windows เป็นสิ่งที่จำเป็นในการปกป้องบัญชี Windows ของคุณไม่ให้บุคคลที่ไม่ได้รับอนุญาตสามารถเข้าถึงได้ และเพื่อใช้คุณสมบัติต่างๆ ของ HP Client Security

4. ในหน้า HP SpareKey ให้เลือกคำถามรักษาความปลอดภัยสามข้อ ป้อนคำตอบสำหรับแต่ละคำถาม จากนั้นคลิก **ถัดไป** นอกจากนี้ยังสามารถกำหนดคำถามเองได้อีกด้วย สำหรับข้อมูลเพิ่มเติม โปรดดู HP SpareKey—การกู้คืนข้อมูลรหัสผ่าน ในหน้า 12

5. ในหน้าลายนิ้วมือ ให้ลงทะเบียนจำนวนลายนิ้วมือขั้นต่ำที่กำหนดไว้เป็นอย่างน้อย จากนั้นคลิกหรือแตะ **ถัดไป** สำหรับข้อมูลเพิ่มเติม โปรดดู รอยนิ้วมือ ในหน้า 11

6. ในหน้า Drive Encryption ให้เปิดใช้งานการเข้ารหัส และสำรองข้อมูลคีย์เข้ารหัส จากนั้นคลิกหรือแตะ **ถัดไป** สำหรับข้อมูลเพิ่มเติม โปรดดูวิธีใช้ซอฟต์แวร์ HP Drive Encryption

   หมายเหตุ: การดำเนินการนี้จะใช้กับสถานการณ์ที่ผู้ใช้เป็นผู้ดูแลระบบ และผู้ดูแลระบบยังไม่ได้กำหนดค่าตัวช่วยการติดตั้ง HP Client Security ก่อนหน้านี้

7. ในหน้าสุดท้ายของตัวช่วยสร้าง ให้คลิกหรือแตะ **เสร็จสิ้น**

   หน้านี้จะให้ข้อมูลสถานะของคุณสมบัติและข้อมูลประจำตัวต่างๆ

8. ตัวช่วยการติดตั้ง HP Client Security ทำให้แน่ใจถึงการเปิดใช้งานของ Just In Time Authentication และ File Sanitizer สำหรับข้อมูลเพิ่มเติม โปรดดูวิธีใช้ซอฟต์แวร์ HP Device Access Manager และ HP File Sanitizer

   หมายเหตุ: การดำเนินการนี้จะใช้กับสถานการณ์ที่ผู้ใช้เป็นผู้ดูแลระบบ และผู้ดูแลระบบยังไม่ได้กำหนดค่าตัวช่วยการติดตั้ง HP Client Security ก่อนหน้านี้

การเปิด HP Client Security

คุณสามารถเปิดโปรแกรม HP Client Security ด้วยวิธีการต่อไปนี้:

หมายเหตุ: ตัวช่วยการติดตั้ง HP Client Security ต้องดำเนินการเสร็จสมบูรณ์ก่อนที่จะสามารถเปิดใช้งานโปรแกรม HP Client Security

- จากหน้าจอเริ่มต้นหรือหน้าจอแอพ ให้คลิกหรือแตะแอพ **HP Client Security**

  - หรือ -

  จากหน้าจอ Windows ให้คลิกหรือแตะแกดเจ็ต **HP Client Security** (Windows 7)

  - หรือ -

  จากเดสก์ท็อป Wondows ให้ดับเบิลคลิกหรือแตะสองครั้งที่ไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ประมาณขวาสุดของแถบงาน

  - หรือ -

  จากเดสก์ท็อป Wondows ให้คลิกหรือแตะไอคอน **HP Client Security** ในพื้นที่แจ้งเตือน จากนั้นเลือก **เปิด HP Client Security**

3 คู่มือการติดตั้งสำหรับธุรกิจขนาดเล็กอย่างง่าย ๆ

บทนี้ถูกออกแบบมาเพื่อแสดงขั้นตอนพื้นฐานในการเปิดใช้งานตัวเลือกที่ใช้งานบ่อยและมีประโยชน์มากที่สุดใน HP Client Security สำหรับธุรกิจขนาดเล็ก เครื่องมือและตัวเลือกมากมายในซอฟต์แวร์นี้จะอนุญาตให้คุณปรับแต่งการกำหนดลักษณะของคุณและตั้งการควบคุมการเข้าถึงของคุณ จุดศูนย์กลางของคู่มือการตั้งค่าอย่างง่าย ๆ ก็คือการนำโมดูลแต่ละรายการมาใช้งานด้วยการพยายามตั้งค่าและเวลาที่น้อยที่สุด สำหรับข้อมูลเพิ่มเติม เลือกโมดูลที่คุณสนจ และจึงคลิก **?** หรือปุ่มช่วยเหลือที่มุมขวาบน ปุ่มนี้จะแสดงข้อมูลเพื่อช่วยคุณกับหน้าต่างที่แสดงผลในปัจจุบันโดยอัตโนมัติ

การเริ่มต้นใช้งาน

1. จากเดสก์ท็อป Windows ให้เปิด HP Client Security โดยการดับเบิลคลิกไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ขวาสุดของแถบงาน
2. ป้อนรหัสผ่านของ Windows ของคุณ หรือสร้างรหัสผ่าน Windows
3. ทำการตั้งค่า HP Client Security ให้เสร็จสิ้น

ในการรับรองความถูกต้องของ HP Client Security ที่จำเป็นเพียงครั้งเดียวในระหว่างการล็อกอินสู่ Windows โปรดดู คุณสมบัติด้านความปลอดภัย ในหน้า 23

Password Manager

ทุกคนมีรหัสผ่านหลาย ๆ ชุด - โดยเฉพาะเมื่อคุณเข้าถึงเว็บไซต์หรือใช้โปรแกรมที่คุณต้องใช้ในการล็อกออน ผู้ใช้ปกติจะใช้รหัสผ่านเดียวกันสำหรับทุก ๆ โปรแกรมและเว็บไซต์ หรือทำอะไรที่สร้างสรรค์เล็กน้อยและลืมว่ารหัสผ่านใดควรใช้งานกับโปรแกรมใด

Password Manager สามารถจำรหัสผ่านของคุณไว้หรือให้ความสามารถในการมองเห็นว่าควรจำและข้ามไซต์ใด ๆ เมื่อคุณลงชื่อบนคอมพิวเตอร์เครื่องนี้ Password Manager ก็จะให้รหัสผ่านหรือข้อมูลส่วนตัวสำหรับโปรแกรมหรือเว็บไซต์ที่เข้าร่วม

เมื่อคุณเข้าถึงโปรแกรมหรือเว็บไซต์ใด ๆ ที่ต้องมีข้อมูลส่วนตัว Password Manager จะจำเว็บไซต์ได้ทันที และจะถามว่าคุณต้องการให้ซอฟต์แวร์จำข้อมูลของคุณไว้หรือไม่ หากคุณไม่ต้องการเก็บบางไซต์ไว้ คุณสามารถปฏิเสธคำขอได้

ในการเริ่มเก็บตำแหน่งเว็บ ชื่อผู้ใช้ และรหัสผ่าน:

1. ตัวอย่างเช่น ให้นำทางไปที่เว็บไซต์หรือแอพพลิเคชันที่เข้าร่วม แล้วคลิกที่ไอคอน Password Manager ที่มุมซ้ายบนของหน้าเว็บเพื่อเพิ่มเว็บการตรวจสอบความถูกต้องทางเว็บ
2. ตั้งชื่อลิงค์ (เลือกได้) และป้อนชื่อผู้ใช้และรหัสผ่านใน Password Manager
3. เมื่อเสร็จสมบูรณ์แล้ว ให้คลิกปุ่ม **OK**
4. Password Manager ยังสามารถบันทึกชื่อผู้ใช้และรหัสผ่านสำหรับการแบ่งปันในเครือข่ายหรือไดร์ฟเครือข่ายที่แมปไว้ด้วย

การดูและจัดการข้อมูลรับรองความถูกต้องที่บันทึกไว้ใน Password Manager

Password Manager อนุญาตให้คุณดู จัดการ สำรองและเปิดใช้การรับรองความถูกต้องของคุณจากตำแหน่งศูนย์กลาง Password Manager ยังทำการสนับสนุนการเปิดบริการไซต์ที่บันทึกไว้จาก Windows

ในการเปิด Password Manager ใช้ปุ่มบนแป้นพิมพ์ต่อไปนี้ Ctrl+แป้น Windows+h เพื่อเปิด Password Manager จากนั้นคลิก **Log in** (ล็อกอิน) เพื่อเปิดและรับรองความถูกต้องของทางลัดที่บันทึกไว้

ตัวเลือกการ **Edit** (แก้ไข) ของ Password Manager ได้อนุญาตให้คุณดูและแก้ไขชื่อ ชื่อสำหรับการเข้าสู่ระบบ และแม้แต่การเปิดเผยรหัสผ่าน

HP Client Security สำหรับธุรกิจขนาดเล็กจะอนุญาตให้สำรองและ/หรือคัดลอกข้อมูลส่วนตัวและการตั้งค่าไว้ที่คอมพิวเตอร์เครื่องอื่น

HP Device Access Manager

Device Access Manager สามารถใช้สำหรับการจำกัดการใช้อุปกรณ์จัดเก็บภายในและภายนอกต่าง ๆ เพื่อให้ข้อมูลของคุณปลอดภัยบนฮาร์ดไดร์ฟและไม่เดินออกจากธุรกิจของคุณ ตัวอย่างหนึ่งก็คือการอนุญาตให้ผู้ใช้เข้าถึงข้อมูลของคุณแต่บล็อกพวกเขาออกจากการคัดลอกลงซีดี เครื่องเล่นเพลงส่วนตัว หรืออุปกรณ์หน่วยความจำ USB

1. การเปิด **Device Access Manager** (โปรดดู การเปิด Device Access Manager ในหน้า 37)

   การเข้าถึงสำหรับผู้ใช้ปัจจุบันจะปรากฏขึ้น

2. ในการเปลี่ยนสิทธิ์ในการเข้าใช้ของผู้ใช้ กลุ่มผู้ใช้หรืออุปกรณ์ ให้คลิกหรือแตะ **Change** (เปลี่ยน) สำหรับข้อมูลเพิ่มเติม โปรดดู มุมมองระบบ ในหน้า 38

HP Drive Encryption

HP Drive Encryption มีไว้สำหรับการปกป้องข้อมูลของคุณโดยการเข้ารหัสฮาร์ดไดร์ฟทั้งแผ่น ข้อมูลในฮาร์ดไดร์ฟของคุณจะได้รับการปกป้องหากคอมพิวเตอร์ของคุณถูกลักขโมยและ/หรือหากฮาร์ดไดร์ฟถูกถอดออกจากคอมพิวเตอร์เดิมและวางไว้ในคอมพิวเตอร์อื่น

ประโยชน์ด้านการรักษาความปลอดภัยเพิ่มเติมก็คือการที่ Drive Encryption กำหนดให้คุณรับรองความถูกต้องอย่างเหมาะสมโดยใช้ชื่อผู้ใช้และรหัสผ่านก่อนระบบปฏิบัติการจะเริ่มทำงาน กระบวนการนี้ถูกเรียกว่า การรับรองความถูกต้องก่อนบูต

ในการทำให้อะไรต่ออะไรง่ายดายขึ้น โมดูลซอฟต์แวร์หลาย ๆ โมดูลจะซิงค์รหัสผ่านโดยอัตโนมัติ โดยรวมถึงรหัสผ่านผู้ใช้ Windows การรับรองความถูกต้องของโดเมน HP Drive Encryption, Password Manager และ HP Client Security.

ในการตั้งค่า HP Drive Encryption ในช่วงการตั้งค่าเริ่มต้นกับตัวช่วยการตั้งค่า HP Client Security โปรดดู การเริ่มต้นใช้งาน ในหน้า 7

4 HP Client Security

หน้าหลักของ HP Client Security เป็นที่ตั้งกลางสำหรับการเข้าถึงคุณสมบัติ โปรแกรม และการตั้งค่าของ HP Client Security อย่างง่าย หน้าหลักนี้จะแบ่งออกเป็นสามส่วน:

- **ข้อมูล**–ให้การเข้าถึงโปรแกรมที่ใช้สำหรับการจัดการความปลอดภัยของข้อมูล
- **อุปกรณ์**–ให้การเข้าถึงโปรแกรมที่ใช้สำหรับการจัดการความปลอดภัยของข้อมูล
- **ข้อมูลระบุตัวตน**–ให้การลงทะเบียนและการจัดการการรับรองความถูกต้องของข้อมูลประจำตัว

เลื่อนเคอร์เซอร์ไปบนไทล์โปรแกรมเพื่อแสดงรายละเอียดของโปรแกรม

HP Client Security อาจให้ลิงก์เชื่อมโยงไปยังผู้ใช้และการตั้งค่าผู้ดูแลระบบที่ด้านล่างของหน้า HP Client Security ให้การเข้าถึงการตั้งค่าขั้นสูงและคุณสมบัติโดยแตะหรือคลิกไอคอน **รูปเกียร์** (การตั้ง)

คุณสมบัติ โปรแกรม และการตั้งค่าข้อมูลระบุตัวตน

คุณสมบัติ โปรแกรม และการตั้งค่าข้อมูลระบุตัวตนที่ได้จาก HP Client Security จะช่วยคุณในการจัดการเรื่องรหัสประจำตัวแบบดิจิตอลหลายอย่าง ให้คลิกหรือแตะไทล์ต่อไปนี้ในหน้าหลักของ HP Client Security จากนั้นป้อนรหัสผ่าน Windows ของคุณ

- **ลายนิ้วมือ**–ลงทะเบียนและจัดการข้อมูลประจำตัวของลายนิ้วมือ
- **SpareKey**–ตั้งค่าและจัดการข้อมูลประจำตัวของ HP SpareKey ที่สามารถใช้ในการล็อกออนคอมพิวเตอร์ของคุณหากข้อมูลประจำตัวสูญหายหรือลืม รวมทั้งยังอนุญาตให้คุณรีเซ็ตรหัสผ่านที่ลืมได้อีกด้วย
- **รหัสผ่าน Windows**–ให้การเข้าถึงอย่างง่ายเพื่อเปลี่ยนรหัสผ่าน Windows ของคุณ
- **อุปกรณ์ Bluetooth**–ช่วยให้คุณลงทะเบียนและจัดการอุปกรณ์ Bluetooth ของคุณ
- **การ์ด**–ช่วยให้คุณลงทะเบียนและจัดการสมาร์ทการ์ด การ์ดแบบไร้สัมผัส และการ์ดระยะใกล้
- **PIN**–ช่วยให้คุณลงทะเบียนและจัดการข้อมูลประจำตัว PIN ของคุณ
- **RSA SecurID**–ช่วยให้คุณลงทะเบียนและจัดการข้อมูลประจำตัว RSA SecurID (หากมีการตั้งค่าที่เหมาะสมพร้อมใช้งาน)
- **Password Manager**–ช่วยให้คุณจัดการรหัสผ่านสำหรับบัญชีและโปรแกรมออนไลน์ของคุณ

รอยนิ้วมือ

ตัวช่วยการติดตั้ง HP Client Security จะนำคุณผ่านกระบวนการตั้งค่า หรือ "การลงทะเบียน" ลายนิ้วมือของคุณ

คุณยังสามารถลงทะเบียนหรือลบลายนิ้วมือของคุณในหน้า ลายนิ้วมือ ซึ่งคุณสามารถเข้าถึงโดยคลิกหรือแตะไอคอน **ลายนิ้วมือ** ในหน้าหลักของ HP Client Security

1. ในหน้า ลายนิ้วมือ ให้ปัดนิ้วจนกว่าจะลงทะเบียนสำเร็จ

   จำนวนนิ้วมือที่กำหนดที่จะต้องลงทะเบียนจะถูกระบบไว้ในหน้าดังกล่าว ขอแนะนำให้ใช้นิ้วชี้หรือนิ้วกลาง
2. ในการลบลายนิ้วมือที่ละทะเบียนไว้ก่อนหน้านี้ ให้คลิกหรือแตะ **ลบ**
3. ในการลงทะเบียนนิ้วมือเพิ่มเติม ให้คลิกหรือแตะ **ลงทะเบียนลายนิ้วมือเพิ่มเติม**
4. คลิกหรือแตะ **บันทึก** ก่อนที่จะออกไปจากหน้าดังกล่าว

⚠ **ข้อควรระวัง:** เมื่อลงทะเบียนลายนิ้วมือด้วยตัวช่วย ข้อมูลลายนิ้วมือจะไม่ถูกบันทึกจนกว่าคุณจะคลิก **ถัดไป** หากคุณทิ้งคอมพิวเตอร์โดยไม่มีการใช้งานเป็นเวลาสักครู่ หรือปิดโปรแกรม การเปลี่ยนแปลงที่คุณทำจะ **ไม่** ถูกบันทึก

- ในการเข้าถึงการตั้งค่าลายนิ้วมือของผู้ดูแลระบบ ซึ่งเป็นที่ที่ผู้ดูแลระบบสามารถระบุการลงทะเบียน ความแม่นยำ และการตั้งค่าอื่นๆ ให้คลิกหรือแตะ **การตั้งค่าของผู้ดูแลระบบ** (ต้องมีสิทธิ์ของผู้ดูแลระบบ)
- ในการเข้าถึงการตั้งค่าลายนิ้วมือของผู้ใช้ ซึ่งเป็นที่ที่คุณสามารถระบุการตั้งค่าที่ควบคุมลักษณะปรากฏและพฤติกรรมของการจดจำลายนิ้วมือ ให้คลิกหรือแตะ **การตั้งค่าของผู้ใช้**

การตั้งค่าลายนิ้วมือของผู้ดูแลระบบ

ผู้ดูแลระบบสามารถระบุการลงทะเบียน ความแม่นยำ และการตั้งค่าอื่น ๆ สำหรับตัวอ่านลายนิ้วมือ ต้องมีสิทธิ์ของผู้ดูแลระบบ

- ในการเข้าถึงการตั้งค่าของผู้ดูแลระบบสำหรับข้อมูลประจำตัวของลายนิ้วมือ ให้คลิกหรือแตะ **การตั้งค่าของผู้ดูแลระบบ** ในหน้าลายนิ้วมือ

- **การลงทะเบียนผู้ใช้**–เลือกจำนวนลายนิ้วมือต่ำสุดและสูงสุดที่ผู้ใช้ได้รับอนุญาตให้สามารถลงทะเบียนได้
- **การจดจำ**–เลื่อนตัวเลื่อนเพื่อปรับความไวที่ตัวอ่านลายนิ้วมือใช้เมื่อคุณปัดนิ้วมือของคุณ

  หากลายนิ้วมือของคุณไม่มีการจดจำอย่างต่อเนื่องสม่ำเสมอ คุณอาจจำเป็นต้องเลือกการตั้งค่าการจดจำที่ต่ำลง การตั้งค่าที่สูงขึ้นจะเป็นการเพิ่มความไวต่อความแปรปรวนในการปัดลายนิ้วมือ ดังนั้นจึงทำให้ลดความเป็นไปได้ของการตอบรับที่ผิดได้ การตั้งค่า **กลาง-สูง** ให้การผสมผสานที่ดีของความปลอดภัยและความสะดวก

การตั้งค่าลายนิ้วมือของผู้ใช้

ในหน้าการตั้งค่าลายนิ้วมือของผู้ใช้ คุณสามารถระบุการตั้งค่าที่ควบคุมลักษณะปรากฏและพฤติกรรมของการจดจำลายนิ้วมือ

- ในการเข้าถึงการตั้งค่าของผู้ใช้สำหรับข้อมูลประจำตัวของลายนิ้วมือ ให้คลิกหรือแตะ **การตั้งค่าผู้ใช้** ในหน้าลายนิ้วมือ

- **เปิดใช้งานเสียงตอบกลับ**–โดยค่าเริ่มต้น HP Client Security จะส่งเสียงตอบกลับเมื่อมีการปัดนิ้วมือ โดยจะมีเสียงที่แตกต่างกันสำหรับเหตุการณ์ที่เจาะจงในโปรแกรม คุณสามารถกำหนดเสียงใหม่ให้กับเหตุการณ์เหล่านี้ผ่านแท็บเสียงในการตั้งค่าเสียงในแผงควบคุม Windows หรือในการยกเลิกการใช้งานเสียงตอบกลับ ให้ล้างกล่องกาเครื่องหมาย
- **แสดงการตอบกลับคุณภาพการสแกน**–ในการแสดงการปัดนิ้วมือทั้งหมดโดยไม่คำนึงถึงคุณภาพการปัด ให้เลือกกล่องกาเครื่องหมายดังกล่าว ในการแสดงเฉพาะครั้งที่มีปัดนิ้วอย่างคุณภาพ ให้ล้างกล่องกาเครื่องหมาย

HP SpareKey–การกู้คืนข้อมูลรหัสผ่าน

HP SpareKey ช่วยให้คุณเข้าถึงคอมพิวเตอร์ของคุณ (ในแพลทฟอร์มที่สนับสนุน) โดยตอบคำถามรักษาความปลอดภัยสามข้อ

HP Client Security จะแจ้งให้คุณตั้งค่า HP SpareKey ส่วนบุคคลในระหว่างการตั้งค่าเริ่มต้นในตัวช่วยการติดตั้ง HP Client Security

ในการตั้งค่า HP SpareKey:

1. ในหน้า HP SpareKey ของตัวช่วยสร้าง ให้เลือกคำถามรักษาความปลอดภัยสามข้อ จากนั้นป้อนคำตอบสำหรับแต่ละคำถาม

   คุณสามารถเลือกคำถามจะรายการที่กำหนดไว้ล่วงหน้าหรือเขียนคำถามของคุณเองก็ได้

2. คลิกหรือแตะ **ลงทะเบียน**

ในการลบ HP SpareKey:

- ให้คลิกหรือแตะ **ลบ SpareKey**

หลังจากได้ตั้งค่า SpareKey คุณสามารถเข้าใช้งานคอมพิวเตอร์ของคุณโดยใช้ SpareKey จากหน้าจอล็อกออนด้วยการรับรองความถูกต้องเมื่อเปิดเครื่องหรือหน้าจอยินดีต้อนรับ Windows

คุณสามารถเลือกคำถามต่างออกไปหรือเปลี่ยนคำตอบของคุณในหน้า SpareKey ซึ่งเข้าถึงจากไทล์การกู้คืนรหัสผ่านในหน้าหลักของ HP Client Security

ในการเข้าถึงการตั้งค่า HP SpareKey ซึ่งเป็นที่ที่ผู้ดูแลระบบสามารถระบุการตั้งค่าที่เกี่ยวข้องกับข้อมูลประจำตัวของ HP SpareKey ให้คลิก **การตั้งค่า** (ต้องมีสิทธิ์ของผู้ดูแลระบบ)

HP SpareKey Settings

ในหน้าการตั้งค่า HP SpareKey Settings คุณสามารถระบุการตั้งค่าที่ควบคุมพฤติกรรมและการใช้ข้อมูลประจำตัวของ HP SpareKey ได้

- ในการเปิดใช้งานหน้าการตั้งค่า HP SpareKey ให้คลิกหรือแตะ **การตั้งค่า** ในหน้า HP SpareKey (ต้องมีสิทธิ์ของผู้ดูแลระบบ)

ผู้ดูแลระบบสามารถเลือกการตั้งค่าต่อไปนี้:

- ระบุคำถามที่เสนอให้กับผู้ใช้แต่ละรายในช่วงการติดตั้ง HP SpareKey
- เพิ่มคำถามรักษาความปลอดภัยได้ถึงสามข้อเข้าในรายการที่เสนอให้กับผู้ใช้
- เลือกว่าจะอนุญาตให้ผู้ใช้เขียนคำถามรักษาความปลอดภัยของตนเองหรือไม่
- ระบุว่าจะอนุญาตให้สภาพแวดล้อมการรับรองความถูกต้องใด (Windows หรือ การรับรองความถูกต้องเมื่อเปิดเครื่อง) สามารถใช้ HP SpareKey สำหรับการกู้คืนรหัสผ่าน

รหัสผ่าน Windows

HP Client Security ทำให้การเปลี่ยนรหัสผ่าน Windows เรียบง่ายและรวดเร็วขึ้นกว่าการเปลี่ยนผ่านแผงควบคุม Windows

ในการเปลี่ยนรหัสผ่าน Windows:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะ **รหัสผ่าน Windows**
2. ป้อนรหัสผ่านปัจจุบันของคุณในกล่องข้อความ **รหัสผ่านปัจจุบัน Windows**
3. พิมพ์รหัสผ่านใหม่ในกล่องข้อความ **รหัสผ่านใหม่ Windows** จากนั้นพิมพ์อีกครั้งในกล่องข้อความ **ยืนยันรหัสผ่านใหม่**
4. คลิกหรือแตะ **เปลี่ยน** เพื่อเปลี่ยนรหัสผ่านปัจจุบันเป็นรหัสผ่านใหม่ที่คุณได้ป้อนทันที

อุปกรณ์ Bluetooth

หากผู้ดูแลระบบเปิดใช้งาน Bluetooth เป็นการรับรองความถูกต้องของข้อมูลประจำตัว คุณสามารถตั้งค่าโทรศัพท์ Bluetooth ร่วมกับข้อมูลประจำตัวอื่นๆ เพื่อเพิ่มความปลอดภัย

หมายเหตุ: สนับสนุนเฉพาะอุปกรณ์โทรศัพท์ Bluetooth เท่านั้น

1. ตรวจสอบว่าได้เปิดใช้งานฟังก์ชั่น Bluetooth บนคอมพิวเตอร์ และได้ตั้งค่าโทรศัพท์ Bluetooth เป็นโหมดการค้นพบ ในการเชื่อมต่อโทรศัพท์ คุณอาจจะต้องพิมพ์รหัสที่สร้างโดยอัตโนมัติบนอุปกรณ์ Bluetooth อาจจำเป็นต้องเปรียบเทียบรหัสการจับคู่ระหว่างคอมพิวเตอร์กับโทรศัพท์ ทั้งนี้ขึ้นอยู่กับการตั้งการกำหนดค่าอุปกรณ์ Bluetooth
2. ในการลงทะเบียนโทรศัพท์ ให้เลือกโทรศัพท์ จากนี้คลิกหรือแตะ **ลงทะเบียน**

ในการเข้าถึง การตั้งค่าอุปกรณ์ Bluetooth ในหน้า 13 หน้าที่ผู้ดูแลระบบสามารถระบบการตั้งค่าสำหรับอุปกรณ์ Bluetooth ให้คลิก **การตั้งค่า** (ต้องมีสิทธิ์ของผู้ดูแลระบบ)

การตั้งค่าอุปกรณ์ Bluetooth

ผู้ดูแลระบบสามารถระบุการตั้งค่าต่อไปนี้ที่ควบคุมพฤติกรรมและการใช้ข้อมูลประจำตัวของอุปกรณ์ Bluetooth:

การรับรองความถูกต้องแบบไม่มีเสียง

- **ใช้อุปกรณ์ Bluetooth ของคุณที่ลงทะเบียนและเชื่อมต่อในช่วงการตรวจสอบข้อมูลระบบตัวตนของคุณ**—เลือกกล่องกาเครื่องหมายเพื่ออนุญาตให้ผู้ใช้สามารถใช้ข้อมูลประจำตัวของ Bluetooth สำหรับการรับรองความถูกต้องโดยผู้ใช้ไม่ต้องดำเนินการอะไร หรือล้างกล่องกาเครื่องหมายเพื่อยกเลิกการใช้งานตัวเลือกนี้

ระยะสำหรับ Bluetooth

- **ล็อคคอมพิวเตอร์ของคุณเมื่ออุปกรณ์ Bluetooth ที่ลงทะเบียนไว้เลื่อนออกไปอยู่นอกช่วงที่คอมพิวเตอร์ของคุณเข้าถึงได้**—เลือกกล่องกาเครื่องหมายเพื่อล็อกคอมพิวเตอร์เมื่ออุปกรณ์ Bluetooth ที่ได้เชื่อมต่อในช่วงล็อกอินออกห่างจากระยะ หรือล้างกล่องกาเครื่องหมายเพื่อยกเลิกการใช้งานตัวเลือกนี้

หมายเหตุ: โมดูล Bluetooth ในคอมพิวเตอร์ของคุณต้องสนับสนุนความสามารถนี้เพื่อที่จะใช้งานคุณสมบัตินี้

การ์ดต่าง ๆ

HP Client Security สามารถสนับสนุนการ์ดระบุตัวตนหลายประเภท โดยการ์ดดังกล่าวจะเป็นการ์ดพลาสติกขนาดเล็กที่มีชิปคอมพิวเตอร์ การ์ดดังกล่าว ได้แก่ สมาร์ทการ์ด การ์ดแบบไร้สัมผัส และการ์ดระยะใกล้ หากหนึ่งในการ์ดเหล่านี้ และตัวอ่านการ์ดที่เหมาะสมเชื่อมต่อกับคอมพิวเตอร์ หากผู้ดูแลระบบได้ติดตั้งไดรฟ์เวอร์ที่เกี่ยวข้องจากผู้ผลิต และหากผู้ดูแลระบบได้เปิดใช้งานการ์ดเป็นการรับรองความถูกต้องของข้อมูลประจำตัว คุณสามารถใช้การ์ดเป็นการรับรองความถูกต้องของข้อมูลประจำตัว

สำหรับสมาร์ทการ์ด ผู้ผลิตควรให้เครื่องมือเพื่อติดตั้งใบรับรองความปลอดภัยและการจัดการ PIN ที่ HP Client Security ในอัลกอริธึมความปลอดภัย จำนวนและประเภทของตัวอักขระที่ใช้เป็น PIN อาจแตกต่างกันไป ผู้ดูแลระบบจำเป็นต้องเริ่มการใช้งานสมาร์ทการ์ดก่อนที่จะสามารถใช้งานได้

HP Client Security สนับสนุนรูปแบบสมาร์ทการ์ดต่อไปนี้:

- CSP
- PKCS11

HP Client Security สนับสนุนรูปแบบการ์ดแบบไร้สัมผัสต่อไปนี้:

- การ์ดหน่วยความจำ HID iCLASS แบบไร้สัมผัส
- การ์ดหน่วยความจำ MiFare Classic 1k, 4k, และมินิแบบไร้สัมผัส

HP Client Security สนับสนุนรูปแบบการ์ดระยะใกล้ต่อไปนี้:

- การ์ดระยะใกล้ HID

ในการลงทะเบียนสมาร์ทการ์ด:

1. เสียบการ์ดในตัวอ่านสมาร์ทการ์ดที่ติดตั้งมา
2. เมื่อระบบตรวจจับการ์ดได้ ให้ป้อน PIN ของการ์ด จากนั้นคลิกหรือแตะ **ลงทะเบียน**

ในการเปลี่ยน PIN สมาร์ทการ์ด:

1. เสียบการ์ดในตัวอ่านสมาร์ทการ์ดที่ติดตั้งมา
2. เมื่อระบบตรวจจับการ์ดได้ ให้ป้อน PIN ของการ์ด จากนั้นคลิกหรือแตะ **รับรองความถูกต้อง**
3. คลิกหรือแตะ **เปลี่ยน PIN** จากนั้นป้อน PIN ใหม่

ในการลงทะเบียนการ์ดแบบไร้สัมผัสหรือการ์ดระยะใกล้:

1. วางการ์ดบนหรือใกล้ๆ ตัวอ่านที่เหมาะสม
2. เมื่อระบบตรวจจับการ์ดได้ ให้คลิกหรือแตะ **ลงทะเบียน**

ในการลบการ์ดที่ละเบียน:

1. เสียบการ์ดเข้ากับตัวอ่าน
2. สำหรับสมาร์ทการ์ดเท่านั้น ให้ป้อน PIN ที่กำหนดไว้ของการ์ด จากนั้นคลิกหรือแตะ **รับรองความถูกต้อง**
3. คลิกหรือแตะ **ลบ**

เมื่อลงทะเบียนการ์ดแล้ว รายละเอียดเกี่ยวกับการ์ดจะแสดงขึ้นมาภายใต้ **การ์ดลงทะเบียน** เมื่อลบการ์ดแล้ว การ์ดดังกล่าวจะถูกเอาออกไปจากรายการ

ในการเข้าถึงการตั้งค่าการ์ดระยะใกล้ การ์ดแบบไร้สัมผัส และสมาร์ทการ์ด ซึ่งเป็นที่ที่ผู้ดูแลระบบสามารถระบุการตั้งค่าที่เกี่ยวข้องกับข้อมูลประจำตัวของการ์ด ให้คลิกหรือแตะ **การตั้งค่า** (ต้องมีสิทธิ์ของผู้ดูแลระบบ)

การตั้งค่าการ์ดระยะใกล้ การ์ดแบบไร้สัมผัส และสมาร์ทการ์ด

ในการเข้าถึงการตั้งค่าสำหรับการ์ด ให้คลิกหรือแตะการ์ดดังกล่าวในรายการ จากนั้นคลิกหรือแตะลูกศรที่แสดง

ในการเปลี่ยน PIN สมาร์ทการ์ด:

1. ให้เสียบการ์ดเข้ากับตัวอ่าน
2. ป้อน PIN ที่กำหนดไว้ของการ์ด จากนั้นคลิกหรือแตะ **ดำเนินการต่อ**
3. ป้อนและยืนยัน PIN ใหม่ จากนั้นคลิกหรือแตะ **ดำเนินการต่อ**

ในการเริ่มการใช้งาน PIN สมาร์ทการ์ด:

1. ให้เสียบการ์ดเข้ากับตัวอ่าน
2. ป้อน PIN ที่กำหนดไว้ของการ์ด จากนั้นคลิกหรือแตะ **ดำเนินการต่อ**
3. ป้อนและยืนยัน PIN ใหม่ จากนั้นคลิกหรือแตะ **ดำเนินการต่อ**
4. คลิกหรือแตะ **ใช่** เพื่อยืนยันการเริ่มการใช้งาน

ในการล้างข้อมูลการ์ด:

1. ให้เสียบการ์ดเข้ากับตัวอ่าน
2. ป้อน PIN ที่กำหนดไว้ของการ์ด (สำหรับสมาร์ทการ์ดเท่านั้น) จากนั้นคลิกหรือแตะ **ดำเนินการต่อ**
3. คลิกหรือแตะ **ใช่** เพื่อยืนยันการลบ

PIN

หากผู้ดูแลระบบได้เปิดใช้งาน PIN เป็นการรับรองความถูกต้องของข้อมูลประจำตัว คุณสามารถตั้งค่า PIN ร่วมกับข้อมูลประจำตัวเพื่อเพิ่มความปลอดภัย

ในการตั้งค่า PIN ใหม่:

- ให้ป้อน PIN แล้วป้อนอีกครั้งเพื่อยืนยัน จากนั้นคลิกหรือแตะ **นำไปใช้**

ในการลบ PIN:

- ให้คลิกหรือแตะ **ลบ** จากนั้นคลิกหรือแตะ **ใช่** เพื่อยืนยัน

ในการเข้าถึงการตั้งค่า PIN ซึ่งเป็นที่ที่ผู้ดูแลระบบสามารถระบุการตั้งค่าที่เกี่ยงข้องกับข้อมูลประจำตัวของ PIN ให้คลิกหรือแตะ **การตั้งค่า** (ต้องมีสิทธิ์ของผู้ดูแลระบบ)

การตั้งค่า PIN

ในหน้าการตั้งค่า PIN คุณสามารถระบุความยาวต่ำสุดและสูงสุดที่ยอมรับได้สำหรับข้อมูลประจำตัวของ PIN

RSA SecurID

หากผู้ดูแลระบบได้เปิดใช้งาน RSA เป็นการรับรองความถูกต้องของข้อมูลประจำตัว และเงื่อนไขต่อไปนี้เป็นจริง คุณจะสามารถลงทะเบียนหรือลบข้อมูลประจำตัวของ RSA SecurID ได้

หมายเหตุ: มีการตั้งค่าที่เหมาะสม

- มีสร้างผู้ใช้บนเซิร์ฟเวอร์ RSA
- มีเชื่อมต่อโทเคน RSA SecurID ที่กำหนดให้กับผู้ใช้และคอมพิวเตอร์กับโดเมนเซิร์ฟเวอร์ RSA
- มีการติดตั้งซอร์ฟแวร์ SecurID บนคอมพิวเตอร์
- มีเชื่อมต่อพร้อมใช้งานสำหรับเซิร์ฟเวอร์ RSA ที่ได้รับการกำหนดค่าอย่างเหมาะสม

ในการลงทะเบียบข้อมูลประจำตัวของ RSA SecurID:

▲ ให้ป้อนชื่อผู้ใช้และรหัสผ่านของ RSA SecurID (รหัสโทเคนของ RSA SecurID หรือ PIN + รหัสโทเคน ขึ้นอยู่กับสภาพแวดล้อม) จากนั้นคลิกหรือแตะ **นำไปใช้**

เมื่อลงทะเบียนสำเร็จแล้ว ข้อความ "ได้ลงทะเบียนข้อมูลประจำตัวของ RSA SecurID สำเร็วแล้ว " จะแสดงขึ้นมา จากนั้นปุ่ม ลบ ก็จะเปิดใช้งาน

ในการลบข้อมูลประจำตัวของ RSA SecurID:

▲ ให้คลิก **ลบ** จากนั้นเลือก **ใช่** ในกล่องสนทนาป๊อปอัพ ซึ่งถามว่า "คุณแน่ใจว่าต้องการลบข้อมูลประจำตัว RSA SecurID ของคุณหรือไม่ ?"

Password Manager

การล็อกออนเว็บไซต์และโปรแกรมเป็นเรื่องที่ง่ายและปลอดภัยมากขึ้นเมื่อคุณใช้ Password Manager คุณสามารถสร้างรหัสผ่านที่มีประสิทธิภาพที่คุณไม่จำเป็นต้องจดหรือจำ จากนั้นล็อกออนอย่างง่ายดายและรวดเร็วด้วยลายนิ้วมือ, สมาร์ทการ์ด, การ์ดระยะใกล้, การ์ดแบบไร้สัมผัส, โทรศัพท์ Bluetooth, PIN, ข้อมูลประจำตัว RSA, หรือรหัสผ่าน Windows ของคุณ

หมายเหตุ: เนื่องจากโครงสร้างหน้าจอล็อกอินของเว็บเปลี่ยนแปลงตลอดเวลา ดังนั้น Password Manager จึงอาจไม่สามารถสนับสนุนเว็บไซต์ทั้งหมดได้ตลอดเวลา

Password Manager เสนอตัวเลือกต่อไปนี้:

หน้า Password Manager

- คลิกหรือแตะบัญชีเพื่อเปิดใช้งานเว็บเพจหรือโปรแกรมและล็อกออนโดยอัตโนมัติ
- จัดระเบียบบัญชีของคุณตามประเภท

ประสิทธิภาพของรหัสผ่าน

- โปรดตรวจสอบว่ารหัสผ่านของคุณมีความเสี่ยงด้านความปลอดภัยหรือไม่
- เมื่อเพิ่มข้อมูลล็อกอิน ให้ตรวจสอบประสิทธิภาพของรหัสผ่านนั้นๆ ที่ใช้สำหรับเว็บไซต์และโปรแกรม
- ประสิทธิภาพของรหัสผ่านจะระบุด้วยตัวแสดงสถานะเป็นสีแดง สีเหลือง หรือสีเขียว

ไอคอน **Password Manager** จะแสดงขึ้นมาที่มุมซ้ายบนของหน้าจอล็อกออนของเว็บเพจหรือโปรแกรม หากยังไม่ได้สร้างการล็อกออนสำหรับเว็บไซต์หรือโปรแกรมดังกล่าว เครื่องหมายบวกจะแสดงขึ้นมาบนไอคอน

▲ ให้คลิกหรือแตะไอคอน **Password Manager** เพื่อแสดงเมนูตามบริบทโดยคุณสามารถเลือกจากตัวเลือกต่อไปนี้:

- เพิ่ม [somedomain.com] ไปยัง Password Manager
- เปิด Password Manager

- การตั้งค่าไอคอน
- วิธีใช้

สำหรับเว็บเพจหรือโปรแกรมที่ยังไม่ได้สร้างการล็อกออน

ตัวเลือกต่อไปนี้จะแสดงขึ้นมาในเมนูตามบริบท:

- **เพิ่ม [somedomain.com] ไปยัง the Password Manager**–ช่วยให้คุณเพิ่มการล็อกออนสำหรับหน้าจอล็อกออนปัจจุบัน
- **เปิด Password Manager**–เปิดใช้งาน Password Manager
- **การตั้งค่าไอคอน**–ช่วยให้คุณระบุเงื่อนไขของไอคอน **Password Manager** ที่แสดงขึ้นมา
- **วิธีใช้**–แสดงวิธีใช้ HP Client Security

สำหรับเว็บเพจหรือโปรแกรมที่มีการสร้างการล็อกออนแล้ว

ตัวเลือกต่อไปนี้จะแสดงขึ้นมาในเมนูตามบริบท:

- **กรอกข้อมูลล็อกออน**–แสดงหน้า **ตรวจสอบข้อมูลระบุตัวตน** หากรับรองความถูกต้องสำเร็จแล้ว ระบบจะวางข้อมูลล็อกออนของคุณในฟิลด์ล็อกออน จากนั้นระบบก็ส่งหน้าดังกล่าว (หากมีการระบุว่ามีการส่งเมื่อมีการสร้างหรือแก้ไขล็อกออนล่าสุด)
- **แก้ไขล็อกออน**–ช่วยให้คุณแก้ไขข้อมูลล็อกออนสำหรับเว็บไซต์นี้
- **เพิ่มล็อกออน**–ช่วยให้คุณเพิ่มบัญชีไปยัง Password Manager
- **เปิด Password Manager**–เปิดใช้งาน Password Manager
- **วิธีใช้**–แสดงวิธีใช้ HP Client Security

หมายเหตุ: ผู้ดูแลระบบของคอมพิวเตอร์เครื่องนี้อาจกำหนดค่าให้ HP Client Security ต้องการข้อมูลประจำตัวมากกว่าหนึ่งข้อมูลขึ้นไปเมื่อตรวจสอบข้อมูลระบุตัวตนของคุณ

การเพิ่มล็อกออน

คุณสามารถเพิ่มการล็อกออนสำหรับเว็บไซต์หรือโปรแกรมได้อย่างง่ายดายโดยป้อนข้อมูลล็อกออนเพียงครั้งเดียว จากนั้น Password Manager ก็จะป้อนข้อมูลให้กับคุณโดยอัตโนมัติ คุณสามารถใช้การล็อกออนเหล่านี้ได้หลังจากเรียกดูเว็บไซต์หรือโปรแกรม

ในการเพิ่มการล็อกออน:

1. เปิดหน้าจอล็อกออนสำหรับเว็บไซต์หรือโปรแกรม
2. คลิกหรือแตะไอคอน **Password Manager** จากนั้นคลิกหรือแตะรายการต่อไปนี้ ทั้งนี้ขึ้นอยู่กับว่าเป็นหน้าจอล็อกออนสำหรับเว็บไซต์หรือโปรแกรม:
   - สำหรับเว็บไซต์ ให้คลิกหรือแตะ **เพิ่ม [ชื่อโดเมน] ไปยัง Password Manager**
   - สำหรับโปรแกรม ให้คลิกหรือแตะ **เพิ่มหน้าจอล็อกออนนี้ไปยัง Password Manager**
3. ป้อนข้อมูลล็อกออนของคุณ ฟิลด์ล็อกออนในหน้าจอ และฟิลด์ที่เกี่ยวข้องในกล่องโต้ตอบจะแสดงเป็นเส้นขอบหนาสีส้ม
   a. ในการป้อนข้อมูลฟิลด์ล็อกอินด้วยตัวเลือกต่อไปนี้ที่มีการกำหนดรูปแบบไว้ล่วงหน้า
   b. ในการดูรหัสผ่านสำหรับล็อกออนนี้ ให้คลิกหรือแตะ **แสดงรหัสผ่าน**
   c. ในการป้อนข้อมูลในฟิลด์ล็อกออน แต่ยังไม่ส่ง ให้ล้างกล่องกาเครื่องหมาย **ส่งข้อมูลล็อกออนโดยอัตโนมัติ**

d. คลิกหรือแตะ **ตกลง** เพื่อเลือกวิธีการรับรองความถูกต้องที่คุณต้องการใช้ (เช่น ลายนิ้วมือ, สมาร์ทการ์ด, การ์ดระยะใกล้, การ์ดแบบไร้สัมผัส, โทรศัพท์ Bluetooth, PIN หรือรหัสผ่าน) จากนั้นล็อกออนด้วยวิธีการรับรองความถูกต้องที่ได้เลือกไว้

ระบบจะเอาเครื่องหมายบวกออกจากไอคอน **Password Manager** เพื่อแจ้งให้คุณทราบว่าได้สร้างการล็อกออนแล้ว

e. หาก Password Manager ตรวจจับฟิลด์ล็อกออนไม่ได้ ให้คลิกหรือแตะ **ฟิลด์เพิ่มเติม**

- เลือกกล่องกาเครื่องหมายสำหรับแต่ละฟิลด์ที่ต้องการสำหรับการล็อกออน หรือล้างกล่องกาเครื่องหมายสำหรับฟิลด์ใดๆ ที่ไม่ต้องการสำหรับการล็อกออน
- คลิกหรือแตะ **ปิด**

แต่ละครั้งที่คุณเข้าใช้งานเว็บไซต์หรือเปิดโปรแกรมดังกล่าว ไอคอน **Password Manager** จะแสดงขึ้นมาที่มุมซ้ายบนของหน้าจอล็อกออนของเว็บไซต์หรือโปรแกรม เพื่อระบุว่าคุณสามารถใช้ข้อมูลประจำตัวที่ได้ลงทะเบียนไว้ในการล็อกออน

การแก้ไขการล็อกออน

ในการแก้ไขการล็อกออน:

1. เปิดหน้าจอล็อกออนสำหรับเว็บไซต์หรือโปรแกรม
2. ในการแสดงกล่องกาเครื่องหมายที่คุณสามารถแก้ไขข้อมูลล็อกออน ให้คลิกหรือแตะไอคอน **Password Manager** จากนั้นคลิกหรือแตะ **แก้ไขการล็อกออน**

   ฟิลด์ล็อกออนในหน้าจอ และฟิลด์ที่เกี่ยวข้องในกล่องโต้ตอบจะแสดงเป็นเส้นขอบหนาสีส้ม

   คุณยังสามารถแก้ไขข้อมูลบัญชีจากหน้า Password Manager โดยคลิกหรือแตะที่ล็อกออนดังกล่าวเพื่อแสดงตัวเลือกสำหรับการแก้ไข จากนั้นเลือก **แก้ไข**
3. แก้ไขข้อมูลการล็อกออน
   - ในการแก้ไข **ชื่อบัญชี** ให้ป้อนชื่อใหม่ในฟิลด์
   - ในการเพิ่มหรือแก้ไขชื่อ **ประเภท** ให้ป้อนหรือแก้ไขชื่อในฟิลด์ **ประเภท**
   - ในการเลือกฟิลด์ล็อกออน **ชื่อผู้ใช้** ด้วยตัวเลือกต่อไปนี้ที่มีการกำหนดรูปแบบไว้ล่วงหน้า

     ตัวเลือกที่มีการกำหนดรูปแบบไว้ล่วงหน้าจะมีให้เลือกใช้งานเมื่อมีการแก้ไขล็อกออนจากคำสั่งแก้ไขในเมนูตามบริบทของไอคอน Password Manager เท่านั้น
   - ในการเลือกฟิลด์ล็อกออน **รหัสผ่าน** ด้วยตัวเลือกต่อไปนี้ที่มีการกำหนดรูปแบบไว้ล่วงหน้า ให้คลิกหรือแตะลูกศรชี้ลงทางด้านขวาของฟิลด์

     ตัวเลือกที่มีการกำหนดรูปแบบไว้ล่วงหน้าจะมีให้เลือกใช้งานเมื่อมีการแก้ไขล็อกออนจากคำสั่งแก้ไขในเมนูตามบริบทของไอคอน Password Manager เท่านั้น
   - ในการเพิ่มฟิลด์เพิ่มเติมจากหน้าจอไปยังการล็อกออนของคุณ ให้คลิกหรือแตะ **ฟิลด์เพิ่มเติม**
   - ในการดูรหัสผ่านสำหรับการล็อกออนนี้ ให้คลิกหรือแตะไอคอน **แสดงรหัสผ่าน**
   - ในการป้อนข้อมูลในฟิลด์ล็อกออน แต่ยังไม่ส่ง ให้ล้างกล่องกาเครื่องหมาย **ส่งข้อมูลล็อกออนโดยอัตโนมัติ**
   - ในการระบุว่าล็อกออนนี้มีรหัสผ่านอันตราย ให้เลือกกล่องกาเครื่องหมาย **รหัสผ่านนี้เป็นอันตราย**

     หลังจากบันทึกการเปลี่ยนแปลง ข้อมูลล็อกออนอื่นๆ ทั้งหมดที่แชร์รหัสผ่านเดียวกับจะถูกระบุว่าเป็นอันตรายด้วย คุณสามารถเข้าใช้งานบัญชีที่ได้รับผลแต่ละบัญชีและเปลี่ยนรหัสผ่านได้หากจำเป็น
4. คลิกหรือแตะ **ตกลง**

การใช้เมนูลิงก์ด่วน Password Manager

Password Manager ให้วิธีการที่ง่ายและรวดเร็วในการเปิดใช้งานเว็บไซต์และโปรแกรมที่คุณได้สร้างการล็อกออน ให้ดับเบิลคลิกหรือแตะสองครั้งล็อกออนโปรแกรมหรือเว็บไซต์จากเมนู **ลิงก์ด่วน Password Manager** หรือจากหน้า Password Manager ภายใน HP Client Security เพื่อเปิดหน้าจอล็อกออน จากนั้นป้อนข้อมูลล็อกออนของคุณ

เมื่อคุณสร้างการล็อกออน ระบบจะเพิ่มการล็อกออนไปยังเมนู **ลิงก์ด่วน** Password Manager

ในการแสดงเมนู **ลิงก์ด่วน**:

- กดแป้นลัด **Password Manager** พร้อมกัน(Ctrl+แป้น Windows+h จะเป็นการเปิดการตั้งค่าจากโรงงาน) ในการเปลี่ยนการกดแป้นลัด จากหน้าหลักของ HP Client Security ให้คลิก **Password Manager** จากนั้นให้คลิกหรือแตะ **การตั้งค่า**

การจัดระเบียบการล็อกออนตามประเภท

สร้างหนึ่งประเภทหรือมากกว่านั้นเพื่อจัดเก็บการล็อกออนให้เป็นระเบียบ

ในการกำหนดประเภทการล็อกออน:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะ **Password Manager**
2. คลิกหรือแตะช่องป้อนข้อมูลของบัญชี จากนั้นคลิกหรือแตะ **แก้ไข**
3. ในฟิลด์ **ประเภท** ให้ป้อนชื่อประเภท
4. คลิกหรือแตะ **บันทึก**

ในการเอาบัญชีออกจากประเภท:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะ **Password Manager**
2. คลิกหรือแตะช่องป้อนข้อมูลของบัญชี จากนั้นคลิกหรือแตะ **แก้ไข**
3. ในฟิลด์ **ประเภท** ให้ลบชื่อประเภท
4. คลิกหรือแตะ **บันทึก**

ในการเปลี่ยนชื่อประเภท:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะ **Password Manager**
2. คลิกหรือแตะช่องป้อนข้อมูลของบัญชี จากนั้นคลิกหรือแตะ **แก้ไข**
3. ในฟิลด์ **ประเภท** ให้เปลี่ยนชื่อประเภท
4. คลิกหรือแตะ **บันทึก**

การจัดการการล็อกออน

Password Manager ทำให้การจัดการข้อมูลการล็อกออนสำหรับชื่อผู้ใช้ รหัสผ่าน และบัญชีล็อกออนหลายบัญชีได้ง่ายจากจุดเดียว

การล็อกออนของคุณจะระบุอยู่ในหน้า Password Manager

ในการจัดการการล็อกออนของคุณ:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะ **Password Manager**
2. คลิกหรือแตะการล็อกออนที่มีอยู่ แล้วเลือกตัวเลือกต่อไปนี้ จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ:
   - **แก้ไข**–แก้ไขการล็อกออน สำหรับข้อมูลเพิ่มเติม โปรดดู การแก้ไขการล็อกออน ในหน้า 18
   - **ล็อกอิน**–ล็อกอินบัญชีที่เลือกไว้
   - **ลบ**–ลบการล็อกออนสำหรับบัญชีที่เลือกไว้

ในการเพิ่มล็อกออนเพิ่มเติมสำหรับเว็บไซต์หรือโปรแกรม:

1. ให้เปิดหน้าจอล็อกออนสำหรับเว็บไซต์หรือโปรแกรม
2. คลิกหรือแตะไอคอน **Password Manager** เพื่อแสดงเมนูตามบริบท
3. คลิกหรือแตะ **เพิ่มล็อกออน** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ

การประเมินประสิทธิภาพของรหัสผ่าน

การใช้รหัสผ่านที่มีประสิทธิภาพสำหรับการล็อกออนเว็บไซต์หรือโปรแกรมของคุณเป็นสิ่งที่สำคัญในการปกป้องข้อมูลระบุตัวตนของคุณ

Password Manager ทำให้สามารถตรวจสอบและปรับปรุงความปลอดภัยของคุณได้ง่ายด้วยการวิเคราะห์ประสิทธิภาพของแต่ละรหัสผ่านที่ใช้ในการล็อกออนเว็บไซต์และโปรแกรมของคุณโดยอัตโนมัติ

ขณะที่คุณกำลังป้อนรหัสผ่านในช่วงการสร้างการล็อกออน Password Manager สำหรับบัญชี แถบสีจะแสดงขึ้นมาใต้รหัสผ่านเพื่อระบุประสิทธิภาพของรหัสผ่าน สีที่แสดงระบุค่าประสิทธิภาพต่อไปนี้:

- **แดง**–ประสิทธิภาพต่ำ
- **เหลือง**–ประสิทธิภาพปานกลาง
- **เขียว**–ประสิทธิภาพสูง

การตั้งค่าไอคอน Password Manager

Password Manager จะพยายามบ่งชี้หน้าจอล็อกออนสำหรับเว็บไซต์และโปรแกรม เมื่อตรวจสอบหน้าจอล็อกออนที่คุณยังไม่ได้สร้างการล็อกออนได้ Password Manager จะแจ้งให้คุณเพิ่มการล็อกออนสำหรับหน้าจอดังกล่าวโดยการแสดงไอคอน **Password Manager** พร้อมเครื่องหมายบวก

1. คลิกหรือแตะ **การตั้งค่าไอคอน** เพื่อปรับแต่งการทำงานของ Password Manager สำหรับการล็อกออนเว็บไซต์
   - **แจ้งให้เพิ่มการล็อกออนสำหรับหน้าจอล็อกออน**–คลิกหรือแตะตัวเลือกนี้เพื่อให้ Password Manager แจ้งให้คุณเพิ่มการล็อกออนเมื่อมีการแสดงหน้าจอล็อกออนที่ยังไม่มีการตั้งค่าล็อกออน
   - **ยกเว้นหน้าจอนี้**–เลือกกล่องกาเครื่องหมายเพื่อไม่ให้ Password Manager แจ้งให้คุณเพิ่มการล็อกอินสำหรับหน้าจอล็ออินนี้อีกครั้ง
   - **อย่าแจ้งเพื่อให้เพิ่มการล็อกออนสำหรับหน้าจอล็อกออน**–เลือกปุ่มเลือก
2. ในการเพิ่มการล็อกออนสำหรับหน้าจอที่มีการยกเว้นไว้ก่อนหน้านี้:
   a. ให้ล็อกออนเว็บไซต์ที่มีการยกเว้นไว้ก่อนหน้าที่
   b. ในการให้ Password Manager จำรหัสผ่านสำหรับเว็บไซต์นี้ ให้คลิกหรือแตะ **จำ** ในกล่องโต้ตอบป๊อบอัพเพื่อบันทึกรหัสผ่านและสร้างการล็อกออนสำหรับหน้าจอ
3. ในการเข้าถึงการตั้งค่า Password Manager ให้คลิกหรือแตะไอคอน Password Manager แล้วคลิกหรือแตะ **เปิด Password Manager** จากนั้นคลิกหรือแตะ **การตั้งค่า** ในหน้า Password Manager

การนำเข้าหรือส่งออกการล็อกออน

ในหน้า นำเข้าและส่งออกของ HP Password Manager คุณจะสามารถนำเข้าการล็อกอินที่บันทึกไว้ผ่านเว็บเบราว์เซอร์บนคอมพิวเตอร์ของคุณได้ คุณยังสามารถนำเข้าข้อมูลจากไฟล์ข้อมูลสำรองของ HP Client Security และส่งออกข้อมูลไปยังไฟล์ข้อมูลสำรองของ HP Client Security ได้อีกด้วย

- ในการเปิดใช้งานหน้านำเข้าและส่งออก ให้คลิกคลิกหรือแตะ **นำเข้าและส่งออก** ในหน้า Password Manager

ในการนำเข้ารหัสผ่านจากเบราว์เซอร์:

1. ให้คลิกหรือแตะเบราว์เซอร์จากที่คุณต้องการนำเข้ารหัสผ่าน (จะแสดงเฉพาะเบราว์เซอร์ที่ติดตั้งเท่านั้น)
2. ล้างกล่องกาเครื่องหมายสำหรับบัญชีที่คุณต้องการนำเข้ารหัสผ่าน
3. คลิกหรือแตะ **นำเข้า**

สามารถดำเนินการการนำเข้าข้อมูลจากหรือการส่งออกข้อมูลไปยังไฟล์ข้อมูลสำรอง HP Client Security ผ่านลิงก์ที่เกี่ยวข้อง (ภายใต้ **ตัวเลือกอื่นๆ)** ในหน้านำเข้าและส่งออก

หมายเหตุ: คุณสมบัตินี้จะนำเข้าและส่งออกเฉพาะข้อมูล Password Manager เท่านั้น สำหรับข้อมูลเกี่ยวกับการสำรองข้อมูลและการกู้คือข้อมูล HP Client Security เพิ่มเติม โปรดดู การสำรองและการกู้คืนข้อมูล ในหน้า 24

ในการนำเข้าข้อมูลจากไฟล์ข้อมูลสำรองของ HP Client Security:

1. จากหน้านำเข้าหรือส่งออก HP Password Manager ให้คลิกหรือแตะ **นำเข้าข้อมูลจากไฟล์ข้อมูลสำรองของ HP Client Security**
2. ตรวจสอบข้อมูลระบุตัวตนของคุณ
3. เลือกไฟล์ข้อมูลสำรองที่สร้างไว้ก่อนหน้านี้ หรือป้อนเส้นทางในฟิลด์ที่ให้มา จากนั้นคลิกหรือแตะ **เรียกดู**
4. ป้อนรหัสผ่านที่ใช้ในการปกป้องไฟล์ จากนั้นคลิกหรือแตะ **ถัดไป**
5. คลิกหรือแตะ **กู้คืนข้อมูล**

ในการส่งออกข้อมูลไปยังไฟล์ข้อมูลสำรองของ HP Client Security:

1. จากหน้านำเข้าและส่งออกของ HP Password Manager ให้คลิกหรือแตะ **ส่งออกข้อมูลจากไฟล์ข้อมูลสำรองของ HP Client Security**
2. ตรวจสอบข้อมูลระบุตัวตนของคุณ จากนั้นคลิกหรือแตะ **ถัดไป**
3. ป้อนชื่อสำหรับไฟล์ข้อมูลสำรอง โดยค่าเริ่มต้น ระบบจะบันทึกไฟล์ไปยังโฟลเดอร์เอกสาร ในการระบุตำแหน่งที่ตั้งอื่น ให้คลิกหรือแตะ **เรียกดู**
4. ป้อนหรือยืนยันรหัสผ่านเพื่อปกป้องไฟล์ จากนั้นคลิกหรือแตะ **บันทึก**

การตั้งค่า

คุณสามารถระบุการตั้งค่าส่วนบุคคลของ Password Manager:

- **แจ้งเพื่อให้เพิ่มการล็อกออนสำหรับหน้าจอล็อกออน**–ไอคอนThe **Password Manager** พร้อมเครื่องหมายบวยจะแสดงขึ้นมาเมื่อใดก็ตามที่มีการตรวจจับหน้าจอล็อกออนของเว็บไซต์หรือโปรแกรม ซึ่งระบุว่าคุณสามารถเพิ่มการล็อกออนสำหรับหน้าจอนี้ไปยังเมนู **การล็อกออน**

  ในการยกเลิกการใช้งานคุณสมบัตินี้ ให้ล้างกล่องกาเครื่องหมายข้าง **แจ้งเพื่อให้เพิ่มการล็อกออนสำหรับหน้าจอล็อกออน**

- **เปิด Password Manager ด้วย Ctrl+Win+h**–แป้นลัดเริ่มต้นที่ใช้เปิดเมนู **ลิงก์ด่วน Password Manager** คือ Ctrl+แป้น Windows+h

  ในการเปลี่ยนแป้นลัด ให้คลิกหรือแตะตัวเลือกนี้ จากนั้นป้อนการกดปุ่มพร้อมกันรูปแบบใหม่ รูปแบบการกดปุ่มพร้อมกันอาจประกอบด้วยปุ่มต่อไปนี้: ctrl, alt,หรือ Shift, และตัวเลขหรือตัวอักษรอย่างน้อยหนึ่งตัว

  ไม่สามารถใช้รูปแบบการกดปุ่มพร้อมกันที่สงวนไว้สำหรับ Windows หรือโปรแกรม Windows ได้

- ในการคืนการตั้งค่ากลับไปยังค่าเริ่มต้นจากโรงงาน ให้คลิกหรือแตะ **กู้คืนข้อมูลการตั้งค่า**

การตั้งค่าขั้นสูง

ผู้ดูแลระบบสามารถเข้าถึงตัวเลือกต่อไปนี้โดยเลือกไอคอน **รูปเกียร์** (การตั้งค่า) ในหน้าหลักของ HP Client Security

- **นโยบายผู้ดูแลระบบ**–ช่วยให้คุณกำหนดค่านโยบายการล็อกออนและเซสชันสำหรับผู้ดูแลระบบ
- **นโยบายผู้ใช้มาตรฐาน**–ช่วยให้คุณกำหนดค่านโยบายการล็อกออนและเซสชันสำหรับผู้ใช้มาตรฐาน
- **คุณสมบัติด้านความปลอดภัย**–ช่วยให้คุณเพิ่มความปลอดภัยของคอมพิวเตอร์โดยปกป้องบัญชี Windows โดยใช้การรับรองความถูกต้องที่มีประสิทธิภาพและ/หรือโดยเปิดใช้งานการรับรองความถูกต้องก่อนการเริ่มต้น Windows
- **ผู้ใช้**–ช่วยให้คุณจัดการผู้ใช้และข้อมูลประจำตัวของผู้ใช้
- **นโยบายของฉัน**–ช่วยให้คุณตรวจสอบนโยบายการรับรองความถูกต้องและสถานะการลงทะเบียน
- **สำรองและกู้คืนข้อมูล**–ช่วยให้คุณสำรองหรือกู้คืนข้อมูล HP Client Security
- **เกี่ยวกับ HP Client Security**–แสดงข้อมูลเวอร์ชันเกี่ยวกับ HP Client Security

นโยบายผู้ดูแลระบบ

คุณสามารถกำหนดค่านโยบายการล็อกออนและเซสชันสำหรับผู้ดูแลระบบของคอมพิวเตอร์เครื่องนี้ได้ นโยบายล็อกออนที่ตั้งค่าที่นี่จะควบคุมข้อมูลประจำตัวที่จำเป็นสำหรับผู้ดูแลระบบแบบโลคัลในการล็อกออน Windows นโยบายล็อกออนที่ตั้งค่าที่นี่จะควบคุมข้อมูลประจำตัวที่จำเป็นสำหรับผู้ดูแลระบบแบบโลคัลในการตรวจสอบข้อมูลระบุตัวตนภายในเซสชัน Windows

โดยค่าเริ่มต้น นโยบายใหม่หรือนโยบายที่มีการเปลี่ยนแปลงทั้งหมดจะมีผลทันทีหลังจากแตะหรือคลิก **นำไปใช้**

ในการเพิ่มนโยบายใหม่:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **นโยบายผู้ดูแลระบบ**
3. คลิกหรือแตะ **เพิ่มนโยบายใหม่**
4. คลิกลูกศรชี้ลงเพื่อเลือกข้อมูลประจำตัวหลักและรอง (เสริม) สำหรับนโยบายใหม่ จากนั้นคลิกหรือแตะ **เพิ่ม**
5. คลิก **นำไปใช้**

ในการหน่วงการมีผลของนโยบายใหม่หรือนโยบายที่มีการเปลี่ยนแปลง:

1. ให้คลิกหรือแตะ **ให้นโยบายนี้มีผลทันที**
2. เลือก **ให้นโยบายนโยบายมีผลตามวันที่ระบุ**
3. ป้อนวันที่หรือใช้ปฏิทินป๊อบอัพเพื่อเลือกวันที่ที่ควรจะให้นโยบายนี้มีผล
4. หากต้องการ ให้เลือกวันเวลาที่ควรแจ้งเตือนผู้ใช้เกี่ยวกับนโยบายใหม่ดังกล่าว
5. คลิก **นำไปใช้**

นโยบายผู้ใช้มาตรฐาน

คุณสามารถกำหนดค่านโยบายการล็อกออนและเซสชันสำหรับผู้ใช้มาตรฐานของคอมพิวเตอร์เครื่องนี้ได้ นโยบายล็อกออนที่ตั้งค่าที่นี่จะควบคุมข้อมูลประจำตัวที่จำเป็นสำหรับผู้ใช้มาตรฐานในการล็อกออน Windows นโยบายล็อกออนที่ตั้งค่าที่นี่จะควบคุมข้อมูลประจำตัวที่จำเป็นสำหรับผู้ใช้มาตรฐานในการตรวจสอบข้อมูลระบุตัวตนภายในเซสชัน Windows

โดยค่าเริ่มต้น นโยบายใหม่หรือนโยบายที่มีการเปลี่ยนแปลงทั้งหมดจะมีผลทันทีหลังจากแตะหรือคลิก **นำไปใช้**

ในการเพิ่มนโยบายใหม่:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **นโยบายผู้ใช้มาตรฐาน**
3. คลิกหรือแตะ **เพิ่มนโยบายใหม่**
4. คลิกลูกศรชี้ลงเพื่อเลือกข้อมูลประจำตัวหลักและรอง (เสริม) สำหรับนโยบายใหม่ จากนั้นคลิกหรือแตะ **เพิ่ม**
5. คลิก **นำไปใช้**

ในการหน่วงการมีผลของนโยบายใหม่หรือนโยบายที่มีการเปลี่ยนแปลง:

1. ให้คลิกหรือแตะ **ให้นโยบายนี้มีผลทันที**
2. เลือก **ให้นโยบายนโยบายมีผลตามวันที่ระบุ**
3. ป้อนวันที่หรือใช้ปฏิทินป๊อบอัพเพื่อเลือกวันที่ที่ควรจะให้นโยบายนี้มีผล
4. หากต้องการ ให้เลือกวันเวลาที่ควรแจ้งเตือนผู้ใช้เกี่ยวกับนโยบายใหม่ดังกล่าว
5. คลิก **นำไปใช้**

คุณสมบัติด้านความปลอดภัย

คุณสามารถเปิดใช้งานคุณสมบัติ HP Client Security ที่ช่วยปกป้องการเข้าใช้งานคอมพิวเตอร์โดยไม่ได้รับอนุญาต

ในการตั้งค่าคุณสมบัติด้านความปลอดภัย:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **คุณสมบัติด้านความปลอดภัย**
3. เปิดใช้งานคุณสมบัติด้านความปลอดภัยโดยเลือกกล่องกาเครื่องหมาย จากนั้นคลิกหรือแตะ **นำไปใช้** ยิ่งคุณเลือกคุณสมบัติมากเท่าใด คอมพิวเตอร์ของคุณก็ยิ่งปลอดภัยมากขึ้นเท่านั้น

   การตั้งค่าเหล่านี้จะนำไปใช้กับผู้ใช้ทั้งหมด

   - **ความปลอดภัยในการล็อกออน Windows**–ปกป้องบัญชี Windows ของคุณโดยการขอให้ระบุข้อมูลประจำตัวของ HP Client Security สำหรับการเข้าใช้งาน
   - **ความปลอดภัยก่อนบูต (การรับรองความถูกต้องเมื่อเปิดเครื่อง)**–ปกป้องคอมพิวเตอร์ของคุณก่อนการเริ่มต้น Windows จะไม่มีตัวเลือกให้เลือกใช้งาน หาก BIOS ไม่สนับสนุน
   - **อนุญาต One Step logon**–การตั้งค่านี้ช่วยข้ามขั้นการล็อกออน Windows หากมีการดำเนินการรับรองความถูกต้องก่อนหน้านี้ที่ระดับการรับรองความถูกต้องเมื่อเปิดเครื่องหรือระดับ Drive Encryption
4. คลิกหรือแตะ **ผู้ใช้** จากนั้นคลิกหรือแตะที่ไทล์ของผู้ใช้

ผู้ใช้

คุณสามารถตรวจสอบและจัดการผู้ใช้ HP Client Security ของคอมพิวเตอร์เครื่องนี้ได้

ในการเพิ่มผู้ใช้ Windows อื่นไปยัง HP Client Security:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **ผู้ใช้**
3. คลิกหรือแตะ **เพิ่มผู้ใช้ Windows อื่นไปยัง HP Client Security**

4. ป้อนชื่อผู้ใช้ที่คุณต้องการเพิ่ม จากนั้นคลิกหรือแตะ **ตกลง**
5. ป้อนรหัสผ่าน Windows ของผู้ใช้

   ไทล์สำหรับผู้ใช้ที่เพิ่มจะแสดงขึ้นมาในหน้าผู้ใช้

ในการลบผู้ใช้ Windows จากนี้ HP Client Security:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **ผู้ใช้**
3. คลิกหรือแตะชื่อผู้ใช้ที่คุณต้องการลบ
4. คลิกหรือแตะ **ลบผู้ใช้** จากนั้นคลิกหรือแตะ **ใช่** เพื่อยืนยัน

ในการแสดงข้อมูลสรุปนโยบายล็อกออนและเซสชันที่มีผลสำหรับผู้ใช้:

- คลิกหรือแตะ **ผู้ใช้** จากนั้นคลิกหรือแตะที่ไทล์ของผู้ใช้

นโยบายของฉัน

คุณสามารถตรวจสอบการรับรองความถูกต้องและสถานะการลงทะเบียนของคุณ หน้านโยบายของฉันยังให้ลิงก์เชื่อมโยงไปยังหน้านโยบายผู้ดูแลระบบและนโยบายผู้ใช้อีกด้วย

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **นโยบายของฉัน**

   นโยบายล็อกออนและเซสชันที่มีผลสำหรับผู้ที่ล็อกออนปัจจุบันจะแสดงขึ้นมา

หน้านโยบายของฉันยังให้ลิงก์เชื่อมโยงไปยัง นโยบายผู้ดูแลระบบ ในหน้า 22 และ นโยบายผู้ใช้มาตรฐาน ในหน้า 22 อีกด้วย

การสำรองและการกู้คืนข้อมูล

ขอแนะนำให้คุณสำรองข้อมูล HP Client Security ของคุณเป็นประจำ ความถี่ของการสำรองข้อมูลขึ้นอยู่กับความถี่ที่ข้อมูลเปลี่ยนแปลง ตัวอย่างเช่น หากคุณเพิ่มการล็อกออนใหม่ทุกวัน คุณควรสำรองข้อมูลทุกวัน

การสำรองข้อมูลยังสามารถนำไปใช้เพื่อโยกย้ายข้อมูลจากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่ง ซึ่งยังเรียกการนำเข้าหรือการส่งออก

หมายเหตุ: คุณสมบัตินี้จะสำรองเฉพาะข้อมูลของ Password Manager เท่านั้น Drive Encryption มีวิธีการสำรองข้อมูลแยกต่างหาก Device Access Manager และการรับรองความถูกต้องของลายนิ้วมือจะไม่ได้รับการสำรองข้อมูล

ต้องมีการติดตั้ง HP Client Security บนคอมพิวเตอร์ใดๆ ที่จะรับข้อมูลที่สำรองไว้ก่อนที่จะสามารถกู้คืนไฟล์ข้อมูลสำรองได้

ในการสำรองข้อมูลของคุณ:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **นโยบายผู้ดูแลระบบ**
3. ให้คลิกหรือแตะ **สำรองและกู้คืนข้อมูล**
4. คลิกหรือแตะ **สำรองข้อมูล** จากนั้นตรวจสอบข้อมูลระบุตัวตนของคุณ
5. เลือกโมดูลที่คุณต้องการรวมในข้อมูลสำรอง จากนั้นคลิกหรือแตะ **ถัดไป**
6. ป้อนชื่อสำหรับไฟล์เก็บข้อมูล โดยค่าเริ่มต้น ระบบจะบันทึกไฟล์ไปยังโฟลเดอร์เอกสาร ในการระบุตำแหน่งที่ตั้งอื่น ให้คลิกหรือแตะ **เรียกดู**

7. ให้ป้อนและยืนยันรหัสผ่านเพื่อปกป้องไฟล์
8. คลิกหรือแตะ **บันทึก**

ในการกู้คืนข้อมูลของคุณ:

1. จากหน้าหลักของ HP Client Security ให้คลิกหรือแตะไอคอน **รูปเกียร์**
2. ในหน้าการตั้งค่าขั้นสูง ให้คลิกหรือแตะ **นโยบายผู้ดูแลระบบ**
3. ให้คลิกหรือแตะ **สำรองและกู้คืนข้อมูล**
4. เลือก **กู้คืนข้อมูล** จากนั้นตรวจสอบข้อมูลระบุตัวตนของคุณ
5. เลือกไฟล์เก็บข้อมูลที่สร้างไว้ก่อนหน้านี้ ป้อนเส้นทางในฟิลด์ที่ให้ไว้ ในการระบุตำแหน่งที่ตั้งอื่น ให้คลิกหรือแตะ **เรียกดู**
6. ป้อนรหัสผ่านที่ใช้ในการปกป้องไฟล์ จากนั้นคลิกหรือแตะ **ถัดไป**
7. เลือกโมดูลที่คุณต้องการกู้คืนข้อมูล
8. คลิกหรือแตะ **กู้คืนข้อมูล**

5 HP Drive Encryption (มีเฉพาะบางรุ่นเท่านั้น)

HP Drive Encryption ให้การปกป้องข้อมูลอย่างสมบูรณ์แบบโดยการเข้ารหัสข้อมูลของคอมพิวเตอร์ของคุณ เมื่อปิดใช้งาน Drive Encryption คุณจำเป็นต้องล็อกอินที่หน้าจอล็อกอินของ Drive Encryption ที่จะแสดงขึ้นมาก่อนที่ระบบปฏิบัติการ Windows® เริ่มทำงาน

หน้าจอหลักของ HP Client Security ช่วยให้ผู้ดูแลระบบ Windows เปิดใช้งาน Drive Encryption, สำรองข้อมูลคีย์เข้ารหัส และเลือกหรือยกเลิกการเลือกไดรฟ์หรือพาร์ติชันสำหรับการเข้ารหัส สำหรับข้อมูลเพิ่มเติม โปรดดูวิธีใช้ซอฟต์แวร์ HP Client Security

สามารถดำเนินงานต่อไปนี้ด้วย Drive Encryption:

- การเลือกการตั้งค่า Drive Encryption:
  - การเข้าหรือถอดรหัสแต่ละไดรฟ์หรือพาร์ติชันโดยใช้การเข้ารหัสซอฟต์แวร์
  - การเข้าหรือถอดรหัสไดรฟ์แบบเข้ารหัสเองแต่ละตัวโดยใช้การเข้ารหัสฮาร์ดแวร์
  - การเพิ่มความปลอดภัยมากขึ้นโดยปิดใช้งานโหมดสลีปหรือสแตนด์บาย เพื่อทำให้แน่ใจว่ามีการรับรองความถูกต้องก่อนบูตเสมอ

หมายเหตุ: สามารถเข้ารหัสฮาร์ดไดรฟ์ SATA ภายในและ SATA ภายนอกได้เท่านั้น

- การสร้างคีย์การสำรอง
- การกู้คืนสิทธิ์การเข้าใช้งานคอมพิวเตอร์ที่ถูกเข้ารหัสโดยใช้คีย์การสำรองและ HP SpareKey
- การเปิดใช้งานการรับรองความถูกต้องก่อนบูตของ Drive Encryption โดยใช้รหัสผ่าน ลายนิ้วมือที่ลงทะเบียน หรือ PIN สำหรับสมาร์ทการ์ดบางประเภท

การเปิด Drive Encryption

ผู้ดูแลระบบสามารถเข้าใช้งาน Drive Encryption โดยการเปิด HP Client Security:

1. จากหน้าจอเริ่มต้น ให้คลิกหรือแตะที่แอพ **HP Client Security** (Windows 8)

   - หรือ -

   จากเดสก์ท็อป Wondows ให้ดับเบิลคลิกหรือแตะสองครั้งที่ไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ประมาณขวาสุดของแถบงาน

2. คลิกหรือแตะไอคอน **Drive Encryption**

งานทั่วไป

การเปิดใช้งาน Drive Encryption สำหรับฮาร์ดไดรฟ์มาตรฐาน

ฮาร์ดไดรฟ์มาตรฐานจะถูกเข้ารหัสโดยใช้การเข้ารหัสซอฟต์แวร์ ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อเข้ารหัสไดรฟ์หรือพาร์ติชันดิสก์:

1. เปิดใช้งาน **Drive Encryption** สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด Drive Encryption ในหน้า 26
2. เลือกกล่องกาเครื่องหมายสำหรับไดฟร์หรือพาร์ติชันที่คุณต้องการเข้ารหัส จากนั้นคลิกหรือแตะ **คีย์การสำรอง**

> **หมายเหตุ:** เพื่อความปลอดภัยที่ดียิ่งขึ้น ให้เลือกกล่องกาเครื่องหมาย **ยกเลิกการใช้งานโหมดสลีปเพื่อเพิ่มความปลอดภัย** เมื่อคุณยกเลิกการใช้งานโหมดสลีป จะไม่มีความเสี่ยงใดๆ ทั้งสิ้นในการจัดเก็บข้อมูลประจำตัวที่ใช้ในการปลดล็อกไดรฟ์ในหน่วยความจำ

3. เลือกตัวเลือกการสำรองข้อมูล จากนั้นคลิกหรือแตะ **สำรองข้อมูล** สำหรับข้อมูลเพิ่มเติม โปรดดู การสำร้องข้อมูลคีย์เข้ารหัส ในหน้า 30
4. คุณสามารถดำเนินการต่อขณะที่มีการสำรองข้อมูลคีย์เข้ารหัสอยู่ อย่ารีบูตคอมพิวเตอร์ของคุณ

> **หมายเหตุ:** คุณจะได้รับการแจ้งเพื่อให้รีสตาร์ทคอมพิวเตอร์ หลังจากรีสตาร์ท หน้าจอก่อนบูตของ Drive Encryption จะแสดงขึ้นมา เพื่อขอการรับรองความถูกต้องก่อน Windows จะเริ่มต้น

Drive Encryption ได้ถูกเปิดใช้งาน การเข้ารหัสพาร์ติชันไดรฟ์ที่เลือกไว้อาจใช้เวลาหลายชั่วโมง ทั้งนี้ขึ้นอยู่กับจำนวนและขนาดของพาร์ติชัน

สำหรับข้อมูลเพิ่มเติม โปรดดูวิธีใช้ซอฟต์แวร์ HP Client Security

การเปิดใช้งาน Drive Encryption สำหรับไดรฟ์แบบเข้ารหัสเอง

สามารถเข้ารหัสไดรฟ์แบบเข้ารหัสเองที่ตรงกับข้อมูลจำเพาะ OPAL ของ Trusted Computing Group สำหรับการจัดการไดรฟ์แบบเข้ารหัสเอง โดยใช้การเข้ารหัสซอฟต์แวร์หรือการเข้ารหัสฮาร์ดแวร์ การเข้ารหัสฮาร์ดแวร์จะเร็วกว่าการเข้ารหัสซอฟต์แวร์อย่างมาก อย่างไรก็ดี คุณไม่สามารถเลือกพาร์ติชันไดรฟ์ที่จะเข้ารหัสได้ เนื่องจากมีการเข้ารหัสทั้งดิสก์ ซึ่งรวมถึงพาร์ติชันใดๆ ก็ตามของดิสก์

ในการเข้ารหัสพาร์ติชันจำเพาะ คุณจำเป็นต้องใช้การเข้ารหัสซอฟต์แวร์ โปรดตรวจสอบว่าได้ล้างกล่องกาเครื่องหมาย **อนุญาตการเข้ารหัสฮาร์ดแวร์สำหรับไดรฟ์แบบเข้ารหัสเอง (SED) เท่านั้น**

ปฏิบัติตามขั้นตอนต่อไปนี้เพื่อเปิดใช้งาน Drive Encryption สำหรับไดรฟ์แบบเข้ารหัสเอง:

1. เปิดใช้งาน **Drive Encryption** สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด Drive Encryption ในหน้า 26
2. เลือกกล่องกาเครื่องหมายสำหรับไดฟร์ที่คุณต้องการเข้ารหัส จากนั้นคลิกหรือแตะ **คีย์การสำรอง**

> **หมายเหตุ:** เพื่อความปลอดภัยที่ดียิ่งขึ้น ให้เลือกกล่องกาเครื่องหมาย **ยกเลิกการใช้งานโหมดสลีปเพื่อเพิ่มความปลอดภัย** เมื่อคุณยกเลิกการใช้งานโหมดสลีป จะไม่มีความเสี่ยงใดๆ ทั้งสิ้นในการจัดเก็บข้อมูลประจำตัวที่ใช้ในการปลดล็อกไดรฟ์ในหน่วยความจำ

3. เลือกตัวเลือกการสำรองข้อมูล จากนั้นคลิกหรือแตะ **สำรองข้อมูล** สำหรับข้อมูลเพิ่มเติม โปรดดู การสำร้องข้อมูลคีย์เข้ารหัส ในหน้า 30
4. คุณสามารถดำเนินการต่อขณะที่มีการสำรองข้อมูลคีย์เข้ารหัสอยู่ อย่ารีบูตคอมพิวเตอร์ของคุณ

> **หมายเหตุ:** สำหรับไดรฟ์แบบเข้ารหัสเอง คุณจะได้รับการแจ้งเตือนเพื่อให้ปิดคอมพิวเตอร์

สำหรับข้อมูลเพิ่มเติม โปรดดูวิธีใช้ซอฟต์แวร์ HP Client Security

การปิดใช้งาน Drive Encryption

1. เปิดใช้งาน **Drive Encryption** สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด Drive Encryption ในหน้า 26
2. ล้างกล่องกาเครื่องหมายสำหรับไดรฟ์ทั้งหมดที่ถูกเข้ารหัส จากนั้นคลิกหรือแตะ **นำไปใช้**

   การปิดใช้งาน Drive Encryption จะเริ่มต้น

   หมายเหตุ: หากใช้การเข้ารหัสซอฟต์แวร์ การถอดรหัสจะเริ่มต้น ซึ่งอาจใช้เวลาหลายชั่วโมง ทั้งนี้ขึ้นอยู่กับขนาดพาร์ติชันของฮาร์ดไดรฟ์ที่ถูกเข้ารหัส เมื่อถอดรหัสเสร็จสมบูรณ์ Drive Encryption ก็จะถูกปิดใช้งาน

   หากใช้การเข้ารหัสฮาร์ดแวร์ ไดรฟ์จะถูกถอดรหัสในทันที และหลังจากนั้นไม่กี่นาที Drive Encryption ก็จะถูกปิดใช้งาน

   ทันทีที่ Drive Encryption ถูกเปิดใช้งาน คุณจะได้รับการแจ้งให้ปิดคอมพิวเตอร์หากมีการเข้ารหัสฮาร์ดแวร์ หรือให้รีสตาร์ทคอมพิวเตอร์หากมีการเข้ารหัสซอฟต์แวร์

การล็อกอินหลังจากเปิดใช้งาน Drive Encryption

เมื่อคุณเปิดคอมพิวเตอร์หลังจากเปิดใช้งาน Drive Encryption และมีการลงทะเบียนบัญชีผู้ใช้ของคุณแล้ว คุณจะต้องล็อกอินที่หน้าจอล็อกอิน Drive Encryption:

หมายเหตุ: หากมาจากโหมดสลีปหรือสแตนด์บาย การรับรองความถูกต้องก่อนบูตของ Drive Encryption จะไม่แสดงขึ้นมาสำหรับการเข้ารหัสซอฟต์แวร์หรือการเข้ารหัสฮาร์ดแวร์ การเข้ารหัสฮาร์ดแวร์ให้ตัวเลือก **ยกเลิกการใช้งานโหมดสลีปเพื่อเพิ่มความปลอดภัย** ซึ่งจะช่วยป้องกันไม่ให้เข้าสู่โหมดสลีปหรือสแตนด์บาย เมื่อเปิดใช้งาน

หากมาจากโหมดไฮเบอร์เนต การรับรองความถูกต้องก่อนบูตของ Drive Encryption จะแสดงขึ้นมาสำหรับทั้งการเข้ารหัสซอฟต์แวร์หรือการเข้ารหัสฮาร์ดแวร์

หมายเหตุ: หากผู้ดูแลระบบ Windows ได้เปิดใช้งานความปลอดภัยก่อนบูต BIOS ใน HP Client Security และหาก One-Step Logon ได้เปิดใช้งาน (ค่าเริ่มต้น) คุณสามารถล็อกอินคอมพิวเตอร์ได้ทันทีหลังจากการรับรองความถูกต้องในช่วงก่อนบูต BIOS โดยไม่จำเป็นต้องรับรองความถูกต้องใหม่ในหน้าจอล็อกอินของ Drive Encryption

การล็อกออนแบบผู้ใช้คนเดียว:

- ในหน้า **ล็อกออน** ให้ป้อนรหัสผ่าน Windows, PIN สมาร์ทการ์ด, SpareKey, หรือปัดนิ้วมือที่ลงทะเบียน

การล็อกออนแบบผู้ใช้หลายคน:

1. ในหน้า **เลือกผู้ใช้เพื่อล็อกออน** ให้เลือกผู้ใช้ที่จะล็อกออนจากรายการแบบหล่นลง จากนั้นคลิกหรือแตะ **ถัดไป**
2. ในหน้า **ล็อกออน** ให้ป้อนรหัสผ่าน Windows, PIN สมาร์ทการ์ด, หรือปัดนิ้วมือที่ลงทะเบียน

หมายเหตุ: สนับสนุนสมาร์ทการ์ดต่อไปนี้:

สมาร์ทการ์ดที่สนับสนุน

- Gemalto Cyberflex Access 64k V2c

หมายเหตุ: หากใช้คีย์การกู้คืนในการล็อกอินที่หน้าจอล็อกอินของ Drive Encryption จำเป็นต้องระบุข้อมูลประจำตัวเพิ่มเติมที่หน้าล็อกออน Windows เพื่อเข้าใช้งานบัญชีผู้ใช้

การเข้ารหัสฮาร์ดไดรฟ์เพิ่มเติม

ขอแนะนำอย่างยิ่งให้คุณใช้ HP Drive Encryption เพื่อป้องกันข้อมูลของคุณโดยการเข้ารหัสฮาร์ดไดรฟ์ หลังจากเปิดใช้งาน ฮาร์ดไดรฟ์ที่เพิ่มหรือพาร์ติชันที่สร้างสามารถถูกเข้ารหัสโดยปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดใช้งาน **Drive Encryption** สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด Drive Encryption ในหน้า 26
2. สำหรับไดรฟ์ที่ถูกเข้ารหัสซอฟต์แวร์ ให้เลือกพาร์ติชันไดรฟ์ที่จะเข้ารหัส

หมายเหตุ: นอกจากนี้ยังใช้ได้ในกรณีที่มีไดฟร์แบบผสม โดยมีฮาร์ดไดรฟ์มาตรฐานอย่างน้อยหนึ่งไดรฟ์และไดรฟ์แบบเข้ารหัสเองอย่างน้อยหนึ่งไดรฟ์อยู่

- หรือ -

- สำหรับไดฟร์ที่ถูกเข้ารหัสฮาร์ดแวร์ ให้เลือกไดรฟ์ที่จะเข้ารหัสเพิ่มเติม

งานขั้นสูง

การจัดการ Drive Encryption (งานของผู้ดูแลระบบ)

ผู้ดูแลระบบสามารถใช้ Drive Encryption เพื่อดูและเปลี่ยนแปลงสถานะการเข้ารหัส (ไม่ถูกเข้ารหัสหรือถูกเข้ารหัส) ของฮาร์ดไดฟร์ทั้งหมดบนคอมพิวเตอร์

- หากมีสถานะเปิดใช้งาน แสดงว่ามีการเปิดใช้งานและกำหนดค่า Drive Encryption ไดรฟ์อยู่ในหนึ่งของสถานะต่อไปนี้:

การเข้ารหัสซอฟต์แวร์

- ไม่ได้เข้ารหัส
- เข้ารหัสแล้ว
- กำลังเข้ารหัส
- กำลังถอดรหัส

การเข้ารหัสฮาร์ดแวร์

- เข้ารหัสแล้ว
- ไม่ถูกเข้ารหัส (สำหรับไดรฟ์เพิ่มเติม)

การเข้ารหัสหรือการถอดรหัสแต่ละพาร์ติชันของไดรฟ์ (เฉพาะการเข้ารหัสซอฟต์แวร์เท่านั้น)

ผู้ดูแลระบบสามารถใช้ Drive Encryption เพื่อเข้ารหัสพาร์ติชันของฮาร์ดไดรฟ์ในคอมพิวเตออย่างหนึ่งน้อยพาร์ติชันร์หรือเพื่อถอดรหัสพาร์ติชันไดรฟ์ใดๆ ที่ถูกเข้ารหัสไว้แล้ว

1. เปิดใช้งาน **Drive Encryption** สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด Drive Encryption ในหน้า 26
2. ภายใต้ **สถานะไดรฟ์** ให้เลือกหรือล้างกล่องกาเครื่องหมายที่อยู่ถัดจากแต่ละพาร์ติชันของฮาร์ดไดรฟ์ที่คุณต้องการเข้ารหัสหรือถอดรหัส จากนั้นคลิกหรือแตะ **นำไปใช้**

หมายเหตุ: เมื่อกำลังเข้ารหัสหรือถอดรหัสพาร์ติชัน แถบความคืบหน้าจะแสดงเปอร์เซ็นต์ของพาร์ติชันที่ถูกเข้ารหัส

หมายเหตุ: ไม่สนับสนุนพาร์ติชันแบบไดนามิก หากพาร์ติชันแสดงสถานะว่า พร้อมใช้งาน แต่ไม่สามารถเข้ารหัสได้เมื่อเลือก แสดงว่าพาร์ติชันดังกล่าวเป็นพาร์ติชันแบบไดนามิก พาร์ติชันแบบไดนามิกมีผลมาจากการหดพาร์ติชันเพื่อสร้างพาร์ติชันใหม่ภายในการจัดการดิสก์

คำเตือนจะแสดงขึ้นมาหากพาร์ติชันจะถูกแปลงไปเป็นพาร์ติชันแบบไดนามิก

การจัดการดิสก์

- **ชื่อเรียก**–คุณสามารถตั้งชื่อไดรฟ์หรือพาร์ติชันของคุณเพื่อให้ง่ายต่อการระบุมากขึ้น
- **ไดรฟ์ที่ถูกยกเลิกการเชื่อมต่อ**–Drive Encryption สามารถติดตามดิสก์ที่ถูกถอดออกจากคอมพิวเตอร์ได้ ดิสก์ที่ถูกถอดออกจากเครื่องคอมพิวเตอร์จะถูกย้ายไปยังรายการส่วนประกอบที่ถูกยกเลิกการเชื่อมต่อโดยอัตโนมัติ หากได้คืนดิสก์ดังกล่าวกลับสู่ระบบตามเดิม ดิสก์ดังกล่าวก็จะปรากฏขึ้นในรายการส่วนประกอบถูกเชื่อมต่ออีกครั้ง
- หากคุณไม่ต้องการติดตามหรือจัดการไดรฟ์ที่ถูกยกเลิกการเชื่อมต่ออีก คุณสามารถเอาไดฟร์ที่ถูกยกเลิกการเชื่อมต่อออกจากรายการส่วนประกอบที่ถูกยกเลิกการเชื่อมต่อ
- Drive Encryption ยังคงเปิดใช้งานอยู่จนกว่าจะมีการล้างกล่องกาเครื่องหมายสำหรับไดรฟ์ทั้งหมดที่ถูกเชื่อมต่อ และรายการส่วนประกอบที่ถูกยกเลิกการเชื่อมต่อก็จะว่าง

การสำรองและการกู้คืนข้อมูล (งานของผู้ดูแลระบบ)

เมื่อเปิดใช้งาน Drive Encryption ผู้ใช้จะสามารถใช้หน้าการสำรองข้อมูลคีย์เข้ารหัส เพื่อสำรองข้อมูลคีย์เข้ารหัสไปยังสื่อบันทึกแบบถอดได้และเพื่อทำการกู้คืนข้อมูล

การสำร้องข้อมูลคีย์เข้ารหัส

ผู้ดูแลระบบสามารถสำรองข้อมูลคีย์เข้ารหัสสำหรับไดรฟ์ที่ถูกเข้ารหัสในอุปกรณ์เก็บข้อมูลแบบถอดได้

ข้อควรระวัง: โปรดตรวจสอบว่าได้เก็บรักษาอุปกรณ์เก็บข้อมูลที่มีคีย์การสำรองในที่ที่ปลอดภัย เพราะหากคุณลืมรหัสผ่าน ทำสมาร์ทการ์ดหาย หรือไม่ได้ลงทะเบียนนิ้วมือ อุปกรณ์นี้ก็จะเป็นหนทางเดียวในการเข้าใช้งานคอมพิวเตอร์ นอกจากนี้ สถานที่จัดเก็บข้อมูลควรมีความปลอดภัย เพราะอุปกรณ์จัดเก็บข้อมูลจะอนุญาตให้เข้าใช้งาน Windows ได้

1. เปิดใช้งาน **Drive Encryption** สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด Drive Encryption ในหน้า 26
2. เลือกกล่องกาเครื่องหมายสำหรับไดรฟ์ จากนั้นคลิกหรือแตะ **คีย์การสำรอง**
3. ภายใต้ **สร้างคีย์การกู้คืน HP Drive Encryption** ให้เลือกตัวเลือกต่อไปนี้:
   - **อุปกรณ์จัดเก็บข้อมูลแบบถอดได้**–เลือกกล่องกาเครื่องหมาย จากนั้นเลือกอุปกรณ์จัดเก็บข้อมูลที่จะมีการบันทึกคีย์เข้ารหัส
   - **SkyDrive**–เลือกกล่องกาเครื่องหมาย คุณจะต้องเชื่อมต่อกับอินเทอร์เน็ต ล็อกอิน Microsoft SkyDrive จากนั้นคลิกหรือแตะ **ใช่**

     หมายเหตุ: ในการใช้คีย์การสำรอง HP Drive Encryption ที่จัดเก็บไว้ที่ SkyDrive คุณจำเป็นต้องดาวน์โหลดจาก SkyDrive ไปยังอุปกรณ์จัดเก็บข้อมูลแบบถอดได้ จากนั้นเสียบอุปกรณ์จัดเก็บข้อมูลเข้ากับคอมพิวเตอร์เครื่องนี้
   - **TPM** (บางรุ่นเท่านั้น)–ช่วยให้คุณกู้คืนข้อมูลโดยใช้รหัสผ่าน TPM

     ข้อควรระวัง: หากมีการล้าง TPM หรือคอมพิวเตอร์มีการชำรุดเสียหาย คุณจะสูญเสียการเข้าถึงการสำรองข้อมูลดังกล่าว หากเลือกวิธีการนี้ คุณควรเลือกวิธีการสำรองข้อมูลแบบอื่นด้วย
4. คลิกหรือแตะ **สำรองข้อมูล**

   คีย์เข้ารหัสจะถูกบันทึกไว้ในอุปกรณ์จัดเก็บข้อมูลที่คุณได้เลือกไว้

การกู้คืนการเข้าใช้งานคอมพิวเตอร์ที่ถูกเปิดใช้งานโดยใช้คีย์การสำรอง

ผู้ดูแลระบบสามารถดำเนินการกู้คืนข้อมูลโดยใช้คีย์ Drive Encryption ที่มีการสำรองข้อมูลไว้ที่อุปกรณ์จัดเก็บข้อมูลแบบถอดได้เมื่อมีการเปิดใช้งาน หรือโดยเลือกตัวเลือก **คีย์การสำรอง** ใน Drive Encryption

1. เสียบอุปกรณ์จัดเก็บข้อมูลแบบถอดได้ที่มีคีย์การสำรอง
2. เปิดเครื่องคอมพิวเตอร์
3. เมื่อกล่องโต้ตอบการล็อกอินของ HP Drive Encryption เปิดขึ้นมา ให้คลิกหรือแตะ **การกู้คืนข้อมูล**

4. ป้อนเส้นทางไฟล์หรือชื่อไฟล์ที่มีคีย์การสำรองของคุณ จากนั้นคลิกหรือแตะ **การกู้คืนข้อมูล**
5. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้คลิกหรือแตะ **ตกลง**

   หน้าจอล็อกออน Windows จะแสดงขึ้นมา

หมายเหตุ: หากใช้คีย์การกู้คืนในการล็อกออนที่หน้าจอล็อกอินของ Drive Encryption จำเป็นต้องระบุข้อมูลประจำตัวเพิ่มเติมที่หน้าล็อกออน Windows เพื่อเข้าใช้งานบัญชีผู้ใช้ ขอแนะนำอย่างยิ่งให้คุณรีเซ็ตรหัสผ่านหลังจากดำเนินการกู้คืนข้อมูล

การดำเนินการกู้คืนข้อมูล HP SpareKey

คุณจำเป็นต้องตอบคำถามรักษาความปลอดภัยให้ถูกต้องก่อนที่คุณจะสามารถเข้าใช้งานคอมพิวเตอร์เพื่อกู้คืนข้อมูล SpareKey ภายในช่วงก่อนบูต Drive Encryption สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าการกู้คืนข้อมูล SpareKey โปรดดูวิธีใช้ซอฟต์แวร์ HP Client Security

ในการดำเนินการกู้คืนข้อมูล HP SpareKey หากคุณลืมรหัสผ่าน:

1. เปิดเครื่องคอมพิวเตอร์
2. เมื่อหน้าเพจ HP Drive Encryption แสดงขึ้นมา ให้นำทางไปยังหน้าล็อกออนของผู้ใช้
3. คลิก **SpareKey**

หมายเหตุ: หากไม่เคยมีการเริ่มใช้งาน SpareKey ใน HP Client Security มาก่อน จะไม่มีปุ่ม **SpareKey** ให้เลือกใช้งาน

4. พิมพ์คำตอบที่ถูกต้องสำหรับคำถามที่แสดงขึ้นมา จากนั้นคลิก**ล็อกออน**

   หน้าจอล็อกออน Windows จะแสดงขึ้นมา

หมายเหตุ: หากใช้ SpareKey เพื่อล็อกออนที่หน้าจอล็อกอิน Drive Encryption จำเป็นต้องมีข้อมูลประจำตัวเพิ่มเติมเมื่อล็อกออน Windows เพื่อเข้าใช้งานบัญชีผู้ใช้ ขอแนะนำอย่างยิ่งให้คุณรีเซ็ตรหัสผ่านหลังจากดำเนินการกู้คืนข้อมูล

6 HP File Sanitizer (มีเฉพาะบางรุ่นเท่านั้น)

File Sanitizer จะอนุญาตให้คุณแบ่งปันสินทรัพย์อย่างปลอดภัย (ตัวอย่างเช่น: ข้อมูลหรือไฟล์ส่วนบุคคล ข้อมูลประวัติหรือข้อมูลที่เกี่ยวข้องกับเว็บ หรือส่วนประกอบอื่นๆ ของข้อมูล) ในฮาร์ดไดรฟ์ภายในของคอมพิวเตอร์ และช่วยให้ล้างฮาร์ดไดรฟ์ภายในของคอมพิวเตอร์เป็นระยะได้อย่างปลอดภัย

File Sanitizer ไม่สามารถใช้ในการทำความสะอาดหรือล้างไดรฟ์ประเภทต่อไปนี้:

- Solid-state drives (SSD) ซึ่งรวมถึงไดรฟ์ข้อมูล RAID ที่ใช้ขยายความสามารถของอุปกรณ์ SSD
- ไดรฟ์ภายนอกที่เชื่อมต่อโดยการอินเทอร์เฟซผ่าน USB, Firewire หรือ eSATA

หากพยายามดำเนินการลบถาวรหรือล้าง SSD ข้อความคำเตือนจะแสดงขึ้นมา และจะไม่มีการดำเนินการดังกล่าว

การลบถาวร

การลบถาวรจะแตกต่างจากการลบใน Windows® เมื่อคุณทำลายสินทรัพย์โดยใช้ File Sanitizer ไฟล์จะถูกเขียนทับด้วยข้อมูลที่ไม่มีความหมาย ทำให้ไม่สามารถกู้คืนข้อมูลดั้งเดิมได้ การลบอย่างง่ายใน Windows อาจไม่มีผลต่อไฟล์ (หรือสินทรัพย์) ในฮาร์ดไดรฟ์ หรือไฟล์หรือสินทรัพย์อยู่ในสถานะที่อาจใช้วิธีการตรวจพิสูจน์เพื่อกู้คืนได้

คุณสามารถกำหนดเวลาทำลายล่วงหน้า หรือคุณสามารถเปิดใช้งานการลบถาวรด้วยตัวเองโดยเลือกไอคอน **File Sanitizer** ในหน้าจอหลักของ HP Client Security หรือใช้ไอคอน **File Sanitizer** บนเดสก์ท็อป Windows สำหรับข้อมูลเพิ่มเติม โปรดอ้างอิง การตั้งค่ากำหนดเวลาทำลาย ในหน้า 33, การลบถาวรโดยคลิกขวา ในหน้า 35, หรือ การเริ่มต้นการลบถาวรด้วยตัวเอง ในหน้า 35

หมายเหตุ: ไฟล์ .dll จะถูกทำลายและเอาออกจากระบบก็ต่อเมื่อมีการย้ายไปยังถังรีไซเคิล

การล้างพื้นที่ว่าง

การลบสินทรัพย์ใน Windows ไม่ได้เอาเนื้อหาของสินทรัพย์ออกจากฮาร์ดไดรฟ์ของคุณโดยสิ้นเชิง Windows จะลบเฉพาะข้อมูลอ้างอิงของสินทรัพย์ หรือตำแหน่งที่ตั้งในฮาร์ดไดรฟ์เท่านั้น เนื้อหาของสินทรัยพ์ยังคงอยู่ในฮาร์ดไดร์ฟจนกว่าสินทรัพย์อื่นจะเขียนทับพื้นที่เดียวกันกับในฮาร์ดไดร์ฟด้วยข้อมูลใหม่

การล้างพื้นที่ว่างช่วยให้คุณเขียนข้อมูลสุ่มทับข้อมูลที่ลบอย่างปลอดภัย ช่วยป้องกันไม่ให้ผู้ใช้ดูเนื้อหาดั้งเดิมของสินทรัพย์ที่ถูกลบ

หมายเหตุ: การล้างพื้นที่ว่างไม่ได้เพิ่มความปลอดภัยให้กับสินทรัพย์ที่ถูกลบ

คุณสามารถกำหนดเวลาการล้างพื้นที่ว่างล่วงหน้า หรือคุณสามารถเปิดใช้งานการล้างพื้นที่ว่างของสินทรัพย์ที่ถูกลบด้วยตัวเองโดยเลือกไอคอน **File Sanitizer** ในหน้าจอหลัก HP Client Security หรือโดยใช้ไอคอน **File Sanitizer** บนเดสก์ท็อป Windows สำหรับข้อมูลเพิ่มเติม โปรดดู การตั้งค่ากำหนดเวลาการล้างพื้นที่ว่าง ในหน้า 34, การเริ่มต้นการล้างพื้นที่ว่างด้วยตัวเอง ในหน้า 36, หรือ การใช้ไอคอน File Sanitizer ในหน้า 35

การเปิด File Sanitizer

1. จากหน้าจอเริ่มต้น ให้คลิกหรือแตะที่แอพ **HP Client Security** (Windows 8)

   - หรือ -

   จากเดสก์ท็อป Wondows ให้ดับเบิลคลิกหรือแตะสองครั้งที่ไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ประมาณขวาสุดของแถบงาน

2. ภายใต้ **ข้อมูล** ให้คลิกหรือแตะ **File Sanitizer**

- หรือ -

▲ ให้ดับเบิลคลิกหรือแตะสองครั้งที่ไอคอน **File Sanitizer** บนเดสก์ท็อป Windows

- หรือ -

▲ ให้คลิกขวาหรือแตะไอคอน **File Sanitizer** บนเดสก์ท็อป Windows ค้างไว้ จากนั้นเลือก **เปิด File Sanitizer**

ขั้นตอนการตั้งค่า

การลบถาวร–File Sanitizer จะลบหรือทำลายประเภทข้อมูลที่เลือกอย่างปลอดภัย

1. ภายใต้ **การลบถาวร** ให้เลือกกล่องกาเครื่องหมายสำหรับไฟล์แต่ละประเภทที่จะทำลาย หรือล้างกล่องกาเครื่องหมายหากคุณไม่ต้องการลบถาวรไฟล์เหล่านั้น
   - **ถังรีไซเคิล**–ทำลายข้อมูลทั้งหมดที่อยู่ภายในถังรีไซเคิล
   - **ไฟล์ระบบชั่วคราว**–ทำลายไฟล์ทั้งหมดที่พบในโฟลเดอร์ชั่วคราวของระบบ ระบบจะค้นหาตัวแปรของสภาพแวดล้อมต่อไปนี้ตามลำดับดังนี้ และเส้นทางแรกที่พบจะถือว่าเป็นโฟลเดอร์ระบบ:
     - TMP
     - TEMP
   - **ไฟล์อินเทอร์เน็ตชั่วคราว**–ทำลายสำเนาเว็บเพจ ภาพ และสื่อบันทึกที่บันทึกโดยเว็บเบราว์เซอร์เพื่อช่วยให้ชมได้รวดเร็วยิ่งขึ้น
   - **คุกกี้**–ทำลายไฟล์ทั้งหมดที่จัดเก็บไว้ในคอมพิวเตอร์โดยเว็บไซต์ เพื่อบันทึกการตั้งค่าส่วนบุคคล เช่น ข้อมูลล็อกอิน
2. ในการเริ่มต้นการลบถาวร ให้คลิกหรือแตะ **ทำลาย**

การล้าง–เขียนข้อมูลสุ่มไปยังพื้นที่ว่างและป้องกันการกู้คืนรายการที่ถูกลบ

▲ ในการเริ่มต้นการล้าง ให้คลิกหรือแตะ **ล้าง**

ตัวเลือก File Sanitizer–เลือกกล่องกาเครื่องหมายเพื่อเปิดใช้งานตัวเลือกต่อไปนี้ หรือล้างกล่องเครื่องหมายเพื่อยกเลิกการใช้งานตัวเลือก:

- **เปิดใช้งานไอคอนเดสก์ท็อป**–แสดงไอคอน File Sanitizer บนเดสก์ท็อป Windows
- **เปิดใช้งานคลิกขวา**–ช่วยให้คุณคลิกขวาหรือแตะที่สินทรัพย์ค้างไว้ จากนั้นเลือก **HP File Sanitizer - ทำลาย**
- **ขอรหัสผ่าน Windows ก่อนการลบถาวรด้วยตัวเอง**–ต้องการการรับรองความถูกต้องด้วยรหัสผ่าน Windows ก่อนการลบถาวรข้อมูลด้วยตัวเอง
- **ทำลายคุกกี้และไฟล์อินเทอร์เน็ตชั่วคราวเมื่อปิดเบราว์เซอร์**–ทำลายสินทรัพย์ที่เกี่ยวข้องกับเว็บที่เลือกไว้ทั้งหมด เช่น ประวัติ URL ของเบราว์เซอร์ เมื่อคุณปิดเว็บเบราว์เซอร์

การตั้งค่ากำหนดเวลาทำลาย

คุณสามารถกำหนดเวลาเพื่อทำลายโดยอัตโนมัติ หรือคุณยังสามารถทำลายสินทรัพย์ด้วยตัวเองได้ทุกเมื่อ สำหรับข้อมูลเพิ่มเติม โปรดดู ขั้นตอนการตั้งค่า ในหน้า 33

1. เปิด File Sanitizer จากนั้นคลิกหรือแตะ **การตั้งค่า**
2. ในการกำหนดเวลาล่วงหน้าเพื่อทำลายสินทรัพย์ที่เลือกไว้ ภายใต้ **กำหนดเวลาทำลาย** ให้เลือก **ไม่**, **หนึ่งครั้ง**, **ทุกวัน**, **ทุกสัปดาห์**, หรือ **ทุกเดือน** จากนั้นเลือกวันและเวลา:
   a. คลิกหรือแตะฟิลด์ชั่วโมง นาที หรือ AM/PM
   b. เลื่อนจนกว่าค่าที่ต้องการจะแสดงขึ้นมาในระดับเดียวกับฟิลด์อื่น

c. คลิกหรือแตะพื้นที่สีขาวรอบๆ ฟิลด์การตั้งค่าเวลา

d. ทำซ้ำสำหรับแต่ละฟิลด์จนกว่าจะได้การกำหนดเวลาที่ต้องการเลือก

3. มีรายการสินทรัพย์สี่ประเภทดังต่อไปนี้:

- **ถังรีไซเคิล**–ทำลายข้อมูลทั้งหมดที่อยู่ภายในถังรีไซเคิล
- **ไฟล์ระบบชั่วคราว**–ทำลายไฟล์ทั้งหมดที่พบในโฟลเดอร์ชั่วคราวของระบบ ระบบจะค้นหาตัวแปรของสภาพแวดล้อมต่อไปนี้ตามลำดับดังนี้ และเส้นทางแรกที่พบจะถือว่าเป็นโฟลเดอร์ระบบ:
  - TMP
  - TEMP
- **ไฟล์อินเทอร์เน็ตชั่วคราว**–ทำลายสำเนาเว็บเพจ ภาพ และสื่อบันทึกที่บันทึกโดยเว็บเบราว์เซอร์เพื่อช่วยให้ชมได้รวดเร็วยิ่งขึ้น
- **คุกกี้**–ทำลายไฟล์ทั้งหมดที่จัดเก็บไว้ในคอมพิวเตอร์โดยเว็บไซต์ เพื่อบันทึกการตั้งค่าส่วนบุคคล เช่น ข้อมูลล็อกอิน

หากมีการเลือกตัวเลือกนี้ สินทรัพย์เหล่านี้จะถูกทำลายตามกำหนดเวลา

4. ในการเลือกสินทรัพย์แบบกำหนดเองเพิ่มเติมเพื่อที่จะทำลาย:

a. ภายใต้ **รายการลบถาวรตามกำหนดเวลา** ให้คลิกหรือแตะ **เพิ่มโฟลเดอร์** จากนั้นนำทางไปยังไฟล์หรือโฟล์เดอร์

b. คลิกหรือแตะ **เปิด** จากนั้นคลิกหรือแตะ **ตกลง**

ในการเอาสินทรัพย์ออกจากรายการลบถาวรตามกำหนดเวลา ให้ล้างกล่องกาเครื่องหมายสำหรับสินทรัพย์ดังกล่าว

การตั้งค่ากำหนดเวลาการล้างพื้นที่ว่าง

การล้างพื้นที่ว่างไม่ได้เพิ่มความปลอดภัยให้กับสินทรัพย์ที่ถูกลบ

1. เปิด File Sanitizer จากนั้นคลิกหรือแตะ **การตั้งค่า**
2. ในการกำหนดเวลาล่วงหน้าเพื่อล้างฮาร์ดไดรฟ์ ภายใต้ **กำหนดเวลาการล้าง** ให้เลือก **ไม่**, **หนึ่งครั้ง**, **ทุกวัน**, **ทุกสัปดาห์**, หรือ **ทุกเดือน** จากนั้นเลือกวันและเวลา:

a. คลิกหรือแตะฟิลด์ชั่วโมง นาที หรือ AM/PM

b. เลื่อนจนกว่าเวลาที่ต้องการจะแสดงขึ้นมาในระดับเดียวกับฟิลด์อื่น

c. คลิกหรือแตะพื้นที่สีขาวรอบๆ ฟิลด์การตั้งค่าเวลา

d. ทำซ้ำจนกว่าจะได้การกำหนดเวลาที่ต้องการเลือก

หมายเหตุ: การดำเนินการล้างพื้นที่ว่างสามารถใช้เวลานานมาก โปรดตรวจสอบว่าได้เชื่อมต่อคอมพิวเตอร์ของคุณกับไฟ AC แม้ว่าจะทำการล้างพื้นที่ว่างในพื้นหลัง แต่การใช้งานโปรเซสเซอร์ที่เพิ่มขึ้นอาจมีผลต่อประสิทธิภาพการทำงานของคอมพิวเตอร์ของคุณได้ สามารถทำการล้างพื้นที่ว่างนอกเวลางานหรือเมื่อไม่ได้ใช้คอมพิวเตอร์ดังกล่าว

การป้องกันไฟล์จากการลบถาวร

ในการป้องกันไฟล์หรือโฟล์เดอร์จากการลบถาวร:

1. เปิด File Sanitizer จากนั้นคลิกหรือแตะ **การตั้งค่า**
2. ภายใต้ **รายการห้ามทำลาย** ให้คลิกหรือแตะ **เพิ่มโฟลเดอร์** จากนั้นนำทางไปยังไฟล์หรือโฟลเดอร์
3. คลิกหรือแตะ **เปิด** จากนั้นคลิกหรือแตะ **ตกลง**

หมายเหตุ: ไฟล์ในรายการนี้จะได้รับการป้องกันตราบใดที่ยังอยู่ในรายการดังกล่าว

ในการเอาสินทรัพย์ออกจากรายการยกเว้น ให้ล้างกล่องเครื่องหมายสำหรับสินทรัพย์ดังกล่าว

งานทั่วไป

ให้ใช้ File Sanitizer ในการดำเนินงานต่อไปนี้:

- **ใช้ไอคอน File Sanitizer เพื่อเริ่มการลบถาวร**–ลากไฟล์ไปยังไอคอน **File Sanitizer** บนเดสก์ท็อป Windows สำหรับรายละเอียด โปรดดู การใช้ไอคอน File Sanitizer ในหน้า 35
- **ทำลายสินทรัพย์จำเพาะหรือสินทรัพย์ที่เลือกไว้ทั้งหมดด้วยตัวเอง**–ทำลายรายการต่างๆ ได้ทุกเมื่อ โดยไม่ต้องรอให้ถึงเวลาทำลายตามกำหนดเวลา สำหรับรายเอียด โปรดดู การลบถาวรโดยคลิกขวา ในหน้า 35 หรือ การเริ่มต้นการลบถาวรด้วยตัวเอง ในหน้า 35
- **เปิดใช้งานการล้างพื้นที่ว่างด้วยตัวเอง**–เปิดใช้งานการล้างพื้นที่ว่างได้ทุกเมื่อ สำหรับรายละเอียด โปรดดู การเริ่มต้นการล้างพื้นที่ว่างด้วยตัวเอง ในหน้า 36
- **ดูไฟล์บันทึก**–ดูไฟล์บันทึกการลบถาวรและการล้างพื้นที่ว่างที่มีข้อผิดพลาดหรือข้อขัดข้องใดๆ จากการดำเนินการลบถาวรหรือการล้างพื้นที่ว่างล่าสุด สำหรับรายละเอียด โปรดดู การดูไฟล์บันทึก ในหน้า 36

หมายเหตุ: การดำเนินการลบถาวรหรือการล้างพื้นที่ว่างสามารถใช้เวลานานมาก แม้ว่าจะทำลายหรือล้างพื้นที่ว่างในพื้นหลัง แต่การใช้งานโปรเซสเซอร์ที่เพิ่มขึ้นอาจมีผลต่อประสิทธิภาพการทำงานของคอมพิวเตอร์ของคุณได้

การใช้ไอคอน File Sanitizer

ข้อควรระวัง: สินทรัพย์ที่ถูกลบถาวรไม่สามารถกู้คืนได้ ให้พิจารณารายการที่คุณเลือกอย่างระมัดระวังหากคุณเลือกทำลายด้วยตัวเอง

เมื่อคุณเริ่มต้นการลบถาวรด้วยตัวเอง สินทรัยพ์ที่อยู่ในรายการลบถาวรมาตรฐานในมุมมอง File Sanitizer จะถูกทำลาย (โปรดดู ขั้นตอนการตั้งค่า ในหน้า 33)

คุณสามารถเริ่มต้นการลบถาวรด้วยตัวเองด้วยวิธีการต่อไปนี้:

1. ให้เปิด File Sanitizer (โปรดดู การเปิด File Sanitizer ในหน้า 32) จากนั้นคลิกหรือแตะ **ทำลาย**
2. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้ตรวจสอบว่าได้ทำเครื่องหมายเลือกสินทรัพย์ที่คุณต้องการลบถาวร จากนั้นคลิกหรือแตะ **ตกลง**

- หรือ -

1. ให้คลิกขวาหรือแตะไอคอน **File Sanitizer** บนเดสก์ท็อป Windows ค้างไว้ จากนั้นคลิกหรือแตะ **ทำลายเดี๋ยวนี้**
2. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้ตรวจสอบว่าได้ทำเครื่องหมายเลือกสินทรัพย์ที่คุณต้องการลบถาวร จากนั้นคลิกหรือแตะ **ทำลาย**

การลบถาวรโดยคลิกขวา

ข้อควรระวัง: สินทรัพย์ที่ถูกลบถาวรไม่สามารถกู้คืนได้ ให้พิจารณารายการที่คุณเลือกอย่างระมัดระวังหากคุณเลือกทำลายด้วยตัวเอง

หากเลือก **เปิดใช้งานการลบถาวรโดยคลิกขวา** ในมุมมอง File Sanitizer คุณสามารถทำลายสินทรัพย์ดังนี้:

1. นำทางไปยังเอกสารหรือโฟลเดอร์ที่คุณต้องการลบถาวร
2. คลิกขวาหรือแตะที่ไฟล์หรือโฟลเดอร์ค้างไว้ จากนั้นเลือก **HP File Sanitizer - ทำลาย**

การเริ่มต้นการลบถาวรด้วยตัวเอง

ข้อควรระวัง: สินทรัพย์ที่ถูกลบถาวรไม่สามารถกู้คืนได้ ให้พิจารณารายการที่คุณเลือกอย่างระมัดระวังหากคุณเลือกทำลายด้วยตัวเอง

เมื่อคุณเริ่มต้นการลบถาวรด้วยตัวเอง สินทรัพย์ที่อยู่ในรายการลบถาวรมาตรฐานในมุมมอง File Sanitizer จะถูกทำลาย (โปรดดู ขั้นตอนการตั้งค่า ในหน้า 33)

คุณสามารถเริ่มต้นการลบถาวรด้วยตัวเองด้วยวิธีการต่อไปนี้:

1. ให้เปิด File Sanitizer (โปรดดู การเปิด File Sanitizer ในหน้า 32) จากนั้นคลิกหรือแตะ **ทำลาย**
2. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้ตรวจสอบว่าได้ทำเครื่องหมายเลือกสินทรัพย์ที่คุณต้องการลบถาวร จากนั้นคลิกหรือแตะ **ตกลง**

- หรือ -

1. ให้คลิกขวาหรือแตะไอคอน **File Sanitizer** บนเดสก์ท็อป Windows ค้างไว้ จากนั้นคลิกหรือแตะ **ทำลายเดี๋ยวนี้**
2. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้ตรวจสอบว่าได้ทำเครื่องหมายเลือกสินทรัพย์ที่คุณต้องการลบถาวร จากนั้นคลิกหรือแตะ **ทำลาย**

การเริ่มต้นการล้างพื้นที่ว่างด้วยตัวเอง

เมื่อคุณเริ่มต้นการล้างด้วยตัวเอง สินทรัพย์ที่อยู่ในรายการลบถาวรมาตรฐานในมุมมอง File Sanitizer จะถูกล้าง (โปรดดู ขั้นตอนการตั้งค่า ในหน้า 33)

คุณสามารถเริ่มต้นการล้างด้วยตัวเองด้วยวิธีการต่อไปนี้:

1. ให้เปิด File Sanitizer (ดู การเปิด File Sanitizer ในหน้า 32) จากนั้นคลิกหรือแตะ **ล้าง**
2. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้คลิกหรือแตะ **ตกลง**

- หรือ -

1. ให้คลิกขวาหรือแตะไอคอน **File Sanitizer** บนเดสก์ท็อป Windows ค้างไว้ จากนั้นคลิกหรือแตะ **ล้างเดี๋ยวนี้**
2. เมื่อกล่องโต้ตอบการยืนยันเปิดขึ้นมา ให้คลิกหรือแตะ **ล้าง**

การดูไฟล์บันทึก

แต่ละครั้งที่มีดำเนินการลบถาวรหรือการล้างพื้นที่ว่าง ระบบจะสร้างไฟล์บันทึกข้อผิดพลาดหรือข้อขัดข้องใดๆ ขึ้นมา ไฟล์บันทึกจะมีการอัปเดตเสมอตามการดำเนินการลบถาวรหรือการล้างพื้นที่ว่างล่าสุด

หมายเหตุ: ไฟล์ที่ถูกทำลายหรือล้างสำเร็จจะไม่ปรากฏอยู่ในไฟล์บันทึก

ระบบจะสร้างไฟล์บันทึกสำหรับการดำเนินการลบถาวร และจะสร้างไฟล์บันทึกอีกไฟล์หนึ่งสำหรับการดำเนินการล้างพื้นที่ว่าง ไฟล์บันทึกทั้งสองอยู่ในฮาร์ดไดรฟ์ในโฟลเดอร์ต่อไปนี้:

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

สำหรับระบบแบบ 64 บิต ไฟล์บันทึกจะอยู่ในในฮาร์ดไดรฟ์ในโฟลเดอร์ต่อไปนี้:

- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_ShredderLog.txt
- C:\Program Files (x86)\Hewlett-Packard\File Sanitizer*[Username]*_DiskBleachLog.txt

7 HP Device Access Manager (มีเฉพาะบางรุ่นเท่านั้น)

HP Device Access Manager ควบคุมการเข้าใช้งานข้อมูลโดยยกเลิกการใช้งานอุปกรณ์ถ่ายโอนข้อมูล

หมายเหตุ: อุปกรณ์ที่ติดต่อสื่อสารกับมนุษย์/อุปกรณ์ที่ได้รับอินพุตจากมนุษย์บางอย่าง เช่น เมาส์ แป้นพิมพ์ ทัชแพด และตัวอ่านลายนิ้วมือไม่ได้ถูกควบคุมโดย Device Access Manager สำหรับข้อมูลเพิ่มเติม โปรดดู ประเภทอุปกรณ์ที่ถูกจัดการ ในหน้า 40

ผู้ดูแลระบบ Windows® ใช้ HP Device Access Manager ในการควบคุมการเข้าใช้งานอุปกรณ์ในระบบและเพื่อป้องกันการใช้งานที่ไม่ได้รับอนุญาต:

- โปรไฟล์อุปกรณ์จะถูกสร้างขึ้นสำหรับผู้ใช้แต่ละคน เพื่อกำหนดว่าอุปกรณ์ใดได้รับอนุญาตหรือปฏิเสธสิทธิ์การเข้าใช้งาน
- Just In Time Authentication (JITA) ช่วยให้ผู้ใช้ที่กำหนดไว้ล่วงหน้าสามารถรับรองความถูกต้องของตนเองเพื่อเข้าใช้งานอุปกรณ์ที่มิฉะนั้นจะถูกปฏิเสธ
- ผู้ดูแลระบบและผู้ใช้ที่เชื่อถือได้จะสามารถถูกยกเว้นจากข้อห้ามสำหรับการเข้าถึงอุปกรณ์ที่บังคับใช้โดย Device Access Manager โดยการเพิ่มไว้ที่กลุ่มผู้ดูแลระบบอุปกรณ์ ความเป็นสมาชิกของกลุ่มนี้จะถูกจัดการโดยใช้การตั้งค่าขั้นสูง
- สามารถให้สิทธิ์หรือปฏิเสธการเข้าใช้งานอุปกรณ์ตามหลักพื้นฐานของการเป็นสมาชิกกลุ่มหรือสำหรับผู้ใช้เป็นรายบุคคล
- สำหรับคลาสอุปกรณ์ประเภทไดร์ฟซีดีรอมและไดร์ฟดีวีดี การเข้าถึงการเขียนและการอ่านจะได้รับอนุญาตและปฏิเสธแยกจากกัน

HP Device Access Manager จะได้รับการกำหนดค่าโดยอัตโนมัติโดยการตั้งค่าต่อไปนี้ในช่วงการดำเนินการของตัวช่วยการติดตั้ง HP Client Security:

- สามารถเปิดใช้งานสื่อบันทึกแบบถอดได้ที่มี Just In Time Authentication (JITA) สำหรับผู้ดูแลระบบและผู้ใช้
- นโยบายอุปกรณ์จะให้สิทธิ์การใช้งานเต็มรูปแบบแก่อุปกรณ์อื่นๆ

การเปิด Device Access Manager

1. จากหน้าจอเริ่มต้น ให้คลิกหรือแตะที่แอพ **HP Client Security** (Windows 8)

   - หรือ -

   จากเดสก์ท็อป Wondows ให้ดับเบิลคลิกหรือแตะสองครั้งที่ไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ประมาณขวาสุดของแถบงาน

2. ภายใต้ **อุปกรณ์** ให้คลิกหรือแตะ **สิทธิ์การเข้าใช้งานอุปกรณ์**

   - ผู้ใช้มาตรฐานสามารถดูการเข้าใช้งานอุปกรณ์ปัจจุบันได้ (โปรดดู มุมมองผู้ใช้ ในหน้า 38)
   - ผู้ดูแลระบบสามารถดูและทำการเปลี่ยนแปลงต่อการเข้าใช้งานของอุปกรณ์ซึ่งปัจจุบันได้รับการกำหนดค่าสำหรับคอมพิวเตอร์โดยคลิกหรือแตะ **เปลี่ยนแปลง** จากนั้นป้อนรหัสผ่านผู้ดูแลระบบ (โปรดดู มุมมองระบบ ในหน้า 38)

มุมมองผู้ใช้

เมื่อเลือก **สิทธิ์การเข้าใช้งานอุปกรณ์** มุมมองผู้ใช้จะแสดงขึ้นมา ผู้ใช้และผู้ดูแลระบบมาตรฐานสามารถดูการเข้าใช้งานของตนเองสำหรับอุปกรณ์ประเภทต่างๆ หรือแต่ละอุปกรณ์ในคอมพิวเตอร์นี้

- **ผู้ใช้ปัจจุบัน**–ชื่อของผู้ใช้ที่ได้ล็อกออนในปัจจุบันจะแสดงขึ้นมา
- **ประเภทอุปกรณ์**–ประเภทของอุปกรณ์จะแสดงขึ้นมา
- **การเข้าใช้งาน**–การเข้าใช้งานอุปกรณ์ประเภทต่างๆ หรืออุปกรณ์บางประเภทที่ได้รับการกำหนดค่าในปัจจุบันของคุณจะแสดงขึ้นมา
- **ระยะเวลา**–ขอบเขตเวลาสำหรับการเข้าใช้งานไดรฟ์ CD/DVD-ROM หรือไดรฟ์ดิสก์แบบถอดได้จะแสดงขึ้นมา
- **การตั้งค่า**–ผู้ดูแลระบบสามารถเปลี่ยนแปลงว่าไดรฟ์ใดจะมีการเข้าใช้งานที่ควบคุมโดย Device Access Manager

มุมมองระบบ

ในมุมมองระบบ ผู้ดูแลระบบสามารถอนุญาตหรือปฏิเสธการเข้าใช้งานอุปกรณ์ในคอมพิวเตอร์เครื่องนี้สำหรับกลุ่มผู้ใช้หรือกลุ่มผู้ดูแลระบบ

- ▲ ผู้ดูแลระบบสามารถเข้าใช้งานมุมมองระบบโดยคลิกหรือแตะ **เปลี่ยนแปลง** ป้อนรหัสผ่านผู้ดูแลระบบ จากนั้นเลือกตัวเลือกต่อไปนี้:

- **Device Access Manager**–ในการเปิดหรือปิด HP Device Access Manager ที่มีการรับรองความถูกต้อง ให้คลิกหรือแตะ **เปิด** หรือ **ปิด**
- **ผู้ใช้หรือกลุ่มในเครื่องพีซีนี้**–แสดงกลุ่มผู้ใช้หรือกลุ่มผู้ดูแลระบบที่ได้รับอนุญาตหรือถูกปฏิเสธการเข้าใช้งานประเภทอุปกรณ์ที่ได้เลือกไว้
- **ประเภทอุปกรณ์**–แสดงประเภทอุปกรณ์และอุปกรณ์ที่มีการติดตั้งในระบบหรือที่อาจมีการติดตั้งในระบบก่อนหน้านี้ ในการขยายรายการ ให้คลิกไอคอน **+** อุปกรณ์ทั้งหมดที่เชื่อมต่อกับคอมพิวเตอร์จะแสดงขึ้นมา และกลุ่มผู้ดูแลระบบและผู้ใช้จะถูกขยายออกเพื่อแสดงข้อมูลสมาชิกภาพ ในการรีเฟรชรายการอุปกรณ์ ให้คลิกไอคอนลูกศรกลม (รีเฟรช)
  - โดยปกติแล้วจะมีการป้องกันข้อมูลประเภทอุปกรณ์ หากมีการตั้งค่าการเข้าใช้งานเป็น **อนุญาต** ผู้ใช้หรือกลุ่มที่เลือกจะสามารถเข้าใช้งานอุปกรณ์ใดๆ ในประเภทอุปกรณ์ดังกล่าวได้
  - ยังมีการป้องกันสำหรับอุปกรณ์บางประเภทอีกด้วย
  - ให้กำหนดค่า Just In Time authentication (JITA) ซึ่งจะอนุญาตให้ผู้ใช้ที่เลือกไว้มีการเข้าใช้งานไดรฟ์ DVD/CD-ROM หรือไดรฟ์ดิสก์แบบถอดได้ผ่านการรับรองความถูกต้องด้วยตัวเอง สำหรับข้อมูลเพิ่มเติม โปรดดู การกำหนดค่า JITA ในหน้า 39
  - อนุญาตหรือปฏิเสธการเข้าใช้งานอุปกรณ์ประเภทอื่นๆ เช่น สื่อบันทึกแบบถอดได้ (เช่า เฟรชไดรฟ์ USB), พอร์ตอนุกรมและขนาน, อุปกรณ์ Bluetooth®, อุปกรณ์โมเดม, อุปกรณ์ PCMCIA/ExpressCard, อุปกรณ์ 1394, ตัวอ่านลายนิ้วมือ และ ตัวอ่านสมาร์ทการ์ด หากมีการปฏิเสธการเข้าใช้งานตัวอ่านลายนิ้วมือและตัวอ่านสมาร์ทการ์ด จะสามารถเข้าใช้อุปกรณ์ดังกล่าวด้วยการรับรองความถูกต้องของข้อมูลประจำตัว แต่ไม่สามารถใช้ในระดับนโยบายเซสชันได้

    หมายเหตุ: หากใช้อุปกรณ์ Bluetooth ด้วยการรับรองความถูกต้องของข้อมูลประจำตัว ไม่ควรมีการจำกัดการเข้าใช้งานอุปกรณ์ Bluetooth ในนโยบาย Device Access Manager

  - เมื่อคุณเลือกการตั้งค่าในระดับประเภทกลุ่มหรืออุปกรณ์ และคุณถูกขอให้เลือกว่าจะนำการตั้งค่าดังกล่าวไปใช้กับออบเจ็กต์ลูกหรือไม่:

    ใช่–การตั้งค่าจะแพร่กระจายออกไป

    ไม่–การตั้งค่าจะไม่แพร่กระจายออกไป
  - อุปกรณ์บางประเภท เช่น DVD และ CD-ROM อาจมีการควบคุมเพิ่มเติมโดยการอนุญาตหรือปฏิเสธการเข้าใช้งานที่แยกจากกันสำหรับการดำเนินการอ่านและเขียน

หมายเหตุ: ไม่สามารถเพิ่มกลุ่มผู้ดูแลระบบไปยังรายการผู้ใช้ได้

- **การเข้าใช้งาน**–คลิกหรือแตะลูกศรชี้ลง จากนั้นเลือกประเภทสิทธิ์ต่อไปนี้เพื่ออนุญาตหรือปฏิเสธการเข้าใช้งาน:
  - **อนุญาต - การเข้าใช้งานเต็ม**
  - **อนุญาต - อ่านอย่างเดียว**
  - **อนุญาต - ต้องการ JITA**–สำหรับข้อมูลเพิ่มเติม โปรดดู การกำหนดค่า JITA ในหน้า 39

    หากเลือกการเข้าใช้งานประเภทนี้ ภายใต้ **ระยะเวลา** ให้คลิกหรือแตะลูกศรชี้ลงเพื่อเลือกขอบเขตเวลา
  - **ปฏิเสธ**
- **ระยะเวลา**–คลิกหรือแตะลูกศรชี้ลงเพื่อเลือกขอบเขตเวลาสำหรับการเข้าใช้งานไดรฟ์ CD/DVD-ROM หรือไดรฟ์ดิสก์แบบถอดได้ (โปรดดู การกำหนดค่า JITA ในหน้า 39)

การกำหนดค่า JITA

การกำหนดค่า JITA จะอนุญาตให้ผู้ดูแลระบบสามารถดูหรือแก้ไขรายชื่อผู้ใช้และกลุ่มที่ได้รับอนุญาตให้เข้าใช้งานอุปกรณ์โดยใช้ Just In Time Authentication (JITA)

ผู้ใช้ที่เปิดใช้งาน JITA จะสามารถเข้าใช้งานอุปกรณ์บางอย่างได้ แต่มีข้อจำกัดตามนโยบายที่สร้างไว้ในมุมมอง **การกำหนดค่าประเภทอุปกรณ์**

สามารถอนุญาตให้ใช้งาน JITA เป็นช่วงเวลาตั้งแต่เป็นนาทีหรือไม่จำกัด ผู้ใช้ประเภทไม่จำกัดจะมีการเข้าใช้งานอุปกรณ์นับตั้งแต่เวลาที่ผู้ใช้รับรองความถูกต้องจนกระทั่งเวลาที่ผู้ใช้ออกจากระบบ

หากผู้ใช้ได้รับช่วงเวลา JITA แบบไม่จำกัด หนึ่งนาทีก่อนช่วงเวลา JITA จะหมด ผู้ใช้จะถูกถามว่าต้องการจะขยายเวลาการเข้าใช้งานหรือไม่ เมื่อผู้ใช้ล็อกออฟจากระบบ หรือมีผู้ใช้รายอื่นล็อกอิน ช่วงเวลา JITA จะหมด ครั้งต่อไปที่ผู้ใช้ล็อกล็อกอินและพยายามเข้าใช้งานอุปกรณ์ที่มีการเปิดใช้งาน JITA พร้อมท์สำหรับป้อนข้อมูลประจำตัวจะแสดงขึ้นมา

JITA จะมีให้เลือกใช้งานสำหรบอุปกรณ์ประเภทต่อไปนี้:

- ไดรฟ์ DVD/CD-ROM
- ดิสก์แบบถอดได้

การสร้างนโยบาย JITA สำหรับผู้ใช้และกลุ่ม

ผู้ดูแลระบบสามารถอนุญาตให้ผู้ใช้หรือกลุ่มเข้าใช้งานอุปกรณ์โดยใช้ Just In Time Authentication (JITA)

1. เปิดใช้งาน **Device Access Manager** จากนั้นคลิกหรือแตะ **เปลี่ยนแปลง**
2. เลือกผู้ใช้หรือกลุ่ม จากนั้นภายใต้ **การเข้าใช้งาน** สำหรับ **ดิสก์ไดรฟ์แบบถอดได้** หรือ **ไดรฟ์ DVD/CD-ROM** ให้คลิกหรือแตะลูกศรชี้ลง แล้วเลือก **อนุญาต - ต้องการ JITA**
3. ภายใต้ **ระยะเวลา** ให้คลิกหรือแตะลูกศรชี้ลงเพื่อเลือกระยะเวลาสำหรับการเข้าใช้งาน JITA

ผู้ใช้ต้องล็อกเอาต์และล็อกอินใหม่อีกครั้งเพื่อให้การตั้งค่า JITA ใหม่มีผล

การยกเลิกการใช้งานนโยบาย JITA สำหรับผู้ใช้หรือกลุ่ม

ผู้ดูแลระบบสามารถยกเลิกการเข้าใช้งานอุปกรณ์ต่างๆ ของผู้ใช้หรือกลุ่มโดยใช้ Just In Time Authentication

1. เปิดใช้งาน **Device Access Manager** จากนั้นคลิกหรือแตะ **เปลี่ยนแปลง**
2. เลือกผู้ใช้หรือกลุ่ม จากนั้นภายใต้ **การเข้าใช้งาน** สำหรับ **ดิสก์ไดรฟ์แบบถอดได้** หรือ **ไดรฟ์ DVD/CD-ROM** ให้คลิกหรือแตะลูกศรชี้ลง แล้วเลือก **ปฏิเสธ**

เมื่อผู้ใช้ล็อกอินและพยายามเข้าใช้งานอุปกรณ์ การเข้าใช้งานจะถูกปฏิเสธ

การตั้งค่า

มุมมอง **การตั้งค่า** อนุญาตให้ผู้ดูแลระบบสามารถดูและเปลี่ยนแปลงไดรฟ์ที่การเข้าใช้งานถูกควบคุมโดย Device Access Manager

หมายเหตุ: ต้องเปิดใช้งาน Device Access Manager เมื่อมีการกำหนดค่ารายการตัวอักษรของไดรฟ์ (โปรดดู มุมมองระบบ ในหน้า 38)

ประเภทอุปกรณ์ที่ถูกจัดการ

HP Device Access Manager ไม่สามารถจัดการประเภทอุปกรณ์ต่อไปนี้:

- อุปกรณ์สัญญาณเข้า/ออก
  - ซีดีรอม
  - ดิสก์ไดรฟ์
  - ตัวควบคุมฟลอปปีดิสก์ (FDC)
  - ตัวควบคุมฮาร์ดดิสก์ (HDC)
  - ประเภทอุปกรณ์ที่ติดต่อสื่อสารกับมนุษย์ (HID)
  - อุปกรณ์ที่ติดต่อสื่อสารกับมนุษย์ด้วยระบบอินฟราเรด
  - เมาส์
  - มัลติพอร์ตอนุกรม
  - แป้นพิมพ์
  - เครื่องพิมพ์แบบปลั๊กแอนด์เพลย์ (PnP)
  - เครื่องพิมพ์
  - อัปเกรดเครื่องพิมพ์
- เปิด/ปิด
  - การสนับสนุนการจัดการพลังงานขั้นสูง (APM)
  - แบตเตอรี่
- อื่นๆ
  - Computer
  - ตัวถอดรหัส
  - จอแสดงผล
  - ไดรเวอร์จอแสดงผลแบบครบวงจรจาก Intel®
  - Legacard
  - ไดรฟ์สื่อบันทึก
  - ตัวเปลี่ยนสื่อ
  - เทคโนโลยีหน่วยความจำ
  - จอภาพ
  - มัลติฟังก์ชัน

- Net client
- Net service
- Net trans
- โปรเซสเซอร์
- อะแดปเตอร์ SCSI
- ตัวเร่งความปลอดภัย
- อุปกรณ์รักษาความปลอดภัย
- ระบบ
- ไม่ทราบ
- เสียง
- สแนปช็อตโวลุ่มข้อมูล

8 HP Trust Circles

HP Trust Circles คือโปรแกรมความปลอดภัยของไฟล์และเอกสารที่รวมการเข้ารหัสไฟล์ในโฟลเดอร์พร้อมความสามารถในการแชร์เอกสารได้อย่างสะดวกในกลุ่มที่ไว้วางใจได้ โปรแกรมนี้จะเข้ารหัสไฟล์ที่อยู่ในโฟลเดอร์ที่ผู้ใช้ระบุไว้ ทำให้ไฟล์ถูกป้องกันภายในกลุ่มที่ไว้วางใจ เมื่อได้รับการป้องกันแล้ว ไฟล์ดังกล่าวจะสามารถถูกใช้และแชร์โดยสมาชิกในกลุ่มที่ไว้วางใจได้ หากผู้ที่ไม่ใช่สมาชิกในกลุ่มได้รับไฟล์ถูกป้องกัน ไฟล์ดังกล่าวจะยังคงถูกเข้ารหัสอยู่ และผู้ที่ไม่ใช่สมาชิกในกลุ่มจะไม่สามารถเข้าใช้งานเนื้อหาได้

การเปิด Trust Circles

1. ในหน้าจอเริ่มต้น ให้คลิกหรือแตะแอพ **HP Client Security**

   - หรือ -

   จากเดสก์ท็อป Windows ให้ดับเบิลคลิกไอคอน **HP Client Security** ในพื้นที่แจ้งเตือนที่อยู่ประมาณขวาสุดของแถบงาน

2. ภายใต้ **ข้อมูล** ให้คลิกหรือแตะ **Trust Circles**

การเริ่มต้นใช้งาน

มีสองวิธีในการส่งอีเมลเชิญและตอบกลับ:

- **โดยใช้ Microsoft® Outlook**–การใช้ Trust Circles ที่มี Microsoft Outlook จะเป็นการดำเนินการเชิญและตอบโดย Trust Circle จากผู้ใช้ Trust Circle อื่น
- **โดยใช้ Gmail, Yahoo, Outlook.com หรือบริการอีเมลอื่นๆ (SMTP)**–เมื่อคุณป้อนชื่อ ที่อยู่อีเมล และรหัสผ่าน Trust Circles จะใช้บริการอีเมลของคุณในการส่งอีเมลไปยังสมาชิกที่เลือกเพื่อเชิญเข้าร่วมกลุ่มของคุณ

ในการตั้งค่าโปรไฟล์เบื้องต้น:

1. ป้อนชื่อและที่อยู่อีเมลของคุณ จากนั้นคลิกหรือแตะ **ถัดไป**

   สมาชิกที่ได้รับการเชิญเข้ากลุ่มของคุณจะสามารถเห็นชื่อดังกล่าวได้ ที่อยู่อีเมลจะใช้สำหรับการส่ง รับ หรือตอบกลับการเชิญ

2. ป้อนรหัสผ่านสำหรับบัญชีอีเมล จากนั้นคลิกหรือแตะ **ถัดไป**

   อีเมลทดสอบจะถูกส่งออกไปเพื่อตรวจสอบว่าการตั้งค่าอีเมลถูกต้อง

   หมายเหตุ: คอมพิวเตอร์จะต้องเชื่อมต่อกับเครือข่าย

3. ในฟิลด์ **ชื่อ Trust Circle** ให้ป้อนชื่อสำหรับ trust circle จากนั้นคลิกหรือแตะ **ถัดไป**
4. เพิ่มสมาชิกและโฟลเดอร์ จากนั้นคลิกหรือแตะ **ถัดไป** trust circle จะถูกสร้างขึ้นพร้อมโฟลเดอร์ใดๆ ที่เลือกไว้ และจะส่งอีเมลเชิญไปยังสมาชิกใดๆ ที่เลือกไว้ หากไม่สามารถส่งอีเมลเชิญด้วยเหตุผลใดๆ ก็ตาม การแจ้งเตือนจะแสดงขึ้นมา สามารถเชิญสมาชิกเข้าร่วมกลุ่มได้ทุกเวลาจากมุมมอง Trust Circle โดยคลิก **Trust Circles ของคุณ** จากนั้นดับเบิลคลิกหรือแตะสองครั้งที่ Trust Circles ดังกล่าว สำหรับข้อมูลเพิ่มเติม โปรดดู Trust Circles ในหน้า 43

Trust Circles

คุณสามารถสร้าง trust circle ในช่วงการตั้งค่าเริ่มต้นหลังจากที่คุณป้อนที่อยู่อีเมล หรือในมุมมอง Trust Circle :

▲ จากมุมมอง Trust Circle ให้คลิกหรือแตะ **สร้าง Trust Circle** จากนั้นป้อนชื่อสำหรับ trust circle

- ในการเพิ่มสมาชิกไปยัง trust circle ให้คลิกหรือแตะไอคอน **M+** ข้างๆ **สมาชิก** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ
- ในการเพิ่มโฟลเดอร์ไปยัง trust circle ให้คลิกหรือแตะไอคอน **+** ข้างๆ **โฟลเดอร์** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ

การเพิ่มโฟลเดอร์ไปยัง trust circle

การเพิ่มโฟลเดอร์ไปยัง trust circle ใหม่:

- ในช่วงการสร้าง trust circle คุณสามารถเพิ่มโฟเดอร์โดยคลิกหรือแตะไอคอน **+** ข้างๆ **โฟลเดอร์** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ

  - หรือ -

- ใน Windows Explorer ให้คลิกขวาหรือแตะโฟลเดอร์ที่ปัจจุบันไม่ได้เป็นส่วนหนึ่งของ trust circle ค้างไว้ แล้วเลือก **Trust Circle** จากนั้นเลือก **สร้าง Trust Circle จากโฟลเดอร์**

คำแนะนำ: คุณสามารถเลือกหนึ่งโฟลเดอร์หรือมากกว่านั้นได้

การเพิ่มโฟลเดอร์ไปยัง Trust Circle ที่มีอยู่:

- จากมุมมอง Trust Circle ให้คลิก **Trust Circles ของคุณ**, ดับเบิลคลิกหรือแตะสองครั้งที่ trust circle ที่มีอยู่เพื่อแสดงโฟลเดอร์ปัจจุบัน, คลิกหรือแตะไอคอน **+** ข้างๆ **โฟลเดอร์** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ

  - หรือ -

- ใน Windows Explorer ให้คลิกขวาหรือแตะโฟลเดอร์ที่ปัจจุบันไม่ได้เป็นส่วนหนึ่งของ trust circle ค้างไว้ แล้วเลือก **Trust Circle** จากนั้นเลือก **เพิ่มไปยัง Trust Circle ที่มีอยู่จากโฟลเดอร์**

คำแนะนำ: คุณสามารถเลือกหนึ่งโฟลเดอร์หรือมากกว่านั้นได้

เมื่อเพิ่มโฟลเดอร์ไปยัง trust circle แล้ว Trust Circles ก็จะเข้ารหัสโฟลเดอร์และเนื้อหาของโฟลเดอร์โดยอัตโนมัติ เมื่อไฟล์ทั้งหมดได้รับการเข้ารหัสแล้ว จะมีการแจ้งเตือนแสดงขึ้นมา นอกจากนี้ สัญลักษณ์แม่กุญแจสีเขียวจะแสดงขึ้นมาบนไอคอนโฟลเดอร์และไอคอนไฟล์ที่ได้รับการเข้ารหัสทั้งหมดในโฟลเดอร์ที่ระบุว่าได้รับการป้องกันเต็มรูปแบบ

การเพิ่มสมาชิกไปยัง trust circle

มีสามขั้นตอนที่ต้องทำในการเพิ่มสมาชิกไปยัง trust circle:

1. **เชิญ**–อันดับแรก เจ้าของ trust circle จะต้องเชิญสมาชิก สามารถส่งอีเมลเชิญถึงผู้ใช้หลายคนหรือรายการ/กลุ่มแบบกระจาย
2. **ยอมรับ**–ผู้ได้รับเชิญได้รับอีเมลเชิญและต้องเลือกว่าจะยอมรับหรือปฏิเสธ หากผู้ได้รับเชิญตอบรับการเชิญ อีเมลตอบกลับจะถูกส่งไปยังผู้เชิญ หากได้ส่งการเชิญถึงกลุ่ม สมาชิกแต่ละคนจะได้รับการเชิญและต้องเลือกว่าจะยอมรับหรือปฏิเสธ
3. **ลงทะเบียน**–ผู้เชิญมีโอกาสสุดท้ายในการตัดสินใจว่าจะเพิ่มสมาชิกไปยัง trust circle หรือไม่ หากผู้เชิญตัดสินใจลงทะเบียนสมาชิก ระบบจะส่งอีเมลไปยังผู้ได้รับเชิญเพื่อแจ้งว่าได้รับการตอบรับการเชิญ ผู้เชิญและผู้ได้รับเชิญสามารถเลือกที่จะตรวจสอบความปลอดภัยของกระบวนการเชิญได้ รหัสการตรวจสอบจะแสดงขึ้นมาสำหรับผู้ได้รับเชิญ ซึ่งผู้ได้รับเชิญจะต้องอ่านรหัสดังกล่าวให้กับผู้เชิญฟังผ่านโทรศัพท์ เมื่อรหัสได้รับการตรวจสอบแล้ว ผู้เชิญสามารถส่งอีเมลการลงทะเบียนขั้นสุดท้าย

การเพิ่มสมาชิกไปยัง trust circle ใหม่:

- ในช่วงการสร้าง trust circle คุณสามารถเพิ่มสมาชิกโดยคลิกหรือแตะไอคอน **M+** ข้างๆ **สมาชิก** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ
  - หากคุณกำลังใช้ Outlook ให้เลือกข้อมูลติดต่อจากสมุดที่อยู่ Outlook จากนั้นคลิก **ตกลง**
  - หากคุณกำลังใช้บริการอีเมลอื่นอยู่ ให้เพิ่มที่อยู่อีเมลใหม่ไปยัง Trust Circle ด้วยตัวเอง หรือคุณสามารถเรียกที่อยู่อีเมลที่ได้ลงทะเบียนใน Trust Circle ก็ได้

การเพิ่มสมาชิกไปยัง trust circle ที่มีอยู่:

- จากมุมมอง Trust Circle ให้คลิก **Trust Circles ของคุณ**, ดับเบิลคลิกหรือแตะสองครั้งที่ trust circle ที่มีอยู่เพื่อแสดงสมาชิกปัจจุบัน, คลิกหรือแตะไอคอน **+** ข้างๆ **สมาชิก** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ
  - หากคุณกำลังใช้ Outlook ให้เลือกข้อมูลติดต่อจากสมุดที่อยู่ Outlook จากนั้นคลิก **ตกลง**
  - หากคุณกำลังใช้บริการอีเมลอื่นอยู่ ให้เพิ่มที่อยู่อีเมลใหม่ไปยัง Trust Circle ด้วยตัวเอง หรือคุณสามารถเรียกที่อยู่อีเมลที่ได้ลงทะเบียนใน Trust Circle ก็ได้

การเพิ่มไฟล์ไปยัง trust circle

คุณสามารถเพิ่มไฟล์ไปยัง trust circle ด้วยวิธีการต่อไปนี้:

- คัดลอกหรือย้ายไฟล์ไปยังโฟลเดอร์ trust circle ที่มีอยู่

  - หรือ -

- ใน Windows Explorer ให้คลิกขวาหรือแตะไฟล์ที่ปัจจุบันยังไม่ได้เข้ารหัสค้างไว้ แล้วเลือก **Trust Circle** จากนั้นเลือก **เข้ารหัส** คุณจะได้รับการแจ้งเตือนเพื่อให้เลือกว่าควรเพิ่มไฟล์ใดไปยัง trust circle

คำแนะนำ: คุณสามารถเลือกหนึ่งไฟล์หรือมากกว่านั้น

โฟลเดอร์ที่ถูกเข้ารหัส

สมาชิกใน trust circle สามารถดูและแก้ไขไฟล์ที่เป็นของ trust circle ได้

หมายเหตุ: Trust Circle Manager/Reader ไม่ได้ซิงค์ไฟล์ระหว่างสมาชิก

ไฟล์ต้องได้รับการแชร์ผ่านวิธีการที่มีอยู่ เช่น อีเมล, ftp, หรือผู้ใช้บริการการจัดเก็บข้อมูลแบบ Cloud ไฟล์ที่คัดลอกไปยัง ย้ายไปยัง หรือสร้างภายในโฟลเดอร์ trust circle จะได้รับการป้องกันในทันที

การเอาโฟลเดอร์ออกจาก trust circle

การเอาโฟลเดอร์ออกจาก trust circle จะเป็นการถอดรหัสโฟลเดอร์และเนื้อหาทั้งหมดของโฟลเดอร์ ตลอดจนยังเป็นการเอาการป้องกันออกด้วย

- จากมุมมอง Trust Circle ให้คลิกหรือแตะ **Trust Circles ของคุณ** แล้วดับเบิลคลิกหรือแตะสองครั้งที่ trust circle ที่มีอยู่ เพื่อแสดงโฟลเดอร์ปัจจุบัน จากนั้นคลิกหรือแตะไอคอน **ถังขยะ** ข้างๆ โฟลเดอร์นั้น

  - หรือ -

- ใน Windows Explorer ให้คลิกขวาหรือแตะโฟลเดอร์ที่ปัจจุบันเป็นส่วนหนึ่งของ trust circle ค้างไว้ แล้วเลือก **Trust Circle** จากนั้นเลือก **เอาออกจา trust circle**

คำแนะนำ: คุณสามารถเลือกหนึ่งโฟลเดอร์หรือมากกว่านั้นได้

การเอาไฟล์ออกจาก trust circle

ในการเอาไฟล์ออกจาก trust circle ใน Windows Explorer ให้คลิกขวาหรือแตะไฟล์ที่ปัจจุบันไม่ได้เข้ารหัสค้างไว้ แล้วเลือก **Trust Circle** จากนั้นเลือก **ถอดรหัสไฟล์**

การเอาสมาชิกออกจาก trust circle

สมาชิกที่ได้รับการลงทะเบียนเต็มรูปแบบจะไม่สามารถเอาออกจาก trust circle ได้ วิธีการอื่นที่สามารถทำได้คือ สร้าง trust circle ใหม่ ด้วยสมาชิกอื่นๆ ทั้งหมด ย้ายไฟล์และโฟลเดอร์ทั้งหมดไปยัง trust circle ใหม่ จากนั้นลบ trust circle เดิม ซึ่งจะทำให้แน่ใจได้ว่าไฟล์ใหม่ที่สมาชิกได้รับจะไม่สามารถเข้าถึงได้ แต่สมาชิกใน trust circle เดิมจะยังคงสามารถเข้าถึงอะไรก็ตามที่มีการแชร์ก่อนหน้านี้ได้

หากสมาชิกไม่ได้รับการลงทะเบียนเต็มรูปแบบ (สมาชิกที่ได้รับการเชิญให้เข้าร่วม trust circle หรือไม่ได้ยอมรับการเชิญเข้าร่วม trust circle) คุณสามารถเอาสมาชิกรายดังกล่าวออกจาก trust circle ด้วยวิธีการต่อไปนี้:

- จากมุมมอง Trust Circle ให้คลิกหรือแตะ **Trust Circles ของคุณ** จากนั้นดับเบิลคลิกหรือแตะสองครั้งที่ trust circle เพื่อแสดงรายชื่อสมาชิกปัจจุบัน คลิกหรือแตะไอคอน **ถังขยะ** ข้างๆ ชื่อสมาชิกที่ต้องการเอาออก
- จากมุมมอง Trust Circle ให้คลิกหรือแตะ **สมาชิก** จากนั้นดับเบิลคลิกหรือแตะสองครั้งที่สมาชิกดังกล่าวเพื่อแสดง trust circles ที่สมาชิกอยู่ คลิกหรือแตะไอคอน **ถังขยะ** ถัดจาก trust circle เพื่อเอาสมาชิกดังกล่าวออกจาก trust circle นั้น

การลบ trust circle

ผู้ใช้ต้องเป็นเจ้าของ trust circle จึงจะสามารถลบ trust circle ได้

- จากมุมมอง Trust Circle ให้คลิกหรือแตะ **Trust Circles ของคุณ** จากนั้นคลิกหรือแตะไอคอน **ถังขยะ** ข้างๆ trust circle ที่จะลบ

  ซึ่งจะเป็นการเอา trust circle ออกจากหน้าดังกล่าว และส่งอีเมลถึงสมาชิกทุกคนของ trust circle เพื่อแจ้งให้ทราบว่า trust circle ได้ถูกลบ ไฟล์หรือโฟลเดอร์ใดๆ ที่รวมอยู่ใน trust circle จะถูกเข้ารหัส

การตั้งค่าลักษณะส่วนบุคคล

จากมุมมอง Trust Circle ให้คลิก **ลักษณะส่วนบุคคล** แท็บสามอันจะแสดงขึ้นมา

- **การตั้งค่าอีเมล**

ตัวเลือก	คำอธิบาย
ชื่อผู้ใช้	ชื่อผู้ใช้ที่ปัจจุบันมีการใช้อยู่จะแสดงขึ้นมา ในการเปลี่ยนแปลงชื่อผู้ใช้ ให้ป้อนชื่อผู้ใช้ใหม่ลงในกล่องข้อความ การเปลี่ยนแปลงจะถูกบันทึกโดยอัตโนมัติ
ที่อยู่อีเมล	บัญชีอีเมลที่ใช้อยู่ในปัจจุบันจะแสดงขึ้นมา ในการเปลี่ยนแปลงที่อยู่อีเมล ให้คลิกหรือแตะ **เปลี่ยนการตั้งค่าอีเมล** จากนั้นปฏิบัติตามคำแนะนำบนหน้าจอ
การยืนยันสมาชิกใหม่	เลือกจากตั้งเลือกต่อไปนี้: ◦ **ยืนยันโดยอัตโนมัติ**–หลังจากได้รับการยอมรับจากผู้ได้รับเชิญ ถือว่าเป็นการยืนยันการเข้าร่วม trust circle โดยไม่ต้องป้อนการยืนยันด้วยตัวเอง จากนั้นอีเมลการยืนยันก็ถูกส่งถึงผู้ได้รับเชิญ ◦ **ยืนยันด้วยตัวเอง**–หลังจากได้รับการยอมรับจากผู้ได้รับเชิญ จำเป็นต้องมีการป้อนการยืนยันด้วยตัวเองเพื่อลงทะเบียนสมาชิกใหม่เข้าใน trust circle จากนั้นอีเมลการยืนยันก็ถูกส่งถึงผู้ได้รับเชิญ ◦ **ต้องการการตรวจสอบ**–หลังจากได้รับการยอมรับจากผู้ได้รับเชิญ จำเป็นต้องมีรหัสการตรวจสอบเพื่อลงทะเบียนผู้ได้รับเชิญอย่างเต็มรูปแบบ เจ้าของ trust circle จะต้องติดต่อผู้ได้รับเชิญและขอรหัสการตรวจสอบจากผู้ได้รับเชิญ หลังจากป้อนรหัสที่ถูกต้อง อีเมลการยืนยันก็จะถูกส่งออกไป

ตัวเลือก	คำอธิบาย
การรับรองความถูกต้องเป็นระยะ	สำหรับการรับรองความถูกต้องเป็นระยะ ผู้ใช้จำเป็นต้องป้อนรหัสผ่าน Windows หลังจากหมดเวลาที่ระบุไว้ (บันทึกเป็นนาที) และขณะที่ดำเนินการงานที่สำคัญด้วย การตั้งค่านี้อนุญาตให้ผู้ใช้สามารถเปิดหรือปิดการรับรองความถูกต้องได้
หมดเวลาการรับรองความถูกต้อง	เลือกช่วงหมดเวลาที่ระบุไว้ (บันทึกเป็นนาที) ก่อนที่จะต้องรับรองความถูกต้อง
อย่าแสดงข้อความการยืนยัน	เลือกกล่องกาเครื่องหมายเพื่อยกเลิกการแสดงข้อความการยืนยัน หรือล้างกล่องกาเครื่องหมายเพื่อแสดงข้อความการยืนยัน
ต้องการช่วยปรับปรุง HP Trust Circle โดยการติดตามการใช้งานแบบไม่ระบุตัวตน	เลือกกล่องกาเครื่องหมายเพื่อเข้าร่วมโปรแกรม หรือล้างกล่องกาเครื่องหมายหากคุณไม่ต้องการเข้าร่วม

- **สำรอง/กู้คืนข้อมูล**

ตัวเลือก	คำอธิบาย
การสำรองข้อมูล	คัดลอกข้อมูลโปรแกรม Trust Circle Manager/Reader (การตั้งค่าและ trust circle) ไปยังไฟล์ข้อมูลสำรอง ในกรณีที่เกิดความเสียหายหรือระบบเกิดขัดข้อง คุณสามารถใช้ไฟล์นี้ในการกู้คืนการติดตั้ง Trust Circles ใหม่ไปยังสถานะที่บันทึกบันทึกในไฟล์ **หมายเหตุ:** เฉพาะข้อมูลโปรแกรม Trust Circle ของคุณเท่านั้นที่จะถูกบันทึกไว้ (trust circle, การตั้งค่า และสมาชิก) ไฟล์จริงในโฟลเดอร์ trust circle จะไม่ถูกสำรองข้อมูล ไฟล์ดังกล่าวควรได้รับการสำรองข้อมูลแยกจากกัน ในการสำรองข้อมูลการตั้งค่า Trust Circle และข้อมูลผู้ใช้: 1. คลิกหรือแตะ **สำรองข้อมูล** 2. เลือกชื่อไฟล์และไดเรกทอรีสำหรับไฟล์ข้อมูลสำรอง จากนั้นคลิกหรือแตะ **บันทึก** 3. ป้อนรหัสผ่าน แล้วยืนยัน จากนั้นคลิกหรือแตะ **ตกลง** รหัสผ่านนี้จะมีความจำเป็นเมื่อต้องการกู้คืนไฟล์นี้
การคืนค่า	กู้คืนข้อมูลการตั้งค่าและ trust circles ไฟล์ข้อมูลสำรอง โดยปกติแล้วจะดำเนินการหลังจากที่ระบบเสียหายหรือโยกย้ายไปยังคอมพิวเตอร์เครื่องอื่น ในการกู้คืนข้อมูลการตั้งค่าและข้อมูลผู้ใช้ของ Trust Circle Manager: 1. ให้คลิกหรือแตะ **กู้คืนข้อมูล** 2. นำทางไปยังไดเรกทอรีและชื่อไฟล์ของไฟล์ข้อมูลสำรอง จากนั้นคลิกหรือแตะ **เปิด** 3. ป้อนรหัสผ่านที่ตั้งค่าไว้ขณะทำการสำรองข้อมูล

- **เกี่ยวกับ**–ซอฟต์แวร์ Trust Circle Manager/Reader จะแสดงขึ้นมา ลิงก์จะแสดงขึ้นมาเพื่อช่วยให้คุณสามารถอัปเกรด Trust Circle Manager เป็นเวอร์ชัน Pro หรือเพื่อแสดงข้อความสิทธิ์ส่วนบุคคล HP

9 การกู้คืนในกรณีที่ถูกโจรกรรม (เฉพาะบางรุ่นเท่านั้น)

Computrace (ซื้อแยกต่างหาก) จะช่วยให้คุณตรวจสอบ จัดการ และติดตามคอมพิวเตอร์ของคุณจากระยะไกล

เมื่อเปิดใช้งานแล้ว Computrace จะถูกกำหนดค่าจาก Absolute Software Customer Center จากศูนย์ลูกค้า ผู้ดูแลระบบสามารถตั้งค่า Computrace ให้ตรวจสอบหรือจัดการคอมพิวเตอร์ หากระบบถูกวางผิดที่หรือถูกลักขโมย ศูนย์ลูกค้าก็จะสามารถช่วยหน่วยงานในท้องถิ่นในการค้นหาและกู้คืนคอมพิวเตอร์ หากกำหนดค่าไว้ Computrace จะสามารถทำงานต่อได้แม้ว่าฮาร์ดไดร์ฟจะถูกลบหรือแทนที่แล้วก็ตาม

ในการเรียกใช้งาน computrace:

1. เชื่อมต่อกับอินเทอร์เน็ต
2. เปิด HP Client Security สำหรับข้อมูลเพิ่มเติม โปรดดู การเปิด HP Client Security ในหน้า 7
3. คลิก **การกู้คืนในกรณีที่ถูกโจรกรรม**
4. ในการเปิดใช้งานตัวช่วยสร้างการเปิดใช้งาน Computrace ให้คลิก **เริ่มใช้งาน**
5. ป้อนข้อมูลติดต่อของคุณและข้อมูลบัตรเครดิตของคุณ หรือป้อนคีย์สินค้าที่ซื้อมาก่อน

ตัวช่วยสร้างการเปิดใช้งานจะจัดการธุรกรรมต่าง ๆ อย่างปลอดภัย และตั้งค่าบัญชีผู้ใช้ของคุณบนเว็บไซต์ของ Absolute Software Customer Center เมื่อสำเร็จ คุณจะได้รับอีเมลยืนยันที่มีข้อมูลบัญชีศูนย์ลูกค้าของคุณ

หากคุณเคยใช้ตัวช่วยสร้างการเปิดใช้งาน Computrace และมีบัญชีผู้ใช้สำหรับศูนย์ลูกค้าของคุณอยู่แล้ว คุณสามารถซื้อใบอนุญาตเพิ่มเติมโดยการติดต่อตัวแทนบัญชี HP ของคุณ

ในการล็อกออนเข้าสู่ศูนย์ลูกค้า:

1. ไปที่ https://cc.absolute.com/
2. ในช่อง **ID ล็อกอิน**และ**รหัสผ่าน** โปรดป้อนข้อมูลประจำตัวที่คุณได้รับในอีเมลการยืนยัน และจึงคลิก**ล็อกอิน**

ในการใช้ศูนย์ลูกค้า คุณสามารถ:

- ตรวจสอบคอมพิวเตอร์ของคุณ
- ปกป้องข้อมูลของคุณจากระยะไกล
- รายงานการโจรกรรมคอมพิวเตอร์ที่ได้รับการคุ้มครองโดย Computrace

▲ คลิก **เรียนรู้เพิ่มเติม** สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Computrace

10 ข้อยกเว้นรหัสผ่านเฉพาะที่

การสนับสนุนรหัสผ่านเฉพาะที่จะมีความจำกัดในระดับการรับรองความถูกต้องเมื่อเปิดเครื่องและระดับ HP Drive Encryption สำหรับข้อมูลเพิ่มเติม โปรดดู Windows IMEs ที่ไม่สนับสนุนระดับการรับรองความถูกต้องเมื่อเปิดเครื่องหรือระดับ Drive Encryption ในหน้า 48

สิ่งที่พึงปฏิบัติเมื่อรหัสผ่านถูกปฏิเสธ

ระบบสามารถปฏิเสธรหัสผ่านเนื่องด้วยเหตุผลต่อไปนี้:

- ผู้ใช้กำลังใช้ IME ที่ไม่สนับสนุน เป็นปัญหาปกติที่เกิดขึ้นกับภาษาแบบสองไบต์ (เช่น เกาหลี ญี่ปุ่น จีน) ในการแก้ไขปัญหานี้:
  1. ให้เพิ่มรูปแบบแป้นพิมพ์ที่สนับสนุน (เพิ่มแป้นพิมพ์ สหรัฐฯ/อังกฤษภายใต้ภาษาขาเข้าเป็นภาษาจีน) โดยใช้ **แผงควบคุม**
  2. ตั้งค่าแป้นพิมพ์ที่สนับสนุนเป็นค่าเริ่มต้น
  3. เปิดใช้งาน HP Client Security จากนั้นป้อนรหัสผ่าน Windows
- ผู้ใช้กำหนดใช้ตัวอักขระที่ไม่สนับสนุน ในการแก้ไขปัญหานี้:
  1. ให้เปลี่ยนรหัสผ่าน Windows เพื่อให้ใช้เฉพาะตัวอักขระที่สนับสนุนเท่านั้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับอักขระที่สนับสนุน โปรดดู การจัดการปุ่มพิเศษ ในหน้า 49
  2. เปิดใช้งาน HP Client Security จากนั้นป้อนรหัสผ่าน Windows

Windows IMEs ที่ไม่สนับสนุนระดับการรับรองความถูกต้องเมื่อเปิดเครื่องหรือระดับ Drive Encryption

ใน Windows ผู้ใช้สามารถเลือก IME (ตัวแก้ไขวิธีการป้อนข้อมูล) เพื่อป้อนอักขระและสัญลักษณ์ที่ซับซ้อน เช่น อักขระภาษาญี่ปุ่นหรือจีน โดยใช้แป้นพิมพ์มาตรฐานตะวันตก

ระบบไม่สนับสนุน IMEs ที่ระดับการรับรองความถูกต้องเมื่อเปิดเครื่องและระดับ Drive Encryption ไม่สามารถป้อนรหัสผ่าน Windows ด้วย IME ที่หน้าจอล็อกอินที่มีการรับรองความถูกต้องเมื่อเปิดเครื่องหรือ HP Drive Encryption และการทำเช่นนั้นอาจเป็นผลให้เกิดการล็อกเอาต์ได้ ในบางครั้ง Microsoft® Windows ไม่ได้แสดง IME ขึ้นมาเมื่อผู้ใช้ป้อนรหัสผ่าน

วิธีการแก้ไขก็คือ ให้สลับไปเป็นรูปแบบแป้นพิมพ์ต่อไปนี้ที่สนับสนุนที่จะแปลเป็นรูปแบบแป้นพิมพ์ 00000411:

- Microsoft IME สำหรับภาษาญี่ปุ่น
- รูปแบบแป้นพิมพ์ภาษาญี่ปุ่น
- Office 2007 IME สำหรับภาษาญี่ปุ่น–หาก Microsoft หรือบุคคลอื่นใช้คำว่า IME หรือตัวแก้ไขวิธีการป้อนข้อมูลจริงๆ แล้ววิธีการป้อนข้อมูลอาจไม่ใช่ IME ก็ได้ ซึ่งสามารถทำให้เกิดความสับสน แต่ซอฟต์แวร์จะอ่านรหัสเลขฐานสิบหก ดังนั้น หาก IME แมปไปยังรูปแบบแป้นพิมพ์ที่สนับสนุน HP Client Security ก็จะสามารถสนับสนันการกำหนดค่า

⚠ **คำเตือน!** เมื่อมีการเปิดใช้งาน HP Client Security รหัสผ่านที่ป้อนด้วย Windows IME จะถูกปฏิเสธ

การเปลี่ยนรหัสผ่านโดยใช้รูปแบบแป้นพิมพ์ที่สนับสนุน

หากเริ่มต้นมีการตั้งรหัสผ่านด้วยรูปแบบแป้นพิมพ์หนึ่ง เช่น ภาษาอังกฤษแบบอเมริกัน (409) จากนั้นผู้ใช้เปลี่ยนรหัสผ่านโดยใช้รูปแบบแป้นพิมพ์อื่นที่สนับสนุน เช่น ลาตินอเมริกา (080A) การเปลี่ยนแปลงรหัสผ่านจะได้ผลใน HP Drive Encryption แต่ไม่ได้ผลใน BIOS หากผู้ใช้ใช้อักขระที่ปรากฏในภาษาที่สองแต่ไม่ปรากฏในภาษาแรก (ตัวอย่างเช่น ē)

หมายเหตุ: ผู้ดูแลระบบสามารถแก้ไขปัญหานี้โดยใช้หน้าผู้ใช้ HP Client Security (เข้าใช้งานจากไอคอน **รูปเกียร์** ในหน้าหลัก) เพื่อเอาผู้ใช้ดังกล่าวออกจาก HP Client Security เลือกรูปแบบแป้นพิมพ์ที่ต้องการในระบบปฏิบัติการ จากนั้นดำเนินการตัวช่วยการติดตั้ง HP Client Security อีกครั้งสำหรับผู้ใช้รายเดิม BIOS จะจัดเก็บรูปแบบแป้นพิมพ์ที่ต้องการและรหัสผ่านที่สามารถพิมพ์ด้วยรูปแบบแป้นพิมพ์นี้จะได้รับการตั้งค่าใน BIOS อย่างเหมาะสม

ปัญหาอีกประการที่อาจเป็นไปได้คือ การใช้รูปแบบแป้นพิมพ์ที่แตกต่างออกไปที่สามารถให้อักขระเดียวกัน ตัวอย่างเช่น ทั้งรูปแบบแป้นพิมพ์สหรัฐฯ สากล (20409) และแป้นพิมพ์ลาตินอเมริกา (080A) สามารถให้ตัวอักขระ é แม้ว่าอาจมีลำดับการกดแป้นที่แตกต่างกัน หากเริ่มต้นมีการตั้งรหัสผ่านด้วยรูปแบบแป้นพิมพ์ลาตินอเมริกา แล้วมีการตั้งค่ารูปแบบแป้นพิมพ์ลาตินอเมริกาใน BIOS แม้ว่ารหัสผ่านจะมีการเปลี่ยนแปลงลำดับโดยใช้รูปแบบแป้นพิมพ์สหรัฐฯ สากล

การจัดการปุ่มพิเศษ

- จีน สโลวาเกีย แคนาดา ฝรั่งเศส เช็ก

  เมื่อผู้ใช้เลือกรูปแบบแป้นพิมพ์ก่อนหน้านี้ชุดใดชุดหนึ่ง และจากนั้นจึงป้อนรหัสผ่าน (ตัวอย่างเช่น abcdef) คุณก็สามารถป้อนรหัสผ่านเดียวกันในขณะที่กำลังกดแป้น shift สำหรับตัวอักษรพิมพ์เล็กและแป้น shift และ caps lock สำหรับตัวอักษรพิมพ์ใหญ่ในการรับรองความถูกต้องตอนเปิดเครื่องและ HP Drive Encryption ผู้ใช้ต้องป้อนรหัสผ่านที่เป็นตัวเลขโดยใช้แผงตัวเลข

- เกาหลี

  เมื่อผู้ใช้เลือกรูปแบบแป้นพิมพ์ภาษาเกาหลี และจากนั้นจึงป้อนรหัสผ่าน คุณก็สามารถป้อนรหัสผ่านเดียวกันในขณะที่กำลังกดแป้น altด้านขวาสำหรับตัวอักษรพิมพ์เล็กและแป้น altด้านขวา และ caps lock สำหรับตัวอักษรพิมพ์ใหญ่ในการรับรองความถูกต้องตอนเปิดเครื่องและ HP Drive Encryption

- อักขระที่ไม่สนับสนุนแสดงในตารางต่อไปนี้:

ภาษา	Windows	BIOS	Drive Encryption
อาราบิก	ปุ่ม ﻷ ,ﻹ, และ ﻵ จะให้อักขระสองตัว	ปุ่ม ﻷ ,ﻹ, และ ﻵ จะให้อักขระหนึ่งตัว	ปุ่ม ﻷ ,ﻹ, และ ﻵ จะให้อักขระหนึ่งตัว
ฝรั่งเศสแบบแคนาดา	ç, è, à, และ é พร้อม caps lock คือ Ç, È, À, และ É ใน Windows	ç, è, à, และ é พร้อม caps lock คือ ç, è, à, และ é ในการรับรองความถูกต้องตอนเปิดเครื่อง	ç, è, à, และ é พร้อม caps lock คือ ç, è, à, และ é ใน HP Drive Encryption
สเปน	40a ไม่สนับสนุน แต่สามารถใช้งานสเปนได้เพราะซอฟต์แวร์แปลงสเปนเป็น c0a อย่างไรก็ดี เนื่องจากมีความแตกต่างในข้อปลีกย่อยระหว่างรูปแบบแป้นพิมพ์ต่างๆ ดังนั้นจึงขอแนะนำให้ผู้ใช้ชาวสเปนเปลี่ยนรูปแบบแป้นพิมพ์ Windows เป็น 1040a (สเปนแบบอื่น) หรือ 080a (ลาตินอเมริกา)	ไม่มี	ไม่มี

ภาษา	Windows	BIOS	Drive Encryption
สหรัฐฯ สากล	◦ ปุ่ม ¡, ¤, ‘, ’, ¥, และ × ในแถวบนสุดใช้ไม่ได้ ◦ ปุ่ม å, ®, และ Þ ในแถวที่สองใช้ไม่ได้ ◦ ปุ่ม á, ð, และ ø ในแถวที่สองใช้ไม่ได้ ◦ ปุ่ม æ ในแถวล่างสุดใช้ไม่ได้	ไม่มี	ไม่มี
เช็ก	◦ ปุ่ม ğ ใช้ไม่ได้ ◦ ปุ่ม į ใช้ไม่ได้ ◦ ปุ่ม ų ใช้ไม่ได้ ◦ ปุ่ม ė, ı, และ ż ใช้ไม่ได้ ◦ ปุ่ม ģ, ķ, ļ, ņ, และ ţ ใช้ไม่ได้	ไม่มี	ไม่มี
สโลวาเกีย	ปุ่ม ż ใช้ไม่ได้	◦ ปุ่ม š, ś, และ ş ใช้ไม่ได้เมื่อพิมพ์ แต่ใช้ได้เมื่อป้อนด้วยซอฟต์คีบอร์ด ◦ ปุ่มตาย ţ ให้อักขระสองตัว	ไม่มี
ฮังการี	ปุ่ม ż ใช้ไม่ได้	ปุ่ม ţ ให้อักขระสองตัว	ไม่มี
สโลเวเนีย	ปุ่ม żŻ ใช้ไม่ได้ใน Windows และปุ่ม alt ให้ปุ่มตายใน BIOS	ปุ่ม ú, Ú, ů, Ů, ş, Ş, ś, Ś, š, และ Š ใช้ไม่ได้ใน BIOS	ไม่มี
ญี่ปุ่น	เมื่อมีภาษานี้ให้เลือกใช้งาน ขอแนะให้ให้ใช้ Microsoft Office 2007 IME แม้ว่าจะมีชื่อ IME แต่ในความเป็นจริงเป็นรูปแบบแป้นพิมพ์ 411 ที่สนับสนุน	ไม่มี	ไม่มี

อภิธานศัพท์

Bluetooth
เทคโนโลยีที่ใช้การส่งข้อมูลด้วยคลื่นวิทยุเพื่อเปิดใช้งานคอมพิวเตอร์ เครื่องพิมพ์ เมาส์ โทรศัพท์มือถือ และอุปกรณ์อื่นๆ ที่มีการเปิดใช้งาน Bluetooth สำหรับการสื่อสารแบบไร้สายในระยะสั้นๆ

Drive Encryption
ปกป้องข้อมูลของคุณโดยการเข้ารหัสฮาร์ดไดร์ฟของคุณ โดยทำให้ไม่สามารถอ่านข้อมูลได้โดยไม่ทำการรับรองความถูกต้องที่เหมาะสม

DriveLock
คุณสมบัติการรักษาความปลอดภัยที่เชื่อมต่อกับฮาร์ดไดร์ฟกับผู้ใช้และขอให้ผู้ใช้พิมพ์รหัสผ่าน DriveLock เมื่อคอมพิวเตอร์เปิดเครื่อง

Just In Time Authentication
โปรดดูวิธีใช้ซอฟต์แวร์ HP Device Access Manager

PIN
เลขประจำตัวสำหรับผู้ใช้ที่ได้รับการลงทะเบียน โดยจะใช้เพื่อการรับรองความถูกต้อง

PKI
มาตรฐาน Public Key Infrastructure ที่กำหนดอินเทอร์เฟซสำหรับการสร้าง ใช้งาน และบริหารจัดการใบรับรองและคีย์การเข้ารหัสแบบ cryptographic

Single Sign On
คุณสมบัติที่เก็บข้อมูลการรับรองความปลอดภัยและอนุญาตให้คุณใช้ HP Client Security ในการเข้าถึงอินเทอร์เน็ตและโปรแกรม Windows ที่ต้องรับรองความถูกต้องของรหัสผ่าน

Trust Circle
ให้ที่เก็บข้อมูลโดยผูกข้อมูลดังกล่าวไว้กับกลุ่มผู้ใช้ที่ไว้วางใจได้ ซึ่งจะป้องกันไม่ให้ข้อมูลตกอยู่ในมือของผู้ที่ประพฤติมิชอบโดยบังเอิญหรือตั้งใจก็ตาม ข้อมูลได้รับการรักษาความปลอดภัยด้วยเทคโนโลยี CryptoMill's Zero Overhead Key Management โดยจะมีการผูกไว้กับกลุ่มที่ไว้วางใจได้ด้วยรหัสลับ ซึ่งจะป้องกันการถอดรหัสลับเอกสารหรือข้อมูลที่สำคัญอื่นๆ ด้านนอก trust circle

Trust Circle Manager/Reader
Trust Circle Reader สามารถยอมรับการเชิญที่ส่งออกไปโดยผู้ใช้ Trust Circle Manager เท่านั้น อย่างไรก็ดี Trust Circle Manager จะอนุญาตให้สร้าง trust circles ได้ คุณสมบัติต่างๆ จะรวมถึงการเชิญผู้อื่นเข้าร่วม trust circle ผ่านอีเมลและการยอมรับการเชิญเข้า trust circle จากผู้อื่น เมื่อสร้าง trust circle กับเพื่อนในระดับเดียวกัน ไฟล์ที่ได้รับการป้องกันโดย trust circle จะสามารถแชร์ได้อย่างปลอดภัย

กลุ่ม
กลุ่มผู้ใช้ที่มีการเข้าถึงหรือการปฏิเสธการเข้าถึงประเภทอุปกรณ์หรืออุปกรณ์บางอย่างในระดับเดียวกัน

การกู้คืนข้อมูล HP SpareKey
ความสามารถในการเข้าถึงคอมพิวเตอร์ของคุณโดยการตอบคำถามรักษาความปลอดภัยอย่างถูกต้อง

การคืนค่า
กระบวนการที่จะคัดลอกข้อมูลโปรแกรมจากไฟล์ข้อมูลสำรองที่บันทึกไว้ก่อนหน้านี้ไปยังโปรแกรมนี้

การรับรองความถูกต้อง
กระบวนการตรวจสอบว่าคุณคือบุคคลที่คุณอ้างสิทธิ์ผ่านการใช้ข้อมูลประจำตัว ซึ่งรวมถึงรหัสผ่าน Windows, ลายนิ้วมือ, สมาร์ทการ์ด, การ์ดแบบไร้สัมผัส หรือการ์ดระยะใกล้

การรับรองความถูกต้องก่อนบูตของ Drive Encryption
หน้าจอล็อกอินที่แสดงขึ้นมาก่อนที่ Windows จะเริ่มต้น ผู้ใช้ต้องป้อนชื่อผู้ใช้ Windows และรหัสผ่าน หรือ PIN สมาร์ทการ์ด หรือปัดนิ้วมือที่ลงทะเบียน หากเลือก one-step logon การป้อนข้อมูลที่ถูกต้องที่หน้าจอล็อกอิน Drive Encryption จะทำให้เข้าถึง Windows โดยตรงโดยไม่ต้องล็อกอินอีกครั้งที่หน้าจอล็อกอิน Windows

การรับรองความถูกต้องเมื่อเปิดเครื่อง

คุณสมบัติด้านการรักษาความปลอดภัยที่จำเป็นมีการรับรองความถูกต้องในบางรูปแบบ เช่นสมาร์ทการ์ด ชิพรักษาความปลอดภัย หรือรหัสผ่าน เมื่อคอมพิวเตอร์ถูกเปิดเครื่อง

การลบถาวรโดยอัตโนมัติ
การลบถาวรที่คุณกำหนดเวลาใน File Sanitizer

การล้างพื้นที่ว่าง
การเขียนข้อมูลสุ่มทับสินทรัยพ์ที่ถูกลบและพื้นที่ที่ไม่ได้ใช้งาน กระบวนการนี้จะช่วยลดการปรากฏอยู่ของสินทรัพย์ที่ถูกลบ เพื่อทำให้กู้คืนสินทรัพย์ดั้งเดิมได้ยากยิ่งขึ้น

การสำรองข้อมูล
ใช้คุณสมบัติการสำรองข้อมูลในการบันทึกสำเนาข้อมูลโปรแกรมที่สำคัญไปยังตำแหน่งภายนอกโปรแกรม ซึ่งสามารถใช้สำหรับการกู้คืนข้อมูลของคอมพิวเตอร์เครื่องเดียวกันหรือเครื่องอื่นในภายหลัง

การเข้ารหัสซอฟตแวร์
การใช้ซอฟต์แวร์เพื่อเข้ารหัสฮาร์ดไดรฟ์ทีละเซกเตอร์ กระบวนการนี้จะช้ากว่าการเข้ารหัสฮาร์ดแวร์

การเข้ารหัสลับ
กระบวนการ เช่นขั้นตอนวิธี ที่ใช้ในการเข้ารหัสแบบ cryptography เพื่อแปลงข้อความธรรมดาเป็นข้อความ cipher ในการป้องกันผู้รับที่ไม่ได้รับอนุญาตจากการอ่านข้อมูล มีการเข้ารหัสข้อมูลหลายประเภท และการเข้ารหัสเหล่านี้ก็เป็นพื้นฐานของความปลอดภัยของเครือข่าย ประเภททั่วไปจะรวมถึงการเข้ารหัสข้อมูลมาตรฐานและการเข้ารหัสคีย์สาธารณะ

การเข้ารหัสฮาร์ดแวร์
การใช้ไดรฟ์แบบเข้ารหัสเองที่ตรงกับข้อมูลจำเพาะ OPAL ของ Trusted Computing Group สำหรับการจัดการไดรฟ์แบบเข้ารหัสเองเพื่อทำการเข้ารหัสแบบทันทีให้เสร็จสมบูรณ์ การเข้ารหัสฮาร์ดแวร์จะรวดเร็วและอาจใช้เวลาเพียงไม่กี่นาที แต่การเข้ารหัสซอฟต์แวร์อาจใช้เวลาหลายชั่วโมง

การเปิดใช้งาน
งานที่ต้องดำเนินการให้เสร็จสมบูรณ์ก่อนที่จะสามารถเข้าใช้งานคุณสมบัติต่างๆ ของ Drive Encryption ได้ ผู้ดูแลระบบสามารถเปิดใช้งาน Drive Encryption ด้วยตัวช่วยการติดตั้ง HP Client Security หรือ HP Client Security กระบวนการเปิดใช้งานประกอบด้วยการเปิดใช้งานซอฟต์แวร์ การเข้ารหัสไดรฟ์ และการสร้างคีย์เข้ารหัสสำรองข้อมูลเริ่มต้นในอุปกรณ์จัดเก็บข้อมูลแบบถอดได้

การ์ด ID
แกดเจ็ตของเดสก์ท็อป Windows ที่ทำงานเพื่อระบุเดสก์ท็อปของคุณด้วยรูปภาพและชื่อผู้ใช้และรูปที่เลือกไว้

การ์ดระยะใกล้
การ์ดพลาสติกที่ประกอบด้วยชิปคอมพิวเตอร์ที่สามารถใช้สำหรับการรับรองความถูกต้องร่วมกับข้อมูลประจำตัวอื่นๆ เพื่อเพิ่มความปลอดภัย

การ์ดแบบไร้สัมผัส
การ์ดพลาสติกที่มีชิปคอมพิวเตอร์ที่สามารถใช้สำหรับการรับรองความถูกต้อง

ข้อมูลตัวตน
ใน HP Client Security กลุ่มข้อมูลประจำตัวหรือการตั้งค่าที่ถูกจัดการโดยบัญชีหรือโปรไฟล์สำหรับการใช้งานพิเศษ

ข้อมูลประจำตัว
ส่วนข้อมุลจำเพาะหรืออุปกรณ์ฮาร์ดแวร์ที่ใช้ในการรับรองความถูกต้องผู้ใช้เป็นรายบุคคล

ความปลอดภัยสำหรับการล็อกออน Windows
ปกป้องบัญชี Windows ของคุณโดยการขอให้ใช้ข้อมูลประจำตัวในการเข้าถึง

ชิพรักษาความปลอดภัย Trusted Platform Module (TPM) ในตัว
TPM จะรับรองความถูกต้องให้คอมพิวเตอร์ แทนผู้ใช้ โดยการเก็บข้อมูลเฉพาะไว้ในระบบโฮสต์ เช่นคีย์การเข้ารหัส ใบอนุญาตดิจิตอล และรหัสผ่าน TPM จะลดความเสี่ยงที่ข้อมูลบนคอมพิวเตอร์จะถูกลักขโมยโดยการโจรกรรมทางกายภาพหรือการโจมตีโดยแฮกเกอร์ภายนอก

ถอดรหัส
ขั้นตอนที่ใช้ในการการเข้ารหัสแบบ cryptography เพื่อแปลงข้อมูลที่เข้ารหัสแล้วเป็นข้อความธรรมดา

ทำลาย
การดำเนินการของอัลกอริธึมที่จะเขียนทับข้อมูลที่อยู่ในสินทรัพย์ด้วยข้อมูลที่ไม่มีความหมาย

ทำลายด้วยตัวเอง
การลบถาวรสินทรัยพ์หรือสินทรัพย์ที่เลือกไว้ในทันที ซึ่งเป็นการเลี่ยงการลบถาวรตามกำหนดเวลา

นโยบายควบคุมการเข้าถึงอุปกรณ์
รายการอุปกรณ์ที่ผู้ใช้ได้รับอนุญาตหรือปฏิเสธการเข้าถึง

บัญชีของผู้ใช้ Windows
ผู้ใช้ที่ได้รับอนุญาตให้ล็อกออนเครือข่ายหรือคอมพิวเตอร์บางเครื่อง

บัญชีเครือข่าย
ผู้ใช้ Windows หรือบัญชีผู้ดูแลระบบ ไม่ว่าจะเป็นคอมพิวเตอร์ภายใน ในกลุ่มงาน หรือบนโดเมน

ประเภทอุปกรณ์
ประเภทที่เฉพาะเจาะจงของอุปกรณ์ทั้งหมด เช่น ไดรฟ์

ผู้ดูแลระบบ
โปรดดู*ผู้ดูแลระบบ Windows*

ผู้ดูแลระบบ Windows
ผู้ใช้มีสิทธิ์การใช้งานเต็มในการแก้ไขสิทธิ์การเข้าใช้งานและจัดการผู้ใช้รายอื่น

ผู้ใช้
ผู้ที่ลงทะเบียนใน Drive Encryption ผู้ใช้ที่ไม่ใช่ผู้ดูแลระบบจะมีสิทธิ์ที่จำกัดในการใช้งาน Drive Encryption โดยจะสามารถลงทะเบียน (ด้วยการอนุมัติจากผู้ดูแลระบบ) และล็อกออนได้เท่านั้น

ระบบไฟล์ที่เข้ารหัส (EFS)
ระบบที่เข้ารหัสไฟล์และโฟลเดอร์ย่อยทั้งหมดในโฟลเดอร์ใดโฟลเดอร์หนึ่ง

รีบูต
กระบวนการเปิดเครื่องคอมพิวเตอร์ใหม่

ลายนิ้วมือ
การคัดแยกภาพลายนิ้วมือระบบดิจิตอล HP Client Security จะไม่จัดเก็บภาพลายนิ้วมือจริงของคุณโดยเด็ดขาด

ล็อกออน
ออปเจ็กต์ภายใน HP Client Security ที่ประกอบด้วยชื่อผู้ใช้และรหัสผ่าน (และอาจมีข้อมูลอื่นๆ ที่ได้เลือกไว้) ที่สามารถใช้ในการล็อกออนเว็บไซต์หรือโปรแกรมอื่นๆ

วิธีการล็อกออนแบบปลอดภัย
วิธีการที่ใช้ในการล็อกออนสู่คอมพิวเตอร์

สมาร์ทการ์ด
อุปกรณ์ฮาร์ดแวร์ที่สามารถใช้กับ PIN สำหรับการรับรองความถูกต้อง

สินทรัพย์
ส่วนประกอบข้อมูลที่มีข้อมูลหรือไฟล์ส่วนบุคคล ข้อมูลประวัติหรือข้อมูลที่เกี่ยวข้องกับเว็บ และอื่นๆ ที่อยู่ในฮารด์ไดรฟ์

ส่วนเก็บข้อมูลถาวรสำหรับการกู้คืนฉุกเฉิน
พื้นที่จัดเก็บที่ได้รับการปกป้องที่อนุญาตให้เข้ารหัสคีย์ผู้ใช้พื้นฐานใหม่จากแคีย์เจ้าของแพลตฟอร์มต่าง ๆ

หน้าจอล็อกออนของ Drive Encryption
โปรดดูส่วนการรับรองความถูกต้องก่อนบูตของ Drive Encryption

หน้าหลัก
ตำแหน่งที่ตั้งส่วนกลางที่คุณสามารถเข้าใช้งานและจัดการคุณสมบัติและการตั้งค่าต่างๆ ใน HP Client Security

อุปกรณ์ที่เชื่อมต่ออยู่
อุปกรณ์ฮาร์ดแวร์ที่เชื่อมต่ออยู่กับพอร์ตบนคอมพิวเตอร์

โดเมน
กลุ่มคอมพิวเตอร์ที่เป็นส่วนหนึ่งของเครือข่ายและแบ่งปันไดเรกทอรี่ฐานที่เหมือนกัน โดเมนจะมีชื่อไม่ซ้ำกัน และแต่ละโดเมนก็มีชุดกฎและกระบวนการที่คล้ายกัน

โฟลเดอร์ Trust Circle
โฟลเดอร์ที่ได้รับการป้องกันโดย trust circle

ดัชนี