คู่มือการจัดการเดสก์ทอป
Business PC

คู่มือการจัดการเดสก์ทอป

Business PC

พิมพ์ครั้งที่สาม (กรกฎาคม 2008)

หมายเลขเอกสาร: 451272-283

เกี่ยวกับคู่มือนี้

คู่มือนี้แสดงคำอธิบายและคำแนะนำเกี่ยวกับการใช้คุณสมบัติการรักษาความปลอดภัยและความสามารถในการจัดการซึ่งติดตั้งไว้ในคอมพิวเตอร์บางรุ่น

⚠ **คำเตือน!** ข้อความในลักษณะนี้หมายถึงการไม่ปฏิบัติตามอาจเป็นผลให้เกิดการบาดเจ็บหรือเสียชีวิต

△ **ข้อควรระวัง:** ข้อความในลักษณะนี้หมายถึงการไม่ปฏิบัติตามอาจเป็นผลให้เกิดความเสียหายต่ออุปกรณ์หรือสูญเสียข้อมูล

หมายเหตุ: ข้อความที่ปรากฏในลักษณะนี้หมายถึงข้อมูลเพิ่มเติมที่สำคัญ

สารบัญ

1 ภาพรวมของการจัดการเดสก์ทอป

ระบบ Client Management Solutions ของ HP เป็นโซลูชันมาตรฐานสำหรับการจัดการและควบคุมระบบเดสก์ทอป เวิร์กสเตชัน และคอมพิวเตอร์โน้ตบุ๊กในสภาวะการทำงานในเน็ตเวิร์ก HP เป็นผู้ริเริ่มระบบจัดการเดสก์ทอปในปี 1995 ด้วยการเปิดตัวคอมพิวเตอร์ส่วนบุคคลที่มีระบบการจัดการเดสก์ทอปอย่างเต็มรูปแบบเป็นครั้งแรก โดย HP เป็นเจ้าของสิทธิบัตรสำหรับเทคโนโลยีระบบการจัดการ นับแต่นั้นมา HP ก็ได้กลายเป็นผู้นำในการพัฒนามาตรฐานและโครงสร้างพื้นฐานที่จำเป็นต่อการใช้งาน การตั้งค่า และการจัดการเดสก์ทอป เวิร์กสเตชัน และคอมพิวเตอร์โน้ตบุ๊กอย่างมีประสิทธิภาพ HP ได้พัฒนาซอฟต์แวร์การจัดการของบริษัทเองและร่วมมือกับผู้ให้บริการโซลูชันซอฟต์แวร์ชั้นนำในอุตสาหกรรมอย่างใกล้ชิดเพื่อสร้างความมั่นใจในการใช้งานร่วมกันระหว่าง HP Client Management Solutions และผลิตภัณฑ์เหล่านี้ HP Client Management Solutions จึงเป็นแง่มุมสำคัญของพันธะสัญญาที่เรามีให้กับคุณ ด้วยโซลูชันซึ่งจะช่วยคุณลดค่าใช้จ่ายโดยรวมในการครอบครองและบำรุงรักษาคอมพิวเตอร์ตลอดอายุการใช้งาน

ความสามารถและคุณสมบัติหลักของการจัดการเดสก์ทอป ได้แก่:

- การตั้งค่าเริ่มต้นและการเริ่มใช้งาน
- การติดตั้งระบบระยะไกล
- การอัพเดตและการจัดการซอฟต์แวร์
- การแฟลช ROM
- การกำหนดค่าตัวเลือกฮาร์ดแวร์
- การควบคุมทรัพย์สินและการรักษาความปลอดภัย
- การแจ้งข้อผิดพลาดและการกู้คืน

หมายเหตุ: การสนับสนุนคุณสมบัติต่างๆ ที่กล่าวถึงในคู่มือนี้อาจแตกต่างกันไปในเครื่องคอมพิวเตอร์และซอฟต์แวร์แต่ละรุ่น

2 การตั้งค่าเริ่มต้นและการเริ่มใช้งาน

คอมพิวเตอร์เครื่องนี้มีการติดตั้งอิมเมจของซอฟต์แวร์ระบบไว้แล้ว หลังจากสิ้นสุดกระบวนการ “แยก” ซอฟต์แวร์ที่ใช้เวลาสั้นๆ เครื่องคอมพิวเตอร์ก็จะพร้อมสำหรับการใช้งาน

คุณอาจต้องการแทนที่อิมเมจของซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าด้วยระบบและซอฟต์แวร์ชุดที่กำหนดขึ้นเอง ซึ่งสามารถทำได้หลายวิธี เช่น:

- ติดตั้งซอฟต์แวร์เพิ่มเติมหลังจากที่แยกอิมเมจของซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าแล้ว
- การใช้เครื่องมือในการใช้งานซอฟต์แวร์ เช่น HP Client Automation Standard Edition, HP Client Automation Enterprise Edition (ใช้เทคโนโลยี Radia) หรือ Altiris Deployment Solution แทนซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าพร้อมด้วยภาพซอฟต์แวร์ที่เลือกกำหนดเอง
- ใช้กระบวนการลอกแบบดิสก์เพื่อคัดลอกเนื้อหาของฮาร์ดไดรฟ์หนึ่งไปยังอีกไดรฟ์หนึ่ง

วิธีการเริ่มต้นใช้งานที่ดีที่สุดขึ้นอยู่กับสภาวะและกระบวนการด้านสารสนเทศของคุณ

ระบบ HP Backup and Recovery, การตั้งค่า ROM และฮาร์ดแวร์ ACPI จะให้ความช่วยเหลือในด้านการเรียกคืนซอฟต์แวร์ระบบ การจัดการการตั้งค่า และการแก้ไขปัญหา รวมถึงการจัดการพลังงาน

หมายเหตุ: โปรดดู HP Backup and Recovery Manager ในหน้า 11 สำหรับข้อมูลเกี่ยวกับการสร้างชุดแผ่นดิสก์สำหรับการเรียกคืน

HP Software Agent

โปรแกรมการจัดการที่โซลูชั่น HP Client Automation Standard และ Enterprise Editions ใช้ถูกโหลดไว้ในคอมพิวเตอร์ล่วงหน้าแล้ว เมื่อติดตั้งโปรแกรมดังกล่าว โปรแกรมนี้จะช่วยให้สามารถสื่อสารกับคอนโซลการจัดการของ HP ได้

ในการติดตั้ง HP Software Agent:

1. คลิก **Start**
2. คลิก **All Programs**
3. คลิก **HP Manageability**
4. คลิก **Radia Management Agent Readme**
5. ทบทวนและทำตามคำแนะนำที่รวมอยู่ในไฟล์ Readme เพื่อติดตั้ง HP Software Agent

HP Software Agent คือองค์ประกอบด้านโครงสร้างพื้นฐานที่สำคัญเพื่อช่วยให้โซลูชัน HP Client Automation ทั้งหมดทำงานได้ หากต้องการเรียนรู้เกี่ยวกับองค์ประกอบด้านโครงสร้างพื้นฐานอื่นๆ ที่จำเป็นสำหรับการใช้โซลูชันการจัดการการตั้งค่าของ HP โปรดเยี่ยมชม http://h20229.www2.hp.com/solutions/ascm/index.html

Altiris Deployment Solution Agent

โปรแกรมนี้ถูกโหลดไว้ล่วงหน้าในคอมพิวเตอร์ เมื่อติดตั้งแล้ว จะช่วยให้สามารถสื่อสารกับคอนโซล Deployment Solution ของผู้ดูแลระบบได้

การติดตั้ง Altiris Deployment Solution Agent:

1. คลิก **Start**
2. คลิก **All Programs**
3. สำหรับ Windows Vista ให้คลิก **Install Altiris DAgent** สำหรับ Windows XP ให้คลิก **Install Altiris AClient**
4. ปฏิบัติตามคำแนะนำที่หน้าจอเพื่อตั้งค่าและกำหนดค่าไคลเอนต์ Altiris

โปรแกรมนี้คือองค์ประกอบด้านโครงสร้างพื้นฐานที่สำคัญเพื่อช่วยให้ Altiris Deployment Solution ซึ่งเป็นส่วนหนึ่งของ Altiris Client Management Suite ทำงานได้ หากต้องการเรียนรู้เกี่ยวกับองค์ประกอบด้านโครงสร้างพื้นฐานอื่นๆ ที่จำเป็นสำหรับการใช้ Altiris Client Management Suite โปรดเยี่ยมชม http://www.hp.com/go/easydeploy

3 การติดตั้งระบบระยะไกล

การติดตั้งระบบระยะไกลช่วยให้คุณสามารถเริ่มต้นและติดตั้งระบบโดยใช้ซอฟต์แวร์และข้อมูลการตั้งค่าที่อยู่ในเซิร์ฟเวอร์ของระบบเน็ตเวิร์ก ด้วยการเริ่มต้นสภาวะการดำเนินการก่อนเริ่มต้นระบบจาก (PXE) คุณสมบัติการติดตั้งระบบระยะไกลมักถูกนำมาใช้เป็นเครื่องมือในการติดตั้งระบบและการตั้งค่า และสามารถใช้ในการทำงานต่อไปนี้:

- ฟอร์แมตฮาร์ดไดรฟ์
- เริ่มต้นใช้งานอิมเมจของซอฟต์แวร์ใน PC ตั้งแต่หนึ่งเครื่องขึ้นไป
- อัพเดต BIOS ระบบในแฟลช ROM จากระยะไกล (การแฟลช ROM ระยะไกล ในหน้า 15)
- กำหนดการตั้งค่า BIOS ของระบบ

ในการเริ่มต้นการติดตั้งระบบระยะไกล ให้กด F12 เมื่อข้อความ **F12 = Network Service Boot** ปรากฏตรงมุมล่างขวาของหน้าจอโลโก้ HP เมื่อกำลังบูตเครื่องคอมพิวเตอร์ จากนั้น ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อดำเนินการต่อ ลำดับการบูตที่เป็นค่าดีฟอลต์เป็นการตั้งค่าใน BIOS ที่สามารถเปลี่ยนให้เป็นการบูตจาก PXE ทุกครั้งได้

4 การอัพเดตและการจัดการซอฟต์แวร์

HP มีเครื่องมือหลายอย่างในการจัดการและการอัพเดตซอฟต์แวร์ในเครื่องเดสก์ทอป เวิร์กสเตชัน และโน้ตบุ๊ก

- HP Client Management Interface
- HP SoftPaq Download Manager
- HP System Software Manager
- HP ProtectTools Security Manager
- HP Client Automation Starter, Standard และ Enterprise Editions
- HP Client Manager จาก Symantec
- Altiris Client Management Suite
- HP Client Catalog สำหรับผลิตภัณฑ์ Microsoft System Center & SMS
- HP Backup and Recovery Manager
- เครื่องพีซีที่ใช้แบรนด์ Intel vPro พร้อม Active Management Technology
- Verdiem Surveyor
- HP Proactive Change Notification
- HP Subscriber's Choice

HP Client Management Interface

ไม่ว่าแผนกไอทีของคุณจะใช้เครื่องมือการจัดการระบบใด แต่การบริหารจัดการสินทรัพย์ทั้งในรูปของฮาร์ดแวร์และซอฟต์แวร์ถือเป็นเรื่องสำคัญ เพื่อควบคุมต้นทุนด้านไอที และช่วยให้ธุรกิจของคุณขยายตัวอย่างรวดเร็ว ผู้ดูแลระบบไอทีสามารถเข้าใช้ HP Client Management Interface โดยการเขียนสคริปต์ง่ายๆ และรวมสคริปต์ไปยังโซลูชันการจัดการของตัวเลือก

คอมพิวเตอร์ธุรกิจใหม่ของ HP สามารถผสานเข้ากับสภาพแวดล้อมด้านไอทีที่ผ่านการจัดการของคุณได้อย่างกลมกลืนเมื่อใช้ HP Client Management Interface (HP CMI) HP CMI มาพร้อมกับอินเตอร์เฟซที่ช่วยให้การรวมคอมพิวเตอร์ธุรกิจของ HP เข้ากับเครื่องมือการจัดการระบบอุตสาหกรรมซึ่งกำลังเป็นที่นิยม (รวมถึง Microsoft Systems Management Server, IBM Tivoli Software และ HP Operations) และแอปพลิเคชันการจัดการที่พัฒนาขึ้นเป็นการภายในตามความต้องการเฉพาะเป็นเรื่องง่าย เมื่อใช้ HP CMI ทั้งเครื่องมือและแอปพลิเคชันการจัดการระบบสามารถร้องขอข้อมูลไคลเอนต์เชิงลึก รับข้อมูลสถานะเกี่ยวกับสภาพการณ์ และจัดการการตั้งค่าระบบ BIOS ได้ด้วยการสื่อสารโดยตรงกับคอมพิวเตอร์ไคลเอนต์ ลดความจำเป็นต้องใช้เอเยนต์หรือซอฟต์แวร์การเชื่อมต่อเพื่อทำการรวมระบบ

HP Client Management Interface อิงอยู่กับมาตรฐานอุตสาหกรรมที่ประกอบด้วย Microsoft Windows Management Interface (MS WMI), Web-Based Enterprise Management (WBEM), System Management BIOS (SMBIOS) และ Advanced Configuration and Power Interface (ACPI) HP CMI คือเทคโนโลยีรากฐานที่

นำมาใช้ใน HP Client Management Solutions HP จะให้คุณมีอิสระในการเลือกวิธีการจัดการคอมพิวเตอร์ไคลเอนต์ HP ของคุณเมื่อคุณใช้ HP CMI

HP Client Management Interface ที่นำมาใช้ร่วมกับซอฟต์แวร์การจัดการระบบจะสามารถ:

- ร้องขอข้อมูลไคลเอนต์เชิงลึก เช่น การจับข้อมูลโดยละเอียดเกี่ยวกับโปรเซสเซอร์ ฮาร์ดไดรฟ์ หน่วยความจำ BIOS ไดรเวอร์ รวมถึงข้อมูลของเซ็นเซอร์ เช่น ความเร็วของพัดลม แรงดันไฟฟ้า และอุณหภูมิ)
- รับข้อมูลสถานะเกี่ยวกับสภาพการณ์–ขอรับการแจ้งเตือนฮาร์ดแวร์ไคลเอนต์ในหลายๆ ลักษณะ (เช่น อุณหภูมิสูงเกินไป พัดลมหยุดกลางคัน และการเปลี่ยนแปลงการกำหนดค่าฮาร์ดแวร์) ที่จะส่งมาที่คอนโซลการจัดการระบบแอปพลิเคชัน หรือคอมพิวเตอร์โลคัลไคลเอนต์ การแจ้งเตือนจะส่งตามเวลาจริงเมื่อถูกกระตุ้นจากเหตุการณ์ที่เกิดกับฮาร์ดแวร์
- จัดการการตั้งค่าระบบ BIOS — ใช้ฟังก์ชัน F10 ซึ่งรวมถึงการตั้งค่าและการเปลี่ยนรหัสผ่าน BIOS และจัดลำดับการบูตคอมพิวเตอร์จากคอนโซลการจัดการระบบของคุณบนระบบไคลเอนต์บางระบบหรือทั้งหมดโดยไม่ต้องเข้าไปที่เครื่องไคลเอนต์แต่ละเครื่อง

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ HP Client Management Interface โปรดดูที่ http://www.hp.com/go/hpcmi/

HP SoftPaq Download Manager

HP SoftPaq Download Manager เป็นอินเตอร์เฟซฟรีที่ใช้งานง่ายในการค้นหาและดาวน์โหลดซอฟต์แวร์อัพเดตสำหรับเครื่องพีซีไคลเอนต์ของ HP ในสภาพแวดล้อมของคุณ ด้วยการระบุรุ่น ระบบปฏิบัติการ และภาษาของคุณ คุณก็จะสามารถค้นหา เรียงลำดับ และเลือก Softpaq ที่คุณต้องการ เมื่อต้องการดาวน์โหลด HP SoftPaq Download Manager ให้ไปที่ http://www.hp.com/go/sdm

HP System Software Manager

HP System Software Manager (SSM) เป็นยูทิลิตีฟรีที่จะใช้งานระบบระยะไกลอัตโนมัติของดีไวซ์ไดรเวอร์ และการอัพเดต BIOS สำหรับเครื่องพีซีธุรกิจของ HP ในระบบเน็ตเวิร์ก เมื่อรัน SSM โปรแกรมจะกำหนด (โดยไม่สอบถามผู้ใช้) ระดับการปรับรุ่นของไดรเวอร์ และ BIOS ที่ติดตั้งในระบบไคลเอนต์แบบเน็ตเวิร์กแต่ละเครื่องและเปรียบเทียบผลลัพธ์กับซอฟต์แวร์ระบบ SoftPaqs ที่ผ่านการทดสอบและจัดเก็บไว้ในที่เก็บไฟล์ส่วนกลาง จากนั้น SSM จะอัพเดตซอฟต์แวร์ระบบที่ใช้รุ่นต่ำกว่าในเครื่องพีซีที่ต่อกับเน็ตเวิร์ก เพื่อให้เป็นรุ่นล่าสุดที่มีอยู่ในที่เก็บไฟล์โดยอัตโนมัติ เนื่องจาก SSM ยอมให้กระจายการอัพเดต SoftPaq ไปยังระบบไคลเอนต์ในรุ่นที่ถูกต้องเท่านั้น ผู้ดูแลระบบจึงสามารถใช้ SSM เพื่อทำการอัพเดตซอฟต์แวร์ระบบให้ทันสมัยได้อย่างมั่นใจและมีประสิทธิภาพ

System Software Manager ผนวกรวมกับเครื่องมือแจกจ่ายซอฟต์แวร์ระดับองค์กร เช่น โซลูชัน HP Client Automation, HP Client Manager จาก Symantec และ Microsoft Systems Management Server (SMS) ด้วยการใช้ SSM คุณจะสามารถแจกจ่ายการอัพเดตที่กำหนดขึ้นเองหรือการอัพเดตของบริษัทอื่น ที่มีการรวมไว้เป็นชุดในรูปแบบ SSM-format

คุณสามารถดาวน์โหลด SSM โดยไม่เสียค่าใช้จ่ายโดยเข้าไปที่ http://www.hp.com/go/ssm

หมายเหตุ: ในขณะนี้ SSM ยังไม่ได้สนับสนุนการแฟลช ROM ระยะไกลบนระบบต่างๆ ที่เปิดใช้ Windows Vista BitLocker และใช้หน่วยวัด TPM เพื่อป้องกันคีย์ BitLocker เนื่องจากการกะพริบของ BIOS จะไม่ตรวจสอบความถูกต้องของลายเซ็นที่มีความน่าเชื่อถือที่ BitLocker สร้างขึ้นสำหรับแพลตฟอร์ม ปิดใช้งาน BitLocker ผ่าน Group Policy เพื่อทำให้ BIOS ของระบบกะพริบ

คุณสามารถเปิดใช้งานการสนับสนุน BitLocker โดยที่ไม่มีหน่วยวัด TPM ของ BIOS เพื่อหลีกเลี่ยงการใช้ปุ่ม BitLocker ไม่ได้ HP ขอแนะนำให้คุณเก็บการสำรองข้อมูลที่ปลอดภัยของใบรับรอง BitLocker ในกรณีการกู้คืนฉุกเฉิน

HP ProtectTools Security Manager

ซอฟต์แวร์ HP ProtectTools Security Manager มาพร้อมกับคุณสมบัติด้านความปลอดภัยที่ช่วยป้องกันการล็อกอินเข้าใช้คอมพิวเตอร์ ระบบเครือข่าย และข้อมูลสำคัญ ส่วนฟังก์ชันความปลอดภัยเพิ่มเติมมาพร้อมกับโมดูลซอฟต์แวร์ต่างๆ ต่อไปนี้:

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

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

คุณอาจเลือกติดตั้งซ้ำ โหลดล่วงหน้าโมดูลซอฟต์แวร์ HP ProtectTools หรือโมดูลซอฟต์แวร์ดังกล่าวอาจมีให้พร้อมดาวน์โหลดจากเว็บไซต์ของ HP สำหรับเดสก์ทอป HP Compaq บางรุ่น สามารถเลือกใช้ HP ProtectTools เป็นอุปกรณ์เสริม เยี่ยมชมที่ http://www.hp.com/products/security สำหรับข้อมูลเพิ่มเติม

HP Client Automation Starter และ Standard Editions

HP Client Automation คือโซลูชันการจัดการฮาร์ดแวร์และซอฟต์แวร์สำหรับสภาพแวดล้อมของ Windows Vista, Windows XP และ HP Thin Client ที่นำมาใช้งานได้ง่าย และใช้ประโยชน์ได้อย่างรวดเร็ว ควบคู่กับการจัดเตรียมพื้นฐานที่แข็งแกร่งไว้รองรับความต้องการในอนาคต โซลูชันนี้แบ่งออกเป็นสองเวอร์ชัน:

- เวอร์ชัน Starter Edition คือผลิตภัณฑ์ที่ให้ฟรีเพื่อใช้จัดการเดสก์ทอป HP เครื่องโน้ตบุ๊ก และเวิร์กสเตชัน จัดเตรียมระบบฮาร์ดแวร์และซอฟต์แวร์ การควบคุมระยะไกล การควบคุมการแจ้งเตือนของ HP การอัพเดต HP BIOS และไดรเวอร์ การรวมเข้ากับ HP Proect Tools และการสนับสนุนเพิ่มเติมสำหรับ Intel AMT โซลูชันในเวอร์ชัน Starter Edition ยังสนับสนุนการใช้ประโยชน์และการจัดการ HP Thin Clients
- เวอร์ชัน Standard Edition ที่พร้อมจำหน่าย ได้รวมฟังก์ชันการทำงานทั้งหมดที่อยู่ในเวอร์ชัน Starter Edition เอาไว้และเพิ่มการใช้งานและการผสานประโยชน์จาก Windows ความสามารถในการจัดการโปรแกรมปะแก้ การแจกจ่ายซอฟต์แวร์และระบบวัดการใช้ซอฟต์แวร์

HP Client Automation Starter และ Standard Editions รองรับการโยกย้ายไปสู่ HP Client Automation Enterprise Edition (ที่ใช้กับเทคโนโลยี Radia) สำหรับการจัดการโดยอัตโนมัติเมื่อเกิดการเปลี่ยนแปลงสภาพแวดล้อมด้านไอทีในปริมาณมาก เป็นไปอย่างต่อเนื่องและแตกต่างกัน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโซลูชัน HP Client Automation เยี่ยมชมที่ http://www.hp.com/go/client

HP Client Automation Enterprise Edition

HP Client Automation Enterprise Edition คือโซลูชันที่ขึ้นอยู่กับนโยบายที่ช่วยให้ผู้ดูแลระบบสามารถจัดการ นำมาใช้ ปะแก้ และจัดการซอฟต์แวร์และเนื้อหาอย่างต่อเนื่องข้ามแพลตฟอร์มไคลเอนต์ต่างๆ ด้วย HP Client Automation Enterprise Edition ผู้เชี่ยวชาญด้านไอทีสามารถ:

- ทำให้กระบวนการจัดการวัฏจักรทั้งหมดเกิดขึ้นได้โดยอัตโนมัติตั้งแต่การค้นหา การใช้งานและการจัดการอย่างต่อเนื่องผ่านการรวมและการนำออก
- ใช้งานโดยอัตโนมัติและจัดการซอฟต์แวร์ทั้งชุด (ระบบปฏิบัติการ โปรแกรม โปรแกรมปะแก้ การตั้งค่าและเนื้อหา) เพื่อเข้าสู่สภาวะที่ต้องการได้โดยอัตโนมัติ
- จัดการซอฟต์แวร์บนอุปกรณ์ใดๆ แบบเสมือนจริง รวมถึงเดสก์ทอป พื้นที่ทำงาน และโน้ตบุ๊ก ในโครงสร้างที่แตกต่างกันหรือโครงการเดียวๆ
- จัดการซอฟต์แวร์บนระบบปฏิบัติการส่วนใหญ่

ด้วยการจัดการการตั้งค่าคอนฟิเกอเรชันอย่างต่อเนื่อง ลูกค้าของ HP ได้รายงานให้ทราบถึงการประหยัดต้นทุนด้านไอทีจำนวนมหาศาล เวลาที่เพิ่มขึ้นในการวางตลาดซอฟต์แวร์และเนื้อหา และผลงานและความพึงพอใจที่เพิ่มขึ้นของผู้ใช้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโซลูชัน HP Client Automation เยี่ยมชมที่ http://www.hp.com/go/client

HP Client Manager จาก Symantec

HP Client Manager จาก Symantec ที่พัฒนาร่วมกับ Altiris สามารถนำไปใช้ได้ฟรีกับเครื่องเดสก์ทอป โน้ตบุ๊ก และเวิร์กสเตชันของ HP ทุกรุ่น SSM ได้รับการผนวกรวมไว้ใน HP Client Manager และช่วยให้สามารถทำการติดตาม ตรวจสอบ และจัดการทุกส่วนในฮาร์ดแวร์ของระบบไคลเอนต์ของ HP ได้จากศูนย์กลาง

ใช้ HP Client Manager จาก Symantec เพื่อ:

- ดูข้อมูลฮาร์ดแวร์ที่เป็นประโยชน์ เช่น การตั้งค่า CPU, หน่วยความจำ วิดีโอ และความปลอดภัย
- ตรวจสอบสถานะของระบบเพื่อแก้ไขปัญหาก่อนที่จะเกิดขึ้น
- รับและติดตั้งไดรเวอร์และอัพเดต BIOS ได้โดยอัตโนมัติโดยไม่ต้องไปที่ตัวเครื่องพีซี
- การกำหนดค่า BIOS และการตั้งค่าความปลอดภัยได้จากระยะไกล
- ประมวลผลอัตโนมัติเพื่อการแก้ไขปัญหาฮาร์ดแวร์ได้อย่างรวดเร็ว

การรวมเข้ากับเครื่องมือ HP Instant Support อย่างเหมาะสมจะช่วยลดเวลาการแก้ปัญหาฮาร์ดแวร์

- การวินิจฉัย–รันและดูรายงานแบบระยะไกลบนเครื่องเดสก์ทอป โน้ตบุ๊ก และเวิร์กสเตชันของ HP
- สแกนสภาพการณ์ของระบบ–ตรวจสอบปัญหาฮาร์ดแวร์ที่รู้จักซึ่งบนในฐานที่ติดตั้งของเครื่องไคลเอนต์ของ HP
- พูดคุยทันที–เชื่อมต่อกับฝ่ายสนับสนุนลูกค้าของ HP เพื่อแก้ปัญหาที่ประสบ
- พื้นฐานความรู้ของ HP — เชื่อมต่อไปยังข้อมูลจากผู้เชี่ยวชาญ
- กระบวนการรวบรวมและนำส่ง SoftPaq โดยอัตโนมัติสำหรับการแก้ปัญหาฮาร์ดแวร์อย่างฉับไว
- บ่งชี้ จัดเก็บไว้ในระบบ และเริ่มต้นระบบด้วยชิปความปลอดภัย HP ProtectTools แบบฝังตัว
- ตัวเลือกสำหรับการแจ้งเตือนสภาพการณ์ที่จะแสดงบนระบบไคลเอนต์
- รายงานข้อมูลระบบเบื้องต้นสำหรับเครื่องไคลเอนต์ที่ไม่ใช่ของ HP
- ตั้งค่าและกำหนดค่าชิปรักษาความปลอดภัย TPM
- การสำรองและเรียกคืนข้อมูลของไคลเอนต์กำหนดตารางที่เป็นศูนย์กลาง
- การสนับสนุนเพิ่มเติมสำหรับใช้จัดการ Intel AMT

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ HP Client Manager จาก Symantec เยี่ยมชมที่ http://www.hp.com/go/clientmanager

Altiris Client Management Suite

Altiris Client Management Suite เป็นโซลูชันที่ใช้งานง่ายสำหรับการจัดการซอฟต์แวร์ตลอดอายุการใช้งานบนเดสก์ทอป โน้ตบุ๊ก และเวิร์กสเตชัน Client Management Suite Level 1 ประกอบด้วยผลิตภัณฑ์ Altiris ดังต่อไปนี้:

- Inventory Solution
- Deployment Solution
- Software Delivery Solution
- Patch Management Solution
- Application Metering Solution
- Application Management Solution
- Carbon Copy Solution

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Altiris Client Management Suite เยี่ยมชมที่ http://www.altiris.com/Products/ClientManagementSuite.aspx

HP Client Catalog สำหรับผลิตภัณฑ์ Microsoft System Center & SMS

HP Client Catalog ช่วยให้ผู้เชี่ยวชาญด้านไอทีที่ใช้ผลิตภัณฑ์ของ Microsoft สามารถทำการติดตั้งซอฟต์แวร์อัพเดตของ HP (Softpaqs) ลงในเครื่องพีซีของ HP โดยอัตโนมัติ ไฟล์แคตตาล็อกมีข้อมูลแพลตฟอร์มโดยละเอียดเกี่ยวกับเดสก์ทอป โน้ตบุ๊ก และเวิร์กสเตชันของ HP โดยสามารถใช้ร่วมกับคุณลักษณะข้อมูลระบบที่กำหนดเองและการอัพเดตของผลิตภัณฑ์ Microsoft เพื่อจัดหาไดรเวอร์แบบอัตโนมัติและติดตั้งอัพเดตลงในคอมพิวเตอร์ไคลเอนต์ของ HP

ผลิตภัณฑ์ Microsoft ที่สามารถใช้งานร่วมกับ HP Client Catalog ได้แก่:

- System Center Configuration Manager 2007
- System Center Essentials 2007
- Systems Management Server (SMS) 2003 R2

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ HP Client Catalog for SMS เยี่ยมชมที่ http://h20331.www2.hp.com/Hpsub/cache/486247-0-0-225-121.html

HP Backup and Recovery Manager

HP Backup and Recovery Manager เป็นแอปพลิเคชันที่ใช้ได้ง่าย และมีประโยชน์ที่อนุญาตให้คุณสำรองข้อมูลและเรียกคืนฮาร์ดไดรฟ์หลักบนคอมพิวเตอร์ แอปพลิเคชันที่ทำงานภายใน Windows เพื่อสร้างการสำรองข้อมูลของ Windows แอปพลิเคชันทั้งหมด และไฟล์ข้อมูลทั้งหมด คุณอาจกำหนดเวลาให้เครื่องทำการสำรองข้อมูลให้โดยอัตโนมัติ หรือเลือกทำการสำรองด้วยตัวคุณเอง ไฟล์ที่สำคัญสามารถจัดเก็บแยกต่างหากจากการสำรองข้อมูลปกติ

HP Backup and Recovery Manager ที่ติดตั้งไว้ล่วงหน้าบน Recovery Partition ของฮาร์ดไดรฟ์และอนุญาตให้คุณ:

จุดการกู้คืนและการสำรองไฟล์สามารถทำการคัดลอกลงแผ่นซีดีหรือแผ่นดีวีดี ขณะที่การสำรองข้อมูลทั้งหมดสามารถคัดลอกไปยังเครือข่ายหรือฮาร์ดดิกส์ตัวที่สอง

HP ขอแนะนำให้คุณสร้างชุดแผ่นดิสก์สำหรับการเรียกคืนทันทีหลังจากใช้คอมพิวเตอร์ และกำหนดเวลาสำรองข้อมูลแบบ Recovery Point โดยอัตโนมัติอย่างสม่ำเสมอ

ในการสร้างชุดแผ่นดิสก์สำหรับการเรียกคืน:

1. คลิก **Start** > **HP Backup and Recovery** > **HP Backup and Recovery Manager** เพื่อเปิด Backup and Recovery Wizard และคลิก **Next**
2. เลือก **Create a set of recovery discs (Recommended)** และคลิก **Next**
3. ปฏิบัติตามคำแนะนำในวิซาร์ด

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้ HP Backup and Recovery Manager โปรดดูที่ *คู่มือผู้ใช้ตัวจัดการการสำรองและการเรียกข้อมูลคืน* ด้วยการเลือก **Start** > **HP Backup and Recovery** > **HP Backup and Recovery Manager Manual**

หมายเหตุ: คุณสามารถสั่งซื้อชุดแผ่นดิสก์สำหรับการเรียกคืนได้จาก HP ด้วยการติดต่อฝ่ายบริการสนับสนุนของ HP ทางโทรศัพท์ ไปที่เว็บไซต์ต่อไปนี้ เลือกประเทศ/พื้นที่ของคุณ และคลิกที่ลิงค์ **Technical support after you buy** ใต้หัวข้อ **Call HP** เพื่อรับหมายเลขโทรศัพท์ของฝ่ายบริการสนับสนุนของประเทศ/พื้นที่ของคุณ

http://welcome.hp.com/country/us/en/wwcontact_us.html

เทคโนโลยีการจัดการ

คอมพิวเตอร์รุ่นต่างๆ ประกอบด้วยเทคโนโลยี vPro หรือเทคโนโลยีมาตรฐาน เทคโนโลยีทั้งสองช่วยให้เกิดการค้นหา การแก้ไข และการป้องกันทรัพย์สินของคอมพิวเตอร์ที่อยู่บนระบบเครือข่ายได้ดียิ่งขึ้น เทคโนโลยีทั้งสองช่วยให้คุณสามารถจัดการเครื่องพีซีได้ไม่ว่าระบบจะเปิดอยู่ ปิดไว้หรือระบบปฏิบัติการค้างอยู่

เทคโนโลยีการจัดการมีคุณลักษณะดังต่อไปนี้:

- ข้อมูลระบบฮาร์ดแวร์
- การแจ้งเตือน
- การจัดการพลังงาน–เปิด/ปิดเครื่อง วงจรของพลังงาน
- การวินิจฉัยและการซ่อมแซมระยะไกล
  - Serial-over-LAN — อนุญาตให้ควบคุมคอนโซลของเครื่องพีซีจากระยะไกลระหว่างขั้นตอนการบูต
  - IDE-Redirect — อนุญาตให้บูตระบบจากบูตไดรฟ์ระยะไกล ดิสก์ หรือภาพ ISO
- การแยกและการกู้คืนบนฮาร์ดแวร์–จำกัดหรือตัดการเข้าสู่ระบบเครือข่ายของเครื่องพีซี หากตรวจพบกิจกรรมที่น่าจะเป็นไวรัส

หมายเหตุ: สำหรับภาพรวมของเทคโนโลยี Intel vPro เยี่ยมชมที่ http://www.intel.com/vpro

สำหรับข้อมูลเฉพาะของ HP เกี่ยวกับเทคโนโลยี Intel vPro โปรดดูรายงานที่ http://www.hp.com/support เลือกประเทศ/พื้นที่และภาษาของคุณ เลือก **โปรดดูที่ข้อมูลการสนับสนุนและการแก้ไขปัญหา** ป้อนหมายเลขรุ่นของคอมพิวเตอร์ และกด Enter ในหมวดหมู่ **ทรัพยากร** ให้คลิก **คู่มือ (คู่มือ ส่วนเสริม ส่วนแนบท้าย อื่นๆ)** ภายใต้ **Quick jump to manuals by category** ให้คลิก **White papers**

เทคโนโลยีการจัดการที่ใช้ได้มีดังนี้:

- AMT (ประกอบด้วย DASH 1.0)
- ASF

ASF และ AMT อาจไม่ได้รับการกำหนดค่าในเวลาเดียวกัน แต่สามารถใช้ร่วมกับเทคโนโลยีทั้งสองได้

ในการกำหนดค่าระบบ Intel vPro สำหรับ AMT หรือ ASF:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Microsoft Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ Ctrl+P ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ

หมายเหตุ: หากคุณไม่ได้กด Ctrl+P ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด Ctrl+P ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

ฮ็อตคีย์นี้จะเข้าสู่ยูทิลิตีการตั้งค่า Intel Management Engine BIOS Execution (MEBx) ยูทิลิตีนี้จะช่วยให้ผู้ใช้กำหนดค่าลักษณะต่างๆ ของเทคโนโลยีการจัดการ ตัวเลือกการกำหนดค่าบางตัวเลือกมีดังนี้:

- เมนูหลัก
  - การกำหนดค่า Intel ® ME
  - การกำหนดค่า Intel ® AMT
  - เปลี่ยนรหัสผ่าน Intel ® ME
  - จบการทำงาน
- การกำหนดค่าแพลตฟอร์ม Intel ® ME
  - การควบคุมสถานะ Intel ® ME (ใช้/ไม่ใช้)
  - การอัพเดตเฟิร์มแวร์ Intel ® ME แบบโลคัล (ใช้/ไม่ใช้)
  - การควบคุมคุณสมบัติ Intel ® ME
  - การควบคุมพลังงาน Intel ® ME
- การกำหนดค่า Intel ® AMT
  - ชื่อโฮสต์
  - TCP/IP
  - กำหนดรุ่น (องค์กร, SMB)
  - การติดตั้งและการกำหนดค่า
  - ยกเลิกการกำหนด
  - SOL/IDE-R (ใช้/ไม่ใช้)
  - นโยบายรหัสผ่าน
  - การอัพเดตเฟิร์มแวร์ที่ปลอดภัย (ใช้/ไม่ใช้)
  - ตั้งค่า PRTC
  - หมดเวลา Idle
- เปลี่ยนรหัสผ่าน Intel ® ME (HP ขอแนะนำให้เปลี่ยนรหัสผ่านนี้ รหัสผ่านที่เป็นค่าเริ่มต้นคือ **admin**)

เพื่อการจัดการระบบ AMT จากระยะไกล ผู้ดูแลระบบต้องใช้คอนโซลระยะไกลที่สนับสนุน AMT คอนโซลการจัดการองค์กรจากบริษัทต่างๆ เช่น HP, Altiris และ Microsoft SMS มีวางจำหน่ายแล้ว ในโหมด SMB เครื่องไคลเอนต์จะเป็นส่วนในการเข้าสู่คุณสมบัตินี้ ให้เปิดเบราเซอร์จากระบบอื่นที่อยู่บนเครือข่าย และป้อน `http://host_name:16992` โดยที่ `host_name` คือชื่อที่ตั้งให้กับระบบ หรือเลือกใช้แอดเดรส IP แทนชื่อโฮสต์

Verdiem Surveyor

Verdiem Surveyor เป็นโซลูชันซอฟต์แวร์ที่ช่วยจัดการค่าใช้จ่ายด้านพลังงานสำหรับพีซี Surveyor ทำหน้าที่ตรวจวัดและรายงานปริมาณพลังงานที่พีซีแต่ละเครื่องใช้ นอกจากนี้ยังควบคุมการตั้งค่าพลังงานสำหรับพีซี โดยทำให้ผู้ดูแลระบบสามารถปรับใช้กลยุทธ์การประหยัดพลังงานทั่วทั้งเครือข่ายได้อย่างง่ายดาย คุณสามารถดาวน์โหลด HP SoftPaq ที่ประกอบด้วยโปรแกรม Surveyor ได้จากไซต์ HP Support และติดตั้งไว้บนเดสก์ทอปเพื่อธุรกิจรุ่นที่รองรับ คุณสามารถซื้อใบอนุญาตใช้ Surveyor สำหรับการจัดการพีซีได้จากตัวแทนของ HP

HP Proactive Change Notification

โปรแกรม Proactive Change Notification จะใช้เว็บไซต์ Subscriber's Choice เพื่อทำการแจ้งเตือนอย่างทันท่วงทีโดยอัตโนมัติ โดยการ:

- ส่งอีเมลแจ้งเตือนการเปลี่ยนแปลงในทันที (PCN) ให้คุณทราบถึงการเปลี่ยนแปลงของฮาร์ดแวร์และซอฟต์แวร์สำหรับคอมพิวเตอร์และเซิร์ฟเวอร์ส่วนใหญ่ที่ใช้ในธุรกิจ โดยสามารถตั้งระยะเวลาล่วงหน้าได้ 60 วัน
- ส่งอีเมลเกี่ยวกับข่าวสารสำหรับลูกค้า คำแนะนำสำหรับลูกค้า ประกาศสำหรับลูกค้า ข่าวสารด้านความปลอดภัย และการเตือนเกี่ยวกับไดรเวอร์ สำหรับคอมพิวเตอร์และเซิร์ฟเวอร์ส่วนใหญ่ที่ใช้ในธุรกิจ

คุณจะเป็นผู้กำหนดโปรไฟล์ของตัวเอง เพื่อให้แน่ใจได้ว่าจะได้รับเฉพาะข้อมูลที่เกี่ยวข้องกับสภาพแวดล้อมไอทีที่ระบุเท่านั้น สำหรับข้อมูลเพิ่มเติมเกี่ยวกับโปรแกรม Proactive Change Notification และการสร้างโปรไฟล์ส่วนตัว โปรดเยี่ยมชมที่ http://h30046.www3.hp.com/subhub.php

Subscriber’s Choice

Subscriber’s Choice เป็นบริการสำหรับไคลเอนต์จาก HP

จากโปรไฟล์ส่วนตัวของคุณ HP จะนำเสนอคำแนะนำเฉพาะเกี่ยวกับผลิตภัณฑ์ บทความ และ/หรือการแจ้งเตือนเกี่ยวกับไดรเวอร์และการสนับสนุน

โดยบริการแจ้งเตือนเกี่ยวกับไดรเวอร์และบริการสนับสนุนจะส่งอีเมลแจ้งให้คุณทราบว่ามีข้อมูลที่คุณได้สมัครสมาชิกไว้ในโปรไฟล์ส่วนตัวของคุณ ซึ่งคุณจะสามารถอ่านและเรียกดูได้ตามต้องการ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ Subscribers Choice และการสร้างโปรไฟล์ส่วนตัว โปรดเยี่ยมชมที่ http://h30046.www3.hp.com/subhub.php

โซลูชันที่เลิกใช้

แพคเกจซอฟต์แวร์สองแพคเกจ อันได้แก่ Altiris Local Recovery และ Dantz Retrospect จะไม่มีวางจำหน่ายบนเครื่องเดสก์ทอป เครื่องโน้ตบุ๊ก หรือเวิร์กสเตชันทางธุรกิจของ HP อีกต่อไป สำหรับเครื่องเดสก์ทอป โน้ตบุ๊ก และเวิร์กสเตชันทางธุรกิจใหม่ๆ ที่เปิดตัวในปี 2006 เครื่องเหล่านี้จะจัดส่งพร้อมกับ HP Backup and Recovery Manager

5 การแฟลช ROM

BIOS ของคอมพิวเตอร์ได้รับการจัดเก็บไว้ในหน่วยความจำ ROM (read only memory) แบบแฟลช ที่สามารถโปรแกรมได้ เมื่อคุณกำหนดรหัสผ่านสำหรับการตั้งค่าในยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) คุณสามารถป้องกัน ROM จากการอัพเดตหรือแทนที่โดยไม่ได้ตั้งใจได้ ซึ่งเป็นสิ่งสำคัญในการทำงานที่สมบูรณ์ของเครื่องคอมพิวเตอร์ หากคุณจำเป็นหรือต้องการอัพเกรด BIOS คุณสามารถดาวน์โหลดอิมเมจ BIOS ล่าสุดได้จากหน้าบริการสนับสนุนและไดรเวอร์ของ HP ที่ http://www.hp.com/support/files

△ **ข้อควรระวัง:** เพื่อการป้องกัน ROM ในระดับสูงสุด โปรดตรวจสอบว่าคุณได้กำหนดรหัสผ่านสำหรับการตั้งค่าไว้ ซึ่งรหัสผ่านนี้จะป้องกันการอัพเกรด ROM โดยไม่ได้รับอนุญาต System Software Manager จะอนุญาตให้ผู้ดูแลระบบทำหน้าที่กำหนดรหัสผ่านสำหรับการตั้งค่าในเครื่องคอมพิวเตอร์หนึ่งเครื่องขึ้นไปได้พร้อมๆ กัน สำหรับข้อมูลเพิ่มเติม เยี่ยมชมที่ http://www.hp.com/go/ssm

การแฟลช ROM ระยะไกล

การแฟลช ROM ระยะไกลจะช่วยให้ผู้ดูแลระบบสามารถอัพเกรด BIOS ในเครื่องคอมพิวเตอร์HP จากระยะไกลได้อย่างปลอดภัย โดยตรงจากศูนย์จัดการเน็ตเวิร์กส่วนกลาง การที่ผู้ดูแลระบบสามารถทำงานนี้จากทางไกลกับคอมพิวเตอร์หลายเครื่อง จะช่วยให้การใช้งานเป็นไปอย่างเสมอต้นเสมอปลาย และเพิ่มขีดความสามารถในการควบคุมอิมเมจ HP PC BIOS ผ่านเน็ตเวิร์ก นอกจากนี้ยังส่งผลให้ประสิทธิภาพการทำงานสูงขึ้น และลดค่าใช้จ่ายในการดูแลรักษาอุปกรณ์อีกด้วย

หมายเหตุ: ในขณะนี้ SSM ยังไม่ได้สนับสนุนการแฟลช ROM ระยะไกลบนระบบต่างๆ ที่เปิดใช้ Windows Vista BitLocker และใช้หน่วยวัด TPM เพื่อป้องกันคีย์ BitLocker เนื่องจากการกะพริบของ BIOS จะไม่ตรวจสอบความถูกต้องของลายเซ็นที่มีความน่าเชื่อถือที่ BitLocker สร้างขึ้นสำหรับแพลตฟอร์ม ปิดใช้งาน BitLocker ผ่าน Group Policy เพื่อทำให้ BIOS ของระบบกะพริบ

เครื่องคอมพิวเตอร์จะต้องเปิด หรือเปิดระบบจากระยะไกล เพื่อที่จะใช้คุณสมบัติ Remote ROM Flash ได้

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการแฟลช ROM ระยะไกล โปรดดูที่ HP Client Manager Software หรือ System Software Manager ที่ http://www.hp.com/go/ssm/

HPQFlash

ยูทิลิตี HPQFlash ใช้เพื่ออัพเดตหรือเรียกคืน BIOS ของระบบภายในบนเครื่องคอมพิวเตอร์แต่ละเครื่อง จากทางระบบปฏิบัติการ Windows

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับ HPQFlash โปรดเยี่ยมชมที่ http://www.hp.com/support/files แล้วใส่หมายเลขรุ่นของคอมพิวเตอร์เมื่อได้รับแจ้ง

6 โหมดกู้คืนฉุกเฉินบล็อคการบูต

โหมดกู้คืนฉุกเฉินบล็อคการบูตช่วยให้สามารถกู้คืนระบบในกรณีที่การแฟลช ROM ล้มเหลว ซึ่งยากที่จะเกิดขึ้น ตัวอย่างเช่น หากเกิดไฟดับระหว่างการอัพเกรด BIOS จะทำให้การแฟลช ROM ไม่สมบูรณ์ ซึ่งส่งผลให้ไม่สามารถใช้งาน BIOS ของระบบได้ บล็อคการบูตนี้เป็นส่วนที่ได้รับการป้องกันการแฟลชใน ROM ซึ่งประกอบด้วยรหัสที่จะตรวจสอบอิมเมจ BIOS ของระบบที่ถูกต้องเมื่อเปิดเครื่อง

- หากอิมเมจของ BIOS ระบบถูกต้อง ระบบจะเริ่มต้นตามปกติ
- หากภาพ BIOS ของระบบไม่ถูกต้อง Boot Block BIOS ที่บันทึกไม่สำเร็จจะให้การสนับสนุนที่เพียงพอสำหรับการค้นหาสื่อแบบเคลื่อนย้ายได้ของไฟล์อิมเมจ BIOS หากพบไฟล์อิมเมจของ BIOS ที่ถูกต้อง จะทำการแฟลชเข้าสู่ ROM โดยอัตโนมัติ

เมื่อตรวจพบ BIOS ระบบที่ไม่ถูกต้อง ไฟ LED ของเพาเวอร์ระบบจะกะพริบ 8 ครั้ง หนึ่งครั้งทุกๆ วินาที ในเวลาเดียวกันลำโพงจะส่งเสียงดัง 8 ครั้ง หากบางส่วนของ ROM ระบบ ที่บรรจุอิมเมจตัวเลือกการแสดงผลของ ROM ไม่ได้รับความเสียหาย ข้อความ **Boot Block Emergency Recovery Mode** จะแสดงขึ้นที่หน้าจอ

ในการเรียกข้อมูลระบบกลับคืนหลังจากที่เข้าสู่โหมดเรียกคืนฉุกเฉินบล็อคการบูต ให้ดำเนินการตามขั้นตอนต่อไปนี้:

1. ปิดเครื่องคอมพิวเตอร์
2. ใส่แผ่นซีดีหรืออุปกรณ์การแฟลช USB ที่มีไฟล์อิมเมจของ BIOS ที่ต้องการในไดเรกทอรี่ราก

   หมายเหตุ: อุปกรณ์สื่อนี้ต้องได้รับการฟอร์แมตในแบบระบบไฟล์ FAT12, FAT16 หรือ FAT32
3. เปิดเครื่องคอมพิวเตอร์

   หากไม่พบอิมเมจ BIOS ที่เหมาะสม คุณจะได้รับแจ้งให้ใส่สื่อที่มีไฟล์อิมเมจ BIOS

   หากระบบสามารถตั้งโปรแกรม ROM อีกครั้งเป็นผลสำเร็จ ระบบจะปิดตัวลงโดยอัตโนมัติ
4. ให้ถอดอุปกรณ์สื่อที่ถอดออกได้ ซึ่งใช้อัพเกรด BIOS นั้นออกจากเครื่อง
5. เปิดเครื่องเพื่อเริ่มการทำงานของคอมพิวเตอร์

หมายเหตุ: BitLocker ป้องกันไม่ให้ Windows Vista บูตเมื่อแผ่นซีดีที่มีไฟล์อิมเมจ BIOS อยู่ในไดรฟ์ออปติคัล หากเปิดใช้งาน BitLocker ให้นำแผ่นซีดีนี้ออกก่อนพยายามบูต Windows Vista

7 การจำลองการตั้งค่า

ขั้นตอนต่อไปนี้ช่วยให้ผู้ดูแลระบบสามารถคัดลอกการตั้งค่าของเครื่องคอมพิวเตอร์ไปยังคอมพิวเตอร์เครื่องอื่นซึ่งเป็นรุ่นเดียวกันได้อย่างง่ายดาย ซึ่งทำให้การตั้งค่าในระบบคอมพิวเตอร์หลายเครื่องเป็นไปอย่างรวดเร็วและสอดคล้องกันมากขึ้น

หมายเหตุ: ขั้นตอนทั้งสองนี้ต้องใช้ดิสเก็ตต์ไดรฟ์ หรือแฟลชไดรฟ์ USB ที่สนับสนุน

การคัดลอกไปยังคอมพิวเตอร์เครื่องเดียว

△ **ข้อควรระวัง:** การกำหนดการตั้งค่าจะเป็นไปตามรุ่นที่ระบุ อาจเกิดความเสียหายกับไฟล์ระบบได้หากคอมพิวเตอร์ต้นทางและปลายทางไม่ใช่รุ่นเดียวกัน ตัวอย่างเช่น อย่าคัดลอกการกำหนดการตั้งค่าจากพีซีรุ่น dc7xxx ไปใช้กับพีซีรุ่น dx7xxx

1. เลือกรูปแบบการตั้งค่าที่ต้องการคัดลอก ปิดเครื่องคอมพิวเตอร์ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Shut Down**
2. หากคุณกำลังใช้อุปกรณ์สื่อสำหรับการแฟลชทาง USB ให้ใส่อุปกรณ์ดังกล่าวในตอนนี้
3. เปิดเครื่องคอมพิวเตอร์
4. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

   หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี
5. หากคุณกำลังใช้ดิสเก็ตต์ ให้ใส่แผ่นในตอนนี้
6. คลิก **File** > **Replicated Setup** > **Save to Removable Media** ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อสร้างแผ่นดิสก์สำหรับการตั้งค่าหรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB
7. ปิดเครื่องที่จะทำการตั้งค่า และใส่แผ่นดิสก์หรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB เพื่อใช้ในการตั้งค่า
8. เปิดคอมพิวเตอร์เครื่องที่จะตั้งค่า
9. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น
10. คลิก **File** > **Replicated Setup** > **Restore from Removable Media** และทำตามคำแนะนำที่ปรากฏบนหน้าจอ
11. เริ่มต้นการทำงานของคอมพิวเตอร์อีกครั้งหลังจากการตั้งค่าเสร็จสมบูรณ์

การคัดลอกไปยังคอมพิวเตอร์หลายเครื่อง

△ **ข้อควรระวัง:** การกำหนดการตั้งค่าจะเป็นไปตามรุ่นที่ระบุ อาจเกิดความเสียหายกับไฟล์ระบบได้หากคอมพิวเตอร์ต้นทางและปลายทางไม่ใช่รุ่นเดียวกัน ตัวอย่างเช่น อย่าคัดลอกการกำหนดการตั้งค่าจากพีซีรุ่น dc7xxx ไปใช้กับพีซีรุ่น dx7xxx

วิธีการนี้จะใช้เวลาเตรียมแผ่นดิสก์หรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB เพื่อใช้ในการตั้งค่า นานกว่าเล็กน้อย แต่การคัดลอกการตั้งค่าไปยังคอมพิวเตอร์เป้าหมายจะเร็วกว่าอย่างเห็นได้ชัด

หมายเหตุ: ขั้นตอนนี้จำเป็นต้องมีแผ่นดิสก์ที่ใช้บูต หรือต้องสร้างอุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่ใช้บูตได้ หากไม่มี Windows XP สำหรับใช้ในการสร้างแผ่นดิสก์ที่ใช้บูตได้ ให้ใช้วิธีการคัดลอกไปยังคอมพิวเตอร์เครื่องเดียวแทน (โปรดดู การคัดลอกไปยังคอมพิวเตอร์เครื่องเดียว ในหน้า 17)

1. การสร้างแผ่นดิสก์ที่ใช้บูต หรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB โปรดดู อุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่สนับสนุน ในหน้า 18 หรือ อุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่ไม่สนับสนุน ในหน้า 20

   △ **ข้อควรระวัง:** คอมพิวเตอร์บางเครื่องจะไม่สามารถบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ได้ หากค่าดีฟอลต์ของลำดับการบูตในยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) แสดงอุปกรณ์ USB ไว้ก่อนหน้าฮาร์ดไดรฟ์ คอมพิวเตอร์เครื่องนั้นจะสามารถบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ได้ มิเช่นก็ต้องใช้ดิสเก็ตต์ที่ใช้บูตได้

2. เลือกรูปแบบการตั้งค่าที่ต้องการคัดลอก ปิดเครื่องคอมพิวเตอร์ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Shut Down**
3. หากคุณกำลังใช้อุปกรณ์สื่อสำหรับการแฟลชทาง USB ให้ใส่อุปกรณ์ดังกล่าวในตอนนี้
4. เปิดเครื่องคอมพิวเตอร์
5. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

   หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

6. หากคุณกำลังใช้ดิสเก็ตต์ ให้ใส่แผ่นในตอนนี้
7. คลิก **File** > **Replicated Setup** > **Save to Removable Media** ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อสร้างแผ่นดิสก์สำหรับการตั้งค่าหรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB
8. ดาวน์โหลดยูทิลิตี BIOS สำหรับตั้งค่าการจำลอง (repset.exe) และคัดลอกไฟล์นี้ไปยังแผ่นดิสก์สำหรับการตั้งค่าหรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB หากต้องการยูทิลิตีนี้ โปรดไปที่ http://welcome.hp.com/country/us/en/support.html และป้อนหมายเลขรุ่นของคอมพิวเตอร์
9. ในแผ่นดิสก์สำหรับการตั้งค่า หรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB ให้สร้างไฟล์ autoexec.bat โดยใส่คำสั่งต่อไปนี้:

   ```
   repset.exe
   ```

10. ปิดคอมพิวเตอร์เครื่องที่ต้องการตั้งค่า ใส่แผ่นดิสก์สำหรับการตั้งค่า หรืออุปกรณ์สื่อสำหรับการแฟลชทาง USB แล้วเปิดเครื่อง ยูทิลิตีการตั้งค่าจะรันโดยอัตโนมัติ
11. เริ่มต้นการทำงานของคอมพิวเตอร์อีกครั้งหลังจากการตั้งค่าเสร็จสมบูรณ์

การสร้างอุปกรณ์ที่ใช้บูต

อุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่สนับสนุน

อุปกรณ์ที่สนับสนุนจะมีอิมเมจที่ติดตั้งไว้แล้วล่วงหน้า เพื่อให้ขั้นตอนการสร้างอุปกรณ์ที่ใช้บูตได้ทำได้อย่างง่ายดาย เครื่อง HP หรือ Compaq ทั้งหมด และอุปกรณ์สื่อสำหรับแฟลชทาง USB อื่นๆ ส่วนใหญ่ จะมีอิมเมจที่ติดตั้งไว้ล่วงหน้า หากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่จะใช้ ไม่มีอิมเมจนี้อยู่ ให้ใช้ขั้นตอนที่จะกล่าวถึงต่อไปในหัวข้อนี้ (โปรดดู อุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่ไม่สนับสนุน ในหน้า 20)

ในการสร้างอุปกรณ์สื่อสำหรับการแฟลชทาง USB เพื่อใช้ในการบูต คุณต้องมี:

- อุปกรณ์สื่อสำหรับแฟลชทาง USB ที่รองรับ
- แผ่นดิสเก็ตต์ DOS ที่สามารถบูตได้ พร้อมโปรแกรม FDISK และ SYS (หากไม่มีโปรแกรม SYS สามารถใช้คำสั่ง FORMAT ได้ แต่ไฟล์ที่มีอยู่ทั้งหมดในอุปกรณ์สื่อสำหรับการแฟลชทาง USB จะสูญหาย)
- เครื่องพีซีที่สามารถบูตได้จากอุปกรณ์สื่อสำหรับการแฟลชทาง USB

△ **ข้อควรระวัง:** เครื่องพีซีรุ่นเก่าบางเครื่องอาจไม่สามารถบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB หากค่าดีฟอลต์ของลำดับการบูตในยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) แสดงอุปกรณ์ USB ไว้ก่อนหน้าฮาร์ดไดรฟ์ คอมพิวเตอร์เครื่องนั้นจะสามารถบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ได้ มิเช่นก็ต้องใช้ดิสเก็ตต์ที่ใช้บูตได้

1. ปิดเครื่องคอมพิวเตอร์
2. ใส่อุปกรณ์สื่อสำหรับการแฟลชทาง USB ในพอร์ต USB ช่องใดช่องหนึ่งของเครื่อง แล้วถอดอุปกรณ์ USB สำหรับการจัดเก็บข้อมูลอื่นๆ ทั้งหมดออก ยกเว้นดิสเก็ตต์ไดรฟ์ USB
3. ใส่แผ่นดิสเก็ตต์ DOS ที่ใช้บูตได้ ซึ่งมีไฟล์ FDISK.COM และ SYS.COM หรือ FORMAT.COM ลงในดิสเก็ตต์ไดรฟ์ แล้วเปิดคอมพิวเตอร์เพื่อบูตจากดิสเก็ตต์ DOS
4. รัน FDISK จากพรอมต์ **A:** โดยพิมพ์ `FDISK` และกด Enter หากมีข้อความแจ้ง ให้คลิก **Yes** (**Y**) เพื่อใช้งานการสนับสนุนส่วนใหญ่ของดิสก์
5. เลือก Choice [5] เพื่อแสดงไดรฟ์ในระบบ อุปกรณ์สื่อสำหรับการแฟลชทาง USB จะเป็นไดรฟ์ที่มีขนาดใกล้เคียงกับขนาดของไดรฟ์ใดไดรฟ์หนึ่งที่แสดงในรายการ โดยปกติจะเป็นไดรฟ์สุดท้ายในรายการ บันทึกตัวอักษรประจำไดรฟ์

   อุปกรณ์สื่อสำหรับการแฟลชทาง USB: _____

   △ **ข้อควรระวัง:** หากไดรฟ์ไม่ตรงกับอุปกรณ์สื่อสำหรับการแฟลชทาง USB อย่าดำเนินการต่อไป เพราะอาจเกิดการสูญหายของข้อมูลได้ โปรดตรวจสอบพอร์ต USB ทั้งหมดสำหรับอุปกรณ์เพิ่มเติมที่ใช้จัดเก็บข้อมูล หากพบ ให้ลบออก บูตเครื่องคอมพิวเตอร์อีกครั้ง และทำตามขั้นตอน 4 หากไม่พบ ระบบอาจไม่สนับสนุนอุปกรณ์สื่อการแฟลชทาง USB หรืออุปกรณ์สื่อการแฟลชทาง USB มีความบกพร่อง อย่าพยายามดำเนินการเพื่อให้อุปกรณ์สื่อสำหรับการแฟลชทาง USB สามารถใช้บูตได้
6. ออกจาก FDISK โดยกดปุ่ม Esc เพื่อกลับไปยังพรอมต์ **A:**
7. หากดิสเก็ตต์ DOS ที่ใช้บูตของคุณ มีไฟล์ SYS.COM ให้ทำตามขั้นตอนข้อ 8 หากไม่มี ให้ไปที่ขั้นตอน 9
8. ที่พรอมต์ **A:** ให้พิมพ์ `SYS x:` โดยที่ x หมายถึงตัวอักษรกำกับไดรฟ์ที่กล่าวถึงข้างต้น

   △ **ข้อควรระวัง:** โปรดตรวจสอบให้แน่ใจว่าคุณใส่ตัวอักษรของไดรฟ์ที่ถูกต้องสำหรับอุปกรณ์สื่อสำหรับการแฟลชทาง USB

   หลังจากไฟล์ระบบได้รับการถ่ายโอนแล้ว SYS จะกลับไปยังพรอมต์ **A:** ดำเนินการต่อไปยังขั้นตอนข้อ 13
9. คัดลอกไฟล์ที่คุณต้องการเก็บจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ไปยังไดเรคทอรีชั่วคราวในไดรฟ์อื่น (เช่น ฮาร์ดไดรฟ์ภายในเครื่อง)
10. ที่พรอมต์ **A:** ให้พิมพ์ `FORMAT /S X:` โดยที่ `X` หมายถึงตัวอักษรกำกับไดรฟ์ที่กล่าวถึงก่อนหน้านี้

    △ **ข้อควรระวัง:** โปรดตรวจสอบให้แน่ใจว่าคุณใส่ตัวอักษรของไดรฟ์ที่ถูกต้องสำหรับอุปกรณ์สื่อสำหรับการแฟลชทาง USB

    FORMAT จะแสดงข้อความ และสอบถามคุณในแต่ละครั้งว่าต้องการดำเนินการต่อหรือไม่ ป้อน `Y` ในแต่ละครั้ง FORMAT จะดำเนินการฟอร์แมตอุปกรณ์สื่อสำหรับการแฟลชทาง USB เพิ่มไฟล์ระบบ และถามชื่อของอุปกรณ์
11. กด Enter หากไม่ต้องการตั้งชื่อ หรือป้อนชื่อหากต้องการ

12. คัดลอกไฟล์ที่คุณบันทึกไว้ในขั้นตอนที่ 9 กลับไปยังอุปกรณ์สื่อสำหรับการแฟลชทาง USB

13. นำดิสเก็ตต์ออก และบูตเครื่องอีกครั้ง คอมพิวเตอร์จะบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ให้เป็นไดรฟ์ C

หมายเหตุ: ค่าดีฟอลต์ของลำดับการบูตจะแตกต่างกันในคอมพิวเตอร์แต่ละเครื่อง และสามารถเปลี่ยนแปลงได้จากยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)

หากคุณใช้เวอร์ชันของ DOS จาก Windows 9x คุณอาจเห็นหน้าจอโลโก้ Windows แสดงขึ้นชั่วครู่ หากคุณไม่ต้องการเห็นหน้าจอนี้ ให้เพิ่มไฟล์ชื่อ LOGO.SYS ไว้ที่ไดเรคทอรีรากของอุปกรณ์สื่อสำหรับการแฟลชทาง USB

กลับไปยัง การคัดลอกไปยังคอมพิวเตอร์หลายเครื่อง ในหน้า 17

อุปกรณ์สื่อสำหรับการแฟลชทาง USB ที่ไม่สนับสนุน

ในการสร้างอุปกรณ์สื่อสำหรับการแฟลชทาง USB เพื่อใช้ในการบูต คุณต้องมี:

- อุปกรณ์สื่อสำหรับการแฟลชทาง USB
- แผ่นดิสเก็ตต์ DOS ที่สามารถบูตได้ พร้อมโปรแกรม FDISK และ SYS (หากไม่มีโปรแกรม SYS สามารถใช้คำสั่ง FORMAT ได้ แต่ไฟล์ที่มีอยู่ทั้งหมดในอุปกรณ์สื่อสำหรับการแฟลชทาง USB จะสูญหาย)
- เครื่องพีซีที่สามารถบูตได้จากอุปกรณ์สื่อสำหรับการแฟลชทาง USB

△ **ข้อควรระวัง:** เครื่องพีซีรุ่นเก่าบางเครื่องอาจไม่สามารถบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB หากค่าดีฟอลต์ของลำดับการบูตในยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) แสดงอุปกรณ์ USB ไว้ก่อนหน้าฮาร์ดไดรฟ์ คอมพิวเตอร์เครื่องนั้นจะสามารถบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ได้ มิเช่นก็ต้องใช้ดิสเก็ตต์ที่ใช้บูตได้

1. หากมีการ์ด PCI ในเครื่อง ซึ่งมีไดรฟ์ SCSI, ATA RAID หรือ SATA ต่ออยู่ ให้ปิดเครื่องแล้วถอดสายไฟออก

   △ **ข้อควรระวัง:** ต้องถอดสายไฟออก

2. เปิดคอมพิวเตอร์และถอดการ์ด PCI

3. ใส่อุปกรณ์สื่อสำหรับการแฟลชทาง USB ในพอร์ต USB ช่องใดช่องหนึ่งของเครื่อง แล้วถอดอุปกรณ์ USB สำหรับการจัดเก็บข้อมูลอื่นๆ ทั้งหมดออก ยกเว้นดิสเก็ตต์ไดรฟ์ USB ใส่ฝาปิดเครื่องคอมพิวเตอร์เข้าที่

4. เสียบสายไฟและเปิดคอมพิวเตอร์

5. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

   หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

6. ไปที่ **Advanced** > **PCI Devices** เพื่อยกเลิกการใช้งานทั้งคอนโทรลเลอร์ PATA และ SATA เมื่อยกเลิกการใช้งานคอนโทรลเลอร์ SATA ให้บันทึก IRQ ที่กำหนดไว้สำหรับคอนโทรลเลอร์นั้น เนื่องจากคุณจะต้องกำหนด IRQ นี้อีกครั้งในภายหลัง ออกจากการตั้งค่า โดยยืนยันการเปลี่ยนแปลง

   SATA IRQ: _____

7. ใส่แผ่นดิสเก็ตต์ DOS ที่ใช้บูตได้ ซึ่งมีไฟล์ FDISK.COM และ SYS.COM หรือ FORMAT.COM ลงในดิสเก็ตต์ไดรฟ์ แล้วเปิดคอมพิวเตอร์เพื่อบูตจากดิสเก็ตต์ DOS

8. รัน FDISK และลบพาร์ทิชันใดๆ ที่มีอยู่ในอุปกรณ์สื่อสำหรับการแฟลชทาง USB สร้างพาร์ทิชันใหม่ และกำหนดให้ใช้งาน ออกจาก FDISK โดยกดปุ่ม Esc

9. หากเครื่องไม่เริ่มต้นการทำงานอีกครั้งโดยอัตโนมัติหลังจากออกจาก FDISK ให้กด Ctrl+Alt+Del เพื่อบูตจากดิสเก็ตต์ DOS อีกครั้ง

10. ที่พรอมต์ **A:** ให้พิมพ์ `FORMAT C: /S` และกด Enter Format จะดำเนินการฟอร์แมตอุปกรณ์สื่อสำหรับการแฟลชทาง USB เพิ่มไฟล์ระบบ และถามชื่อของอุปกรณ์
11. กด Enter หากไม่ต้องการตั้งชื่อ หรือป้อนชื่อหากต้องการ
12. ปิดคอมพิวเตอร์ และถอดปลั๊กสายไฟ เปิดฝาคอมพิวเตอร์ และติดตั้งการ์ด PCI ที่ถอดออกไปก่อนหน้านี้กลับคืน ใส่ฝาปิดเครื่องคอมพิวเตอร์เข้าที่
13. เสียบปลั๊กไฟ นำแผ่นดิสก์ออก และเปิดคอมพิวเตอร์
14. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น
15. ไปที่ **Advanced** > **PCI Devices** และเปิดใช้การทำงานของคอนโทรลเลอร์ PATA และ SATA ที่ยกเลิกไปในขั้นตอนที่ 6 อีกครั้ง ใส่คอนโทรลเลอร์ SATA ไว้ที่ IRQ เดิม
16. จัดเก็บการเปลี่ยนแปลงและออกจากโปรแกรม คอมพิวเตอร์จะบูตจากอุปกรณ์สื่อสำหรับการแฟลชทาง USB ให้เป็นไดรฟ์ C

หมายเหตุ: ค่าดีฟอลต์ของลำดับการบูตจะแตกต่างกันในคอมพิวเตอร์แต่ละเครื่อง และสามารถเปลี่ยนแปลงได้จากยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10) ดูที่ *ยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)* สำหรับคำแนะนำ

หากคุณใช้เวอร์ชันของ DOS จาก Windows 9x คุณอาจเห็นหน้าจอโลโก้ Windows แสดงขึ้นชั่วครู่ หากคุณไม่ต้องการเห็นหน้าจอนี้ ให้เพิ่มไฟล์ชื่อ LOGO.SYS ไว้ที่ไดเรคทอรีรากของอุปกรณ์สื่อสำหรับการแฟลชทาง USB

กลับไปยัง การคัดลอกไปยังคอมพิวเตอร์หลายเครื่อง ในหน้า 17

8 ไฟสถานะเปิดเครื่องแบบสองสถานะ

เมื่อใช้คุณสมบัติ Advanced Configuration and Power Interface (ACPI) ปุ่มเพาเวอร์สามารถทำงานเป็นปุ่มเปิด/ปิดเครื่องตามปกติหรือเป็นปุ่มพักการทำงานก็ได้ คุณสมบัติสแตนด์บายจะไม่ปิดเครื่องคอมพิวเตอร์อย่างสมบูรณ์ แต่จะทำให้เครื่องคอมพิวเตอร์อยู่ในโหมดสแตนด์บายซึ่งใช้พลังงานน้อย ซึ่งทำให้คุณสามารถหยุดการทำงานของเครื่องได้อย่างรวดเร็วโดยไม่ต้องปิดแอปพลิเคชันต่างๆ และสามารถกลับมาใช้งานในสภาวะเดิมได้โดยไม่สูญเสียข้อมูล

ในการเปลี่ยนการตั้งค่าปุ่มเพาเวอร์ของเครื่องคอมพิวเตอร์ ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. คลิกซ้ายที่ **Start Button** และเลือก **Control Panel** > **Power Options**
2. เมื่ออยู่ใน **Power Options Properties** ให้เลือกแท็บ **Advanced**
3. ในหัวข้อ **Power Button** ให้เลือก **Stand by**

หลังจากที่ตั้งค่าปุ่มเพาเวอร์ให้ทำงานเป็นปุ่มพักการทำงานแล้ว ให้กดปุ่มเพาเวอร์เพื่อนำคอมพิวเตอร์เข้าสู่สภาวะการใช้พลังงานน้อย (พักการทำงาน) กดปุ่มอีกครั้งเพื่อออกจากสภาวะพักการทำงานและกลับสู่การใช้พลังงานเต็มอัตรา เมื่อต้องการปิดเครื่องคอมพิวเตอร์โดยสมบูรณ์ ให้กดปุ่มเพาเวอร์ค้างไว้เป็นเวลา 4 วินาที

△ **ข้อควรระวัง:** อย่าใช้ปุ่มเพาเวอร์เพื่อปิดคอมพิวเตอร์ ยกเว้นแต่ระบบไม่ตอบสนองการทำงาน การปิดด้วยปุ่มเพาเวอร์ โดยไม่ได้สื่อสารกับระบบปฏิบัติการอาจเป็นเหตุให้เกิดความเสียหายกับฮาร์ดไดรฟ์หรือข้อมูลในฮาร์ดไดรฟ์สูญหายได้

9 การสนับสนุนบนเว็บไซต์ของ HP

วิศวกรของ HPได้ทดสอบและปรับปรุงซอฟต์แวร์ที่ HP และผู้ผลิตรายอื่นผลิตขึ้น และพัฒนาซอฟต์แวร์สนับสนุนสำหรับระบบปฏิบัติการ เพื่อให้คุณมั่นใจถึงประสิทธิภาพ และสมรรถนะสูงสุดสำหรับเครื่องคอมพิวเตอร์ของ HP

เมื่อมีการเปลี่ยนไปยังระบบปฏิบัติการใหม่หรือระบบปฏิบัติการที่ปรับปรุงใหม่ การใช้ซอฟต์แวร์สนับสนุนที่ได้รับการออกแบบเพื่อระบบนั้นโดยเฉพาะเป็นสิ่งสำคัญ หากคุณต้องการใช้ Microsoft Windows ที่มีเวอร์ชันต่างจากที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ คุณจะต้องติดตั้งไดรเวอร์และยูทิลิตีในเวอร์ชันที่ตรงกัน เพื่อให้สามารถใช้คุณสมบัติที่สนับสนุนและฟังก์ชันต่างๆ ได้อย่างเหมาะสม

HP ช่วยให้การค้นหา การเข้าใช้ การประเมิน และการติดตั้งซอฟต์แวร์สนับสนุนเวอร์ชันล่าสุดเป็นไปได้ง่ายขึ้น โดยคุณสามารถดาวน์โหลดซอฟต์แวร์จาก http://www.hp.com/support

เว็บไซต์นี้ประกอบด้วยดีไวซ์ไดรเวอร์ ยูทิลิตี และอิมเมจของ ROM ที่แฟลชได้ในเวอร์ชันล่าสุด สำหรับใช้งานกับระบบปฏิบัติการ Microsoft Windows เวอร์ชันล่าสุดในเครื่องคอมพิวเตอร์ HP

10 มาตรฐานอุตสาหกรรม

โซลูชันการจัดการของ HP ผสมผสานรวมเข้ากับแอปพลิเคชันการจัดการระบบแบบอื่นๆ และอิงตามมาตรฐานอุตสาหกรรม เช่น:

- Web-Based Enterprise Management (WBEM)
- Windows Management Interface (WMI)
- เทคโนโลยี Wake on LAN
- ACPI
- SMBIOS
- การสนับสนุน Pre-boot Execution (PXE)

11 การควบคุมทรัพย์สินและการรักษาความปลอดภัย

คุณสมบัติการติดตามสินทรัพย์ที่มาพร้อมกับคอมพิวเตอร์ช่วยให้ข้อมูลการติดตามทรัพย์สินที่สำคัญซึ่งสามารถจัดการได้โดยโปรแกรม HP Systems Insight Manager, HP Client Manager, HP Configuration Management Solution, HP Client Configuration Manager หรือแอปพลิเคชันการจัดการระบบอื่นๆ การทำงานร่วมกันของคุณสมบัติการติดตามสินทรัพย์และผลิตภัณฑ์เหล่านี้อย่างสมบูรณ์แบบโดยอัตโนมัติจะช่วยให้คุณสามารถเลือกเครื่องมือในการจัดการที่เหมาะสมกับสภาวะการทำงานของคุณมากที่สุด และสามารถใช้ประโยชน์จากเครื่องมือที่มีอยู่เดิมได้อย่างคุ้มค่า

นอกจากนี้ HP ยังมีโซลูชันที่หลากหลายสำหรับควบคุมการเข้าถึงส่วนประกอบและข้อมูลที่สำคัญต่างๆ หากติดตั้ง HP Embedded Security for ProtectTools ไว้ จะช่วยป้องกัน การเข้าใช้ข้อมูล โดยไม่ได้รับอนุญาต และตรวจสอบความสมบูรณ์ของระบบและความถูกต้องของผู้ใช้รายอื่นที่พยายามเข้าสู่ระบบ (สำหรับข้อมูลเพิ่มเติม โปรดดูจากคู่มือ *HP ProtectTools Security Manager Guide* ที่ http://www.hp.com/products/security) คุณสมบัติการรักษาความปลอดภัย อย่างเช่น HP Embedded Security สำหรับ ProtectTools เซนเซอร์ Smart Cover และล็อค Smart Cover ซึ่งมีให้ในผลิตภัณฑ์บางรุ่น จะช่วยป้องกันการเข้าถึงส่วนประกอบภายในของเครื่องคอมพิวเตอร์โดยไม่ได้รับอนุญาตได้ และด้วยการตัดการทำงานของพอร์ตขนาน อนุกรม หรือ USB หรือตัดการทำงานในการบูตจากสื่อ คุณจะสามารถป้องกันการเข้าถึงข้อมูลที่สำคัญได้ การแจ้งเตือนการเปลี่ยนหน่วยความจำและเซ็นเซอร์ Smart Cover สามารถจะส่งต่อไปยังแอปพลิเคชันการจัดการระบบเพื่อแจ้งให้ทราบถึงการบุกรุกส่วนประกอบภายในของคอมพิวเตอร์ได้อย่างทันท่วงที

หมายเหตุ: HP Embedded Security for Protect Tools, เซ็นเซอร์ Smart Cover และล็อค Smart Cover เป็นอุปกรณ์เสริมสำหรับคอมพิวเตอร์บางรุ่น

ใช้ยูทิลิตีต่อไปนี้เพื่อรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ HP:

- สำหรับการรักษาความปลอดภัยภายใน ให้ใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์ โปรดดูที่ *คู่มือยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)* ซึ่งมาพร้อมกับเครื่องคอมพิวเตอร์ เพื่อดูข้อมูลและคำแนะนำเพิ่มเติมเกี่ยวกับการใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์ ซอฟต์แวร์นี้จะช่วยให้คุณสามารถใช้งานและควบคุมการรักษาความปลอดภัยได้อย่างแน่นอนและทั่วถึงจากยูทิลิตีบรรทัดคำสั่งที่ง่ายดาย
- ส่วนการจัดการระยะไกล ให้ใช้ HP Client Manager จาก Symantec, HP Client Automation หรือ System Software Manager ซอฟต์แวร์นี้จะช่วยให้คุณสามารถใช้งานและควบคุมการรักษาความปลอดภัยได้อย่างแน่นอนและทั่วถึง

ตารางและหัวข้อต่อไปนี้จะกล่าวถึงคุณสมบัติการจัดการด้านความปลอดภัยภายในเครื่องคอมพิวเตอร์โดยใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)

ตาราง 11-1 ภาพรวมของคุณสมบัติการรักษาความปลอดภัย

ตัวเลือก	คำอธิบาย
Setup Password	ใช้สำหรับกำหนดและเปิดใช้งานรหัสผ่านสำหรับการตั้งค่า (สำหรับผู้ดูแลระบบ) **หมายเหตุ:** หากกำหนดรหัสผ่านสำหรับการตั้งค่าแล้ว คุณจะต้องใช้รหัสผ่านนั้นในการเปลี่ยนตัวเลือกของโปรแกรมการตั้งค่าระบบ แฟลช ROM หรือเปลี่ยนแปลงการตั้งค่าพลักแอนด์เพลย์ใน Windows
Power-On Password	ให้กำหนดและใช้งานรหัสผ่านเมื่อเปิดเครื่อง ข้อความแจ้งเตือนรหัสผ่านเมื่อเปิดเครื่องแสดงขึ้นหลังจากรอบการเปิด ในกรณีที่ผู้ใช้ป้อนรหัสผ่านเมื่อเปิดเครื่องไม่ถูกต้อง เครื่องจะไม่บูต **หมายเหตุ:** รหัสผ่านนี้จะไม่ปรากฏตอนวอร์มบูต หรือการกด Ctrl+Alt+Delete หรือ **การรีสตาร์ทจาก Windows** เว้นแต่ได้เปิดใช้ **ตัวเลือกรหัสผ่าน** (ดูด้านล่างนี้)

ตาราง 11-1 ภาพรวมของคุณสมบัติการรักษาความปลอดภัย (ต่อ)

Password Options (ตัวเลือกนี้จะปรากฏเฉพาะเมื่อมีการกำหนดรหัสผ่านหรือตั้งค่ารหัสผ่านเมื่อเปิดเครื่องไว้)	ให้คุณเลือกที่จะ: • Lock legacy resources (จะปรากฏขึ้นหากได้การตั้งค่าระหัสผ่าน) • เปิดหรือปิดใช้งานโหมดเน็กเวิร์กเซิร์ฟเวอร์ (จะปรากฏขึ้นหากมีการกำหนดรหัสผ่านเมื่อเปิดเครื่องไว้) • ระบุว่าจะต้องใช้รหัสผ่านสำหรับการวอร์มบูต (Ctrl+Alt+Delete) หรือไม่ (จะปรากฏขึ้นหากมีการกำหนดรหัสผ่านเมื่อเปิดเครื่องไว้) • ใช้งาน/ไม่ใช้ตั้งค่าโหมด Browse (จะปรากฏขึ้นเมื่อได้ตั้งรหัสผ่านสำหรับการตั้งค่า) (ใช้สำหรับการดู แต่ไม่สามารถเปลี่ยนแปลงตัวเลือกการตั้งค่า F10 หากไม่ได้ป้อนรหัสผ่านสำหรับการตั้งค่า) • ใช้/ไม่ใช้รหัสผ่านที่เข้มงวด (ปรากฏขึ้นหากมีการตั้งค่ารหัสผ่านป้องกันการเปิดเครื่อง) ซึ่งเมื่อถูกเปิดใช้ จะข้ามจัมเปอร์รหัสผ่านบนบอร์ดเพื่อปิดใช้งานรหัสผ่านป้องกันการเปิดเครื่อง โปรดดูที่ *คู่มือการจัดการเดสก์ท็อป* สำหรับข้อมูลเพิ่มเติม
Smart Cover (สำหรับบางรุ่น)	ให้คุณเลือกที่จะ: • ล็อค/ปลดล็อค Cover Lock • ตั้งค่าเซ็นเซอร์ของ Smart Cover ไว้ที่ Disable/Notify User/Setup Password **หมายเหตุ:** *Notify User* แจ้งผู้ใช้ว่าเซ็นเซอร์ตรวจพบว่ามีการถอดฝาครอบเครื่องออก *Setup Password* กำหนดให้ป้อนรหัสผ่านสำหรับการตั้งค่าเพื่อบูตระบบ หากเซ็นเซอร์ตรวจพบว่ามีการถอดฝาครอบเครื่องออก คุณสมบัตินี้มีให้ในบางรุ่นเท่านั้น
Device Security	ให้คุณกำหนดอุปกรณ์เป็นใช้ได้/อุปกรณ์ที่ซ่อนไว้สำหรับ: • พอร์ตอนุกรม • พอร์ตขนาน • พอร์ต USB ด้านหลัง • พอร์ต USB ด้านหน้า • พอร์ต USB ภายใน • สัญญาณเสียงระบบ • คอนโทรลเลอร์เน็ตเวิร์ก (บางรุ่น) • แผ่นดิสก์รุ่นเก่า • อุปกรณ์รักษาความปลอดภัยที่ฝังอยู่ภายใน (บางรุ่น) • SATA0 • SATA1 (บางรุ่น) • SATA2 (บางรุ่น) • SATA3 (บางรุ่น) • eSATA (บางรุ่น)
Network Service Boot	ใช้/ตัดการใช้คุณสมบัติในการบูตจากระบบปฏิบัติการที่ติดตั้งไว้ในเซิร์ฟเวอร์ของเน็ตเวิร์ก (คุณสมบัตินี้มีในรุ่นที่มี NIC เท่านั้น คอนโทรลเลอร์เน็ตเวิร์กจะต้องมีบัส PCI เอ็กซ์แพนชันการ์ดหรืออยู่ภายในเมนบอร์ด)
System IDs	ให้คุณกำหนด: • แท็กกำกับสินทรัพย์ (ตัวระบุแบบ 18 ไบต์) ซึ่งเป็นเลขที่สินทรัพย์ที่บริษัทจะระบุให้กับคอมพิวเตอร์ • แท็กแสดงความเป็นเจ้าของ (ตัวระบุแบบ 80 ไบต์) ที่แสดงระหว่างกระบวนการ POST

ตาราง 11-1 ภาพรวมของคุณสมบัติการรักษาความปลอดภัย (ต่อ)

	• ซีเรียลนัมเบอร์ของโครงเครื่องหรือหมายเลขระบุเฉพาะระดับสากล (UUID) หมายเลข UUID สามารถอัพเดตได้ต่อเมื่อซีเรียลนัมเบอร์ของโครงเครื่องปัจจุบันไม่ถูกต้อง (หมายเลข ID เหล่านี้โดยปกติจะถูกกำหนดมาจากโรงงานและใช้ระบุเครื่องคอมพิวเตอร์โดยเฉพาะ) • การตั้งค่าพื้นที่สำหรับแป้นพิมพ์ (เช่น English หรือ German) สำหรับการป้อน System ID
DriveLock Security	ใช้กำหนดหรือแก้ไขรหัสผ่านหลักหรือรหัสผ่านของผู้ใช้สำหรับฮาร์ดไดรฟ์ เมื่อใช้คุณสมบัตินี้ ผู้ใช้จะได้รับแจ้งให้ป้อนรหัสผ่านสำหรับตัวล็อคไดรฟ์ในระหว่างกระบวนการ POST หากป้อนรหัสผ่านไม่ถูกต้อง ผู้ใช้จะไม่สามารถเข้าใช้ฮาร์ดไดรฟ์ได้จนกว่าจะป้อนรหัสผ่านที่ถูกต้องระหว่างการบูตในภายหลัง **หมายเหตุ:** ตัวเลือกนี้จะปรากฏเฉพาะเมื่อมีไดรฟ์อย่างน้อยหนึ่งไดรฟ์ที่รองรับการใช้คุณสมบัติ DriveLock

ตาราง 11-1 ภาพรวมของคุณสมบัติการรักษาความปลอดภัย (ต่อ)

ความปลอดภัยของระบบ (บางรุ่น: ตัวเลือกเหล่านี้ขึ้นอยู่กับฮาร์ดแวร์)	การป้องกันการเรียกใช้ข้อมูล (บางรุ่น) (ใช้/ไม่ใช้) - ช่วยป้องกันการละเมิดความปลอดภัยของระบบปฏิบัติการ เทคโนโลยี Virtualization (บางรุ่น) (ใช้/ไม่ใช้) - ควบคุมคุณสมบัติเสมือนจริงของโปรเซสเซอร์ การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง เทคโนโลยี Virtualization Directed I/O (บางรุ่น) (ใช้/ไม่ใช้) - ควบคุมคุณสมบัติการรีแมป DMA เสมือนจริงของชิปเซ็ต การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง เทคโนโลยี Trusted Execution (บางรุ่น) (ใช้/ไม่ใช้) - ควบคุมโปรเซสเซอร์และคุณสมบัติชิปเซ็ตที่จำเป็นสำหรับการสนับสนุนคุณลักษณะเสมือนจริง การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง ในการเปิดใช้งานคุณสมบัตินี้ คุณต้องเปิดใช้งานคุณสมบัติต่อไปนี้: • การสนับสนุนอุปกรณ์ป้องกันความปลอดภัยภายใน • Virtualization Technology • Virtualization Technology Directed I/O การสนับสนุนอุปกรณ์ป้องกันความปลอดภัยภายใน (บางรุ่น) (ใช้/ไม่ใช้) - อนุญาตให้เรียกใช้และยกเลิกการเรียกใช้อุปกรณ์ป้องกันความปลอดภัยภายใน การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง **หมายเหตุ:** ในการกำหนดค่าอุปกรณ์ป้องกันความปลอดภัยภายใน ต้องตั้งรหัสผ่านการตั้งค่า • รีเซ็ตค่ากลับเป็นค่าที่มาจากโรงงาน (บางรุ่น) (ห้ามรีเซ็ต/รีเซ็ต) - การรีเซ็ตค่ากลับเป็นค่าที่มาจากโรงงานจะลบคีย์ความปลอดภัยทั้งหมด การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง **ข้อควรระวัง:** อุปกรณ์ป้องกันความปลอดภัยภายในถือเป็นองค์ประกอบที่สำคัญของโครงสร้างความปลอดภัยจำนวนมาก การลบคีย์ความปลอดภัยจะป้องกันการเข้าสู่ข้อมูลที่มีอุปกรณ์ป้องกันความปลอดภัยภายในป้องกันไว้ การเลือกรีเซ็ตค่ากลับเป็นค่าที่มาจากโรงงานอาจทำให้ข้อมูลสูญหายได้ • การสนับสนุนการตรวจสอบความถูกต้องเมื่อเปิดเครื่องไว้ (บางรุ่น) - (ใช้/ไม่ใช้) ควบคุมโครงสร้างการตรวจสอบความถูกต้องด้วยรหัสผ่านเมื่อเปิดเครื่อง ที่ช่วยให้ใช้อุปกรณ์ป้องกันความปลอดภัยภายในได้อย่างคุ้มค่า การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง • รีเซ็ตใบรับรองการตรวจสอบความถูกต้อง (บางรุ่น) (ห้ามรีเซ็ต/รีเซ็ต) - เลือกการรีเซ็ตคือการยกเลิกการใช้การสนับสนุนการตรวจสอบความถูกต้องด้วยรหัสผ่านเมื่อเปิดเครื่อง และล้างข้อมูลการตรวจสอบความถูกต้องออกจากอุปกรณ์ป้องกันความปลอดภัยภายใน การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง การจัดการ OS ของอุปกรณ์ป้องกันความปลอดภัยภายใน (บางรุ่น) (ใช้/ไม่ใช้) - ตัวเลือกนี้อนุญาตให้ผู้ใช้จำกัดการควบคุมอุปกรณ์ป้องกันความปลอดภัยภายในของระบบปฏิบัติการ การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง ตัวเลือกนี้อนุญาตให้ผู้ใช้จำกัดการควบคุมอุปกรณ์รักษาความปลอดภัยที่มีอยู่ภายในของระบบปฏิบัติการ • รีเซ็ตอุปกรณ์ป้องกันความปลอดภัยภายในผ่าน OS (บางรุ่น) (ใช้/ไม่ใช้) - ตัวเลือกนี้อนุญาตให้ผู้ใช้จำกัดความสามารถของระบบปฏิบัติการในการแจ้งขอรีเซ็ตค่ากลับเป็นค่าที่มาจากโรงงานของอุปกรณ์ป้องกันความปลอดภัยภายใน การเปลี่ยนแปลงการตั้งค่านี้จะต้องปิดและเปิดคอมพิวเตอร์อีกครั้ง **หมายเหตุ:** ในการเปิดใช้งานตัวเลือกนี้ ต้องตั้งรหัสผ่านการตั้งค่า การสนับสนุนรหัสผ่าน BIOS ของสมาร์ทการ์ด (บางรุ่น) (ใช้/ไม่ใช้) - อนุญาตให้ผู้ใช้เปิดใช้งาน/ปิดใช้งานสมาร์ทการ์ดที่จะนำมาใช้แทนรหัสผ่านเมื่อเปิดเครื่องและรหัสผ่านเมื่อกำหนดค่า การตั้งค่านี้ต้องอาศัยการเริ่มต้นการทำงานเพิ่มเติมภายใน ProtectTools ก่อนที่ตัวเลือกนี้จะมีผลใช้ PAVP (บางรุ่น) (ปิดใช้งาน/ต่ำสุด/สูงสุด) - PAVP เปิดใช้ Protected Audio Video Path ในชิปเซ็ต โดยอาจอนุญาตให้ดูเนื้อหาความละเอียดสูงที่ถูกป้องกัน ซึ่งมิฉะนั้นจะถูกห้ามไม่ให้เล่น การเลือกตัวเลือก สูงสุด จะมอบหมายหน่วยความจำระบบ 96 เมกะไบต์ให้แก่ PAVP โดยเฉพาะ
Setup Security Level	จัดเตรียมวิธีการที่อนุญาตการเข้าถึงแบบจำกัดสำหรับผู้ใช้เพื่อทำการเปลี่ยนแปลงตัวเลือกการตั้งค่าเฉพาะ โดยไม่ต้องทราบรหัสผ่านสำหรับการตั้งค่า คุณสมบัตินี้ช่วยให้ผู้ดูแลระบบมีความยืดหยุ่นในการป้องกันการเปลี่ยนแปลงตัวเลือกการตั้งค่าที่สำคัญ ในขณะที่อนุญาตให้ผู้ใช้ดูการตั้งค่าของระบบและกำหนดค่าตัวเลือกที่ไม่สำคัญ ผู้ดูแลระบบจะระบุสิทธิ์การเข้าใช้ตัวเลือกการตั้งค่าบางตัวเลือกโดยจะพิจารณาเป็นกรณีไปผ่านเมนูระดับการตั้งค่าการรักษาความปลอดภัย ตามค่าดีฟอลต์นั้น ตัวเลือกการตั้งค่าทั้งหมดกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ เพื่อแจ้งให้ทราบว่า ผู้ใช้ต้องป้อนรหัสผ่านสำหรับการตั้งค่าที่ถูกต้องในระหว่างการ POST เพื่อทำการเปลี่ยนแปลงตัวเลือกใดๆ ผู้ดูแลระบบอาจจะตั้งค่ารายการตัวเลือกบางรายการเป็น None เพื่อแจ้งให้ทราบว่า ผู้ใช้สามารถทำการเปลี่ยนแปลงตัวเลือกบางตัวเลือกได้เมื่อเข้าถึงการตั้งค่าได้ด้วยรหัสผ่านที่ไม่ถูกต้อง ตัวเลือก None ถูกแทนที่ด้วยตัวเลือก รหัสผ่านป้องกันการเปิดเครื่อง เมื่อเปิดใช้ตัวเลือกรหัสผ่านป้องกันการเปิดเครื่องแล้ว

ตาราง 11-1 ภาพรวมของคุณสมบัติการรักษาความปลอดภัย (ต่อ)

หมายเหตุ:	ต้องตั้งการตั้งค่าโหมด Browse เป็นเปิดใช้งานอยู่เพื่อให้ผู้ใช้เข้าสู่โปรแกรมการตั้งค่าได้

การป้องกันด้วยรหัสผ่าน

รหัสผ่านเมื่อเปิดเครื่องจะป้องกันการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาตด้วยการให้ผู้ใช้ป้อนรหัสผ่านเพื่อเข้าใช้แอปพลิเคชันหรือข้อมูลทุกครั้งที่เปิดหรือเริ่มระบบใหม่ ส่วนรหัสผ่านสำหรับการตั้งค่าซึ่งป้องกันการเข้าใช้โปรแกรมการตั้งค่าคอมพิวเตอร์จะสามารถใช้แทนรหัสผ่านเมื่อเปิดเครื่องได้ ซึ่งหมายความว่า เมื่อระบบให้ป้อนรหัสผ่านเมื่อเปิดเครื่อง การป้อนรหัสผ่านสำหรับการตั้งค่าแทนจะมีผลเช่นเดียวกัน

คุณสามารถกำหนดรหัสผ่านสำหรับการตั้งค่าของคอมพิวเตอร์ทั้งเน็ตเวิร์ก ซึ่งทำให้ผู้ดูแลระบบสามารถล็อกอินเข้าสู่เครื่องคอมพิวเตอร์ทุกเครื่องเพื่อดำเนินการซ่อมบำรุง โดยไม่ต้องทราบรหัสผ่านเมื่อเปิดเครื่อง แม้ว่าจะมีกำหนดไว้ก็ตาม

การกำหนดรหัสผ่านสำหรับการตั้งค่าโดยใช้โปรแกรมการตั้งค่าคอมพิวเตอร์

หากระบบมีอุปกรณ์ป้องกันความปลอดภัยภายใน ให้ดูรายละเอียดเพิ่มเติมใน *คู่มือ HP ProtectTools Security Manager* ที่ http://www.hp.com การกำหนดรหัสผ่านสำหรับการตั้งค่าจากโปรแกรมการตั้งค่าคอมพิวเตอร์จะป้องกันการแก้ไขการตั้งค่าของเครื่องคอมพิวเตอร์ (การใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)) หากไม่ได้ป้อนรหัสผ่าน

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

> **หมายเหตุ:** หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เลือก **Security** จากนั้นเลือก **Setup Password** และปฏิบัติตามคำแนะนำบนหน้าจอ
4. ก่อนที่จะออกจากโปรแกรม ให้คลิกที่ **File** > **Save Changes and Exit**

การกำหนดรหัสผ่านเมื่อเปิดเครื่องโดยใช้โปรแกรมการตั้งค่าคอมพิวเตอร์

การกำหนดรหัสผ่านเมื่อเปิดเครื่องในโปรแกรมการตั้งค่าคอมพิวเตอร์จะป้องกันการเข้าใช้เครื่องคอมพิวเตอร์เมื่อเปิดระบบหากไม่ได้ป้อนรหัสผ่าน เมื่อกำหนดรหัสผ่านเมื่อเปิดเครื่องแล้ว โปรแกรมการตั้งค่าคอมพิวเตอร์จะแสดง **Password Options** ใต้เมนู **Security** ตัวเลือกของรหัสผ่านจะรวมถึง **Password Prompt on Warm Boot** เมื่อเลือก **Password Prompt on Warm Boot** คุณจะต้องป้อนรหัสผ่านทุกครั้งที่รีบูตเครื่องคอมพิวเตอร์

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

> **หมายเหตุ:** หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เลือก **Security** จากนั้นเลือก **Power-On Password** และปฏิบัติตามคำแนะนำบนหน้าจอ
4. ก่อนที่จะออกจากโปรแกรม ให้คลิกที่ **File** > **Save Changes and Exit**

การป้อนรหัสผ่านเมื่อเปิดเครื่อง

ในการป้อนรหัสผ่านเมื่อเปิดเครื่อง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart the Computer**
2. เมื่อไอคอนรูปกุญแจปรากฏบนหน้าจอ ให้พิมพ์รหัสผ่านปัจจุบัน แล้วกด Enter

หมายเหตุ: พิมพ์รหัสผ่านที่ถูกต้อง และด้วยเหตุผลด้านความปลอดภัย ตัวอักษรที่คุณพิมพ์จะไม่ปรากฏบนหน้าจอ

หากคุณป้อนรหัสผ่านไม่ถูกต้อง ไอคอนรูปกุญแจหักจะปรากฏขึ้น ให้ลองพิมพ์อีกครั้ง หากใส่รหัสผ่านผิดติดต่อกันสามครั้ง คุณจะต้องปิดเครื่องคอมพิวเตอร์ แล้วเปิดใหม่อีกครั้งก่อนที่จะดำเนินการต่อ

การป้อนรหัสผ่านสำหรับการตั้งค่า

หากระบบมีอุปกรณ์ป้องกันความปลอดภัยภายใน ให้ดูรายละเอียดเพิ่มเติมใน *คู่มือ HP ProtectTools Security Manager* ที่ http://www.hp.com

หากมีการกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ในคอมพิวเตอร์ ระบบจะให้คุณป้อนรหัสผ่านดังกล่าวทุกครั้งที่รันโปรแกรมการตั้งค่าคอมพิวเตอร์

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เมื่อไอคอนรูปกุญแจปรากฏบนหน้าจอ ให้พิมพ์รหัสผ่านสำหรับการตั้งค่า แล้วกด Enter

หมายเหตุ: พิมพ์รหัสผ่านที่ถูกต้อง และด้วยเหตุผลด้านความปลอดภัย ตัวอักษรที่คุณพิมพ์จะไม่ปรากฏบนหน้าจอ

หากคุณป้อนรหัสผ่านไม่ถูกต้อง ไอคอนรูปกุญแจหักจะปรากฏขึ้น ให้ลองพิมพ์อีกครั้ง หากใส่รหัสผ่านผิดติดต่อกันสามครั้ง คุณจะต้องปิดเครื่องคอมพิวเตอร์ แล้วเปิดใหม่อีกครั้งก่อนที่จะดำเนินการต่อ

การเปลี่ยนรหัสผ่านเมื่อเปิดเครื่องหรือรหัสผ่านสำหรับการตั้งค่า

หากระบบมีอุปกรณ์ป้องกันความปลอดภัยภายใน ให้ดูรายละเอียดเพิ่มเติมใน *คู่มือ HP ProtectTools Security Manager* ที่ http://www.hp.com

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart the Computer**
2. หากต้องการเปลี่ยนรหัสผ่านเมื่อเปิดเครื่อง ให้ทำตามขั้นตอน 3

   ในการเปลี่ยนรหัสผ่านสำหรับการตั้งค่า ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เมื่อไอคอนรูปกุญแจปรากฏขึ้น ให้พิมพ์รหัสผ่านปัจจุบัน ตามด้วยเครื่องหมายทับ (/) หรือตัวคั่นอื่น รหัสผ่านใหม่ ตามด้วยเครื่องหมายคั่น (/) หรือตัวคั่นอื่น และรหัสผ่านใหม่อีกครั้งตามที่แสดงต่อไปนี้: รหัสผ่านปัจจุบัน/รหัสผ่านใหม่/รหัสผ่านใหม่

หมายเหตุ: พิมพ์รหัสผ่านที่ถูกต้อง และด้วยเหตุผลด้านความปลอดภัย ตัวอักษรที่คุณพิมพ์จะไม่ปรากฏบนหน้าจอ

4. กด Enter

รหัสผ่านใหม่จะมีผลเมื่อคุณเปิดเครื่องในครั้งถัดไป

หมายเหตุ: โปรดดูที่ อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ ในหน้า 31 สำหรับข้อมูลเกี่ยวกับอักขระที่ใช้เป็นตัวคั่น นอกจากนี้ คุณสามารถเปลี่ยนรหัสผ่านเมื่อเปิดเครื่องและรหัสผ่านสำหรับการตั้งค่าโดยใช้ตัวเลือก Security ในโปรแกรมการตั้งค่าคอมพิวเตอร์

การลบรหัสผ่านเมื่อเปิดเครื่องหรือรหัสผ่านสำหรับการตั้งค่า

หากระบบมีอุปกรณ์ป้องกันความปลอดภัยภายใน ให้ดูรายละเอียดเพิ่มเติมใน *คู่มือ HP ProtectTools Security Manager* ที่ http://www.hp.com

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart the Computer**

2. หากต้องการลบรหัสผ่านเมื่อเปิดเครื่อง ให้ทำตามขั้นตอน 3

   ในการลบรหัสผ่านสำหรับการตั้งค่า ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

   หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เมื่อไอคอนรูปกุญแจปรากฏขึ้น ให้พิมพ์รหัสผ่านปัจจุบันตามด้วยเครื่องหมายทับ (/) หรือตัวคั่นอื่นตามที่แสดงดังนี้: รหัสผ่านปัจจุบัน/

4. กด Enter

หมายเหตุ: โปรดดู อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ ในหน้า 31 เพื่อดูข้อมูลเกี่ยวกับอักขระอื่นๆ ที่ใช้เป็นตัวคั่น นอกจากนี้ คุณสามารถเปลี่ยนรหัสผ่านเมื่อเปิดเครื่องและรหัสผ่านสำหรับการตั้งค่าโดยใช้ตัวเลือก Security ในโปรแกรมการตั้งค่าคอมพิวเตอร์

อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ

การออกแบบแป้นพิมพ์จะเป็นไปตามมาตรฐานของแต่ละประเทศ/พื้นที่ รูปแบบการพิมพ์และปุ่มที่ใช้สำหรับการเปลี่ยนหรือลบรหัสผ่านจะขึ้นอยู่กับแป้นพิมพ์ที่มาพร้อมกับคอมพิวเตอร์

อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ					
/	อาราบิค	-	กรีก	/	รัสเซีย
=	เบลเยี่ยม	.	ฮิบรู	-	สโลวาเกีย
-	BHCMSS*	-	ฮังการี	-	สเปน
/	บราซิล	-	อิตาลี	/	สวีเดน/ฟินแลนด์
/	จีน	/	ญี่ปุ่น	-	สวิส
-	เช็ก	/	เกาหลี	/	ไต้หวัน
-	เดนมาร์ก	-	ลาตินอเมริกา	/	ไทย
!	ฝรั่งเศส	-	นอร์เวย์	.	ตุรกี
é	ฝรั่งเศสแบบแคนาดา	-	โปแลนด์	/	อังกฤษ สหรัฐฯ

อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ	
- เยอรมัน	- โปรตุเกส
*บอสเนีย-เฮอเซโกวินา โครเอเชีย มอนติเนโกร เซอร์เบีย และสโลวาเนีย	

การยกเลิกรหัสผ่าน

โปรดดูคำแนะนำเกี่ยวกับการยกเลิกรหัสผ่านใน *คู่มือการแก้ไขปัญหา* ใน *แผ่นซีดี Documentation and Diagnostics* โปรดดูคำแนะนำเกี่ยวกับการยกเลิกรหัสผ่านใน *คู่มือการแก้ไขปัญหา*

หากระบบมีอุปกรณ์ป้องกันความปลอดภัยภายใน ให้ดูรายละเอียดเพิ่มเติมใน *คู่มือ HP ProtectTools Security Manager* ที่ http://www.hp.com

DriveLock

DriveLock เป็นคุณสมบัติป้องกันความปลอดภัยระดับมาตรฐานอุตสาหกรรม ที่จะป้องกันการเข้าถึงข้อมูลในฮาร์ดไดรฟ์ ATA โดยไม่ได้รับอนุญาต ตัวล็อคไดรฟ์เป็นส่วนเสริมของโปรแกรมการตั้งค่าคอมพิวเตอร์ ซึ่งสามารถใช้ได้เมื่อตรวจพบฮาร์ดไดรฟ์ที่รองรับชุดคำสั่งระบบความปลอดภัย ATA เท่านั้น DriveLock เป็นคุณสมบัติสำหรับผู้ใช้ HP ที่ให้ความสำคัญสูงสุดในการป้องกันข้อมูล ซึ่งในกรณีนี้ มูลค่าของฮาร์ดไดรฟ์และการสูญเสียข้อมูลในไดรฟ์เปรียบเทียบไม่ได้กับเลยกับกับความเสียหายที่อาจเกิดขึ้นจากการล่วงละเมิดเข้าใช้ข้อมูลสำคัญโดยไม่ได้รับอนุญาต และเพื่อเพิ่มความยืดหยุ่นในกรณีที่คุณลืมรหัสผ่านโดยยังคงระดับการรักษาความปลอดภัยไว้นั้น คุณสมบัติ DriveLock ของ HP จึงใช้รูปแบบการป้องกันด้วยรหัสผ่านสองค่า รหัสผ่านชุดหนึ่งจะถูกกำหนดและใช้โดยผู้ดูแลระบบ ส่วนอีกชุดหนึ่งจะถูกกำหนดและใช้โดยผู้ใช้ปลายทาง และจะไม่มี “หนทางพิเศษ” สำหรับปลดล็อคไดรฟ์หากรหัสผ่านทั้งสองค่าสูญหายไป ดังนั้น คุณสมบัติ DriveLock จะปลอดภัยที่สุดในกรณีที่มีการจำลองข้อมูลในไดรฟ์ไปยังระบบข้อมูลขององค์กร หรือมีการสำรองข้อมูลอย่างสม่ำเสมอ ในกรณีที่ไม่สามารถจำรหัสผ่านทั้งสองค่าของตัวล็อคไดรฟ์ ฮาร์ดไดรฟ์นั้นก็จะใช้ไม่ได้อีกต่อไป ทางเลือกนี้อาจเสี่ยงเกินไปสำหรับผู้ใช้ที่ไม่มีความจำเป็นต้องใช้การป้องกันในระดับนี้ แต่สำหรับผู้ใช้ที่มีความจำเป็น ความเสี่ยงนี้อาจคุ้มค่าเมื่อคำนึงถึงข้อมูลที่เก็บรักษาในไดรฟ์

การใช้ตัวล็อคไดรฟ์

เมื่อตรวจพบฮาร์ดไดรฟ์ตั้งแต่หนึ่งตัวที่สนับสนุนชุดคำสั่งความปลอดภัย ATA ตัวเลือกของ Drivelock จะปรากฏใต้เมนู Security ในโปรแกรมการตั้งค่าคอมพิวเตอร์ ผู้ใช้จะเห็นตัวเลือกในการกำหนดรหัสผ่านหลักหรือใช้งานคุณสมบัติ DriveLock และจะต้องป้อนรหัสผ่านสำหรับผู้ใช้ จึงจะสามารถใช้คุณสมบัตินี้ได้ และเนื่องจากการกำหนดค่าของ DriveLock ในครั้งแรกมักกระทำโดยผู้ดูแลระบบ ดังนั้นจึงควรกำหนดรหัสผ่านหลักก่อน ทั้งนี้ HP ขอแนะนำให้ผู้ดูแลระบบกำหนดรหัสผ่านหลักไว้ ไม่ว่าจะต้องการใช้คุณสมบัติ DriveLock หรือไม่ก็ตาม เพื่อที่ผู้ดูแลระบบจะสามารถแก้ไขการตั้งค่าตัวล็อคไดรฟ์ได้หากมีการล็อคไดรฟ์ในอนาคต เมื่อกำหนดรหัสผ่านหลักแล้ว ผู้ดูแลระบบสามารถใช้คุณสมบัตินี้ หรือเลือกที่จะไม่ใช้คุณสมบัตินี้ก็ได้

หากมีฮาร์ดไดรฟ์ที่ถูกล็อค กระบวนการ POST จะให้คุณป้อนรหัสผ่านเพื่อปลดล็อคไดรฟ์ หากมีการกำหนดรหัสผ่านเมื่อเปิดเครื่องไว้ และรหัสผ่านนั้นตรงกับรหัสผ่านสำหรับผู้ใช้ของตัวล็อคไดรฟ์ กระบวนการ POST จะไม่ให้คุณป้อนรหัสผ่านอีกครั้ง แต่หากไม่มีการกำหนดรหัสผ่านเมื่อเปิดเครื่องไว้ ผู้ใช้จะต้องป้อนรหัสผ่านสำหรับ DriveLock เมื่อเริ่มระบบคอมพิวเตอร์จากเครื่องที่เย็น คุณอาจต้องใช้รหัสผ่านหลักหรือรหัสผ่านสำหรับผู้ใช้ สำหรับการเริ่มระบบคอมพิวเตอร์แบบวอร์มบูต ให้ป้อนรหัสผ่านตัวเดียวกับที่ใช้ปลดล็อคไดรฟ์ในระหว่างการเริ่มระบบคอมพิวเตอร์จากเครื่องที่เย็นที่ทำไปก่อนหน้านี้ ผู้ใช้สามารถป้อนรหัสผ่านได้เพียงสองครั้ง ในการเริ่มระบบคอมพิวเตอร์จากเครื่องที่เย็น หากรหัสผ่านไม่ถูกต้องทั้งสองครั้ง กระบวนการ POST จะดำเนินการต่อ แต่จะไม่สามารถเข้าสู่ไดรฟ์ดังกล่าวได้ สำหรับการเริ่มระบบคอมพิวเตอร์แบบวอร์มบูตหรือการเปิดจาก Windows หากรหัสผ่านไม่ถูกต้องทั้งสองครั้ง กระบวนการ POST จะหยุดลง และผู้ใช้จะได้รับคำแนะนำให้หมุนเวียนพลังงาน

การใช้งาน DriveLock

การใช้งานตัวล็อคไดรฟ์เหมาะที่สุดกับสภาพแวดล้อมแบบองค์กร และผู้ดูแลระบบจะต้องตั้งค่าฮาร์ดไดรฟ์ ซึ่งรวมถึงการกำหนดรหัสผ่านหลักของตัวล็อคไดรฟ์ และรหัสผ่านสำหรับผู้ใช้ชั่วคราวด้วย ในกรณีที่ผู้ใช้ลืมรหัสผ่านสำหรับผู้ใช้ หรือเมื่อมีการเปลี่ยนมือผู้ใช้ คุณสามารถใช้รหัสผ่านหลักเพื่อรีเซ็ตรหัสผ่านสำหรับผู้ใช้และสามารถใช้งานไดรฟ์ได้อีกครั้ง

HP ขอแนะนำให้ผู้ดูแลระบบที่เลือกใช้คุณสมบัตินี้ควรกำหนดนโยบายภายในองค์กรสำหรับการกำหนดและเก็บรักษารหัสผ่านหลัก เพื่อป้องกันเหตุการณ์ที่ผู้ใช้อาจจงใจหรือมิได้จงใจกำหนดรหัสผ่านทั้งสองชุดก่อนที่จะออกจากองค์กร ซึ่งหากเป็นเช่นนั้น จะต้องมีการเปลี่ยนฮาร์ดไดรฟ์ใหม่ เพราะจะไม่สามารถใช้งานฮาร์ดไดรฟ์นี้ได้อีก และเช่นเดียวกัน หากไม่มีการกำหนดรหัสผ่านหลักไว้ ผู้ดูแลระบบอาจไม่สามารถเข้าสู่ฮาร์ดไดรฟ์ได้ และจะไม่สามารถดำเนินการตรวจสอบซอฟต์แวร์ตามปกติได้โดยไม่ได้รับอนุญาต รวมถึงฟังก์ชันการควบคุมทรัพย์สินและการสนับสนุนอื่นๆ ด้วย

ทั้งนี้ HP ไม่แนะนำให้ใช้คุณสมบัติตัวล็อคไดรฟ์สำหรับผู้ใช้ที่ไม่มีความจำเป็นต้องใช้ระบบรักษาความปลอดภัยที่เข้มงวดเช่นนี้ ผู้ใช้ในกลุ่มนี้รวมถึงผู้ใช้คอมพิวเตอร์ส่วนบุคคล หรือผู้ใช้ที่ไม่ได้เก็บข้อมูลสำคัญไว้ในฮาร์ดไดรฟ์เป็นประจำ สำหรับผู้ใช้เหล่านี้ การสูญเสียฮาร์ดไดรฟ์เนื่องจากการลืมรหัสผ่านทั้งสองชุดจะไม่คุ้มกับการใช้ตัวล็อคไดรฟ์เพื่อป้องกันข้อมูล คุณสามารถจำกัดการเข้าใช้โปรแกรมการตั้งค่าคอมพิวเตอร์และตัวล็อคไดรฟ์ด้วยรหัสผ่านสำหรับการตั้งค่า โดยผู้ดูแลระบบสามารถกำหนดรหัสผ่านสำหรับการตั้งค่าขึ้นโดยไม่ให้ผู้ใช้อื่นทราบรหัสผ่านนั้น ก็จะสามารถจำกัดการใช้งานตัวล็อคไดรฟ์ได้

เซ็นเซอร์ Smart Cover

เซ็นเซอร์ Cover Removal ซึ่งมีให้ในบางรุ่น เป็นเทคโนโลยีการผสมผสานระหว่างฮาร์ดแวร์และซอฟต์แวร์ ซึ่งใช้สำหรับการแจ้งเมื่อมีการเปิดฝาครอบหรือแผงปิดด้านข้างของเครื่อง โดยมีระดับการป้องกันสามระดับ ดังที่จะอธิบายในตารางต่อไปนี้

ตาราง 11-2 ระดับการป้องกันด้วยเซ็นเซอร์ Smart Cover

ระดับ	การตั้งค่า	คำอธิบาย
ระดับ 0	Disabled	ไม่ใช้งานเซ็นเซอร์ Smart Cover (ดีฟอลต์)
ระดับ 1	Notify User	เมื่อเริ่มระบบคอมพิวเตอร์ใหม่ หน้าจอจะแสดงข้อความแจ้งว่ามีการเปิดฝาครอบเครื่องหรือแผงปิดด้านข้าง
ระดับ 2	Setup Password	เมื่อเริ่มระบบคอมพิวเตอร์ใหม่ หน้าจอจะแสดงข้อความแจ้งว่ามีการเปิดฝาครอบเครื่องหรือแผงปิดด้านข้าง คุณจะต้องป้อนรหัสผ่านสำหรับการตั้งค่าเพื่อดำเนินการต่อ

หมายเหตุ: การตั้งค่าเหล่านี้สามารถเปลี่ยนแปลงได้โดยใช้โปรแกรมการตั้งค่าคอมพิวเตอร์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าคอมพิวเตอร์ โปรดดูที่ *คู่มือยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)*

การกำหนดระดับการป้องกันของเซ็นเซอร์ Smart Cover

ในการกำหนดระดับการป้องกันของเซ็นเซอร์ Smart Cover โปรดปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

   หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี
3. เลือก **Security** > **Smart Cover** > **Cover Removal Sensor** และเลือกระดับความปลอดภัยที่ต้องการ
4. ก่อนที่จะออกจากโปรแกรม ให้คลิกที่ **File** > **Save Changes and Exit**

ล็อค Smart Cover

Smart Cover Lock เป็นล็อคฝาปิดเครื่องที่ควบคุมด้วยซอฟต์แวร์ซึ่งมีอยู่ในคอมพิวเตอร์ HP บางรุ่น ล็อคนี้จะป้องกันการเข้าถึงส่วนประกอบภายในเครื่องโดยไม่ได้รับอนุญาต คอมพิวเตอร์จะส่งถึงมือคุณโดยที่ล็อค SmartCover อยู่ในตำแหน่งปลดล็อค

△ **ข้อควรระวัง:** เพื่อการป้องกันสูงสุด โปรดตรวจสอบว่าคุณได้กำหนดรหัสผ่านสำหรับการตั้งค่าแล้ว รหัสผ่านสำหรับการตั้งค่าจะป้องกันการเข้าใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์โดยไม่ได้รับอนุญาต

หมายเหตุ: ล็อค Smart Cover มีให้เลือกในแบบตัวเลือกสำหรับเครื่องบางรุ่น

การล็อคด้วยล็อค Smart Cover

ในการใช้ล็อค Smart Cover ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เลือก **Security** > **Smart Cover** > **Cover Lock** > **Lock option**
4. ก่อนที่จะออกจากโปรแกรม ให้คลิกที่ **File** > **Save Changes and Exit**

การปลดล็อค Smart Cover

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows ให้คลิก **Start** > **Shut Down** > **Restart**
2. ทันทีที่คอมพิวเตอร์เปิด ให้กดฮ็อตคีย์ F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการ เพื่อเข้าสู่การตั้งค่าคอมพิวเตอร์ กด Enter หากต้องการข้ามหน้าจอเริ่มต้น

หมายเหตุ: หากคุณไม่ได้กด F10 ภายในเวลาที่เหมาะสม คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่ และกด F10 ก่อนที่คอมพิวเตอร์จะบูตเข้าสู่ระบบปฏิบัติการเพื่อเข้าถึงยูทิลิตี

3. เลือก **Security** > **Smart Cover** > **Cover Lock** > **Unlock**
4. ก่อนที่จะออกจากโปรแกรม ให้คลิกที่ **File** > **Save Changes and Exit**

การใช้กุญแจ Smart Cover FailSafe

หากคุณใช้งานล็อค Smart Cover และไม่สามารถป้อนรหัสผ่านเพื่อยกเลิกการทำงานของล็อค คุณจะต้องใช้กุญแจ Smart Cover FailSafe เพื่อเปิดฝาเครื่อง คุณจะต้องใช้กุญแจในกรณีต่อไปนี้:

- ไฟดับ
- การเริ่มระบบล้มเหลว
- ส่วนประกอบของ PC (เช่น โปรเซสเซอร์หรือแหล่งจ่ายไฟ) ล้มเหลว
- ลืมรหัสผ่าน

△ **ข้อควรระวัง:** กุญแจ Smart Cover FailSafe เป็นเครื่องมือพิเศษที่สามารถสั่งซื้อได้จาก HP เตรียมตัวให้พร้อม สั่งซื้อกุญแจนี้จากผู้ให้บริการหรือตัวแทนจำหน่ายที่ได้รับอนุญาตก่อนที่คุณจะต้องใช้

ในการรับกุญแจ FailSafe ให้ดำเนินการอย่างใดอย่างหนึ่งต่อไปนี้:

- ติดต่อผู้ให้บริการหรือตัวแทนจำหน่ายที่ได้รับอนุญาตของ HP
- ติดต่อหมายเลขที่เหมาะสมในใบรับประกัน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้กุญแจ Smart Cover FailSafe โปรดดู *คู่มืออ้างอิงฮาร์ดแวร์*

การล็อคด้วยสายเคเบิล

แผงด้านหลังของเครื่องคอมพิวเตอร์ (บางรุ่น) สามารถรองรับการล็อคด้วยสายเคเบิลเพื่อยึดคอมพิวเตอร์ไว้กับที่

สำหรับคำแนะนำพร้อมภาพประกอบ โปรดดูที่ *คู่มืออ้างอิงฮาร์ดแวร์*

เทคโนโลยีตรวจสอบลายนิ้วมือ

เพื่อตัดปัญหาในการป้อนรหัสผ่านสำหรับผู้ใช้ เทคโนโลยีตรวจสอบลายนิ้วมือของ HP ได้เพิ่มความปลอดภัยให้กับระบบเน็ตเวิร์ก ทำให้กระบวนการล็อกอินง่ายขึ้น และลดค่าใช้จ่ายที่เกี่ยวข้องกับการจัดการเน็ตเวิร์กขององค์กรลง โดยมีราคาที่เหมาะสม ไม่ใช่เฉพาะสำหรับองค์กรที่ต้องการการป้องกันด้วยเทคโนโลยีระดับสูงอีกต่อไป

หมายเหตุ: การรองรับเทคโนโลยีตรวจสอบลายนิ้วมือจะต่างกันไปในแต่ละรุ่น

การแจ้งข้อผิดพลาดและการเรียกคืนข้อมูลระบบ

การแจ้งข้อผิดพลาดและการเรียกคืนข้อมูลระบบเป็นการผสมผสานเทคโนโลยีของฮาร์ดแวร์และซอฟต์แวร์เข้าด้วยกันเพื่อป้องกันการสูญเสียข้อมูลสำคัญ และลดเวลาซ่อมบำรุงที่ไม่ได้วางแผนไว้

หากคอมพิวเตอร์เชื่อมต่ออยู่กับเน็ตเวิร์กที่ควบคุมโดย HP Client Manager คอมพิวเตอร์จะแจ้งข้อผิดพลาดไปยังแอปพลิเคชันการจัดการเน็ตเวิร์กด้วย ซอฟต์แวร์ HP Client Manager ยังให้คุณสามารถกำหนดตารางเวลาการวินิจฉัยระยะไกล เพื่อรันคอมพิวเตอร์ทั้งหมดที่อยู่ภายใต้การควบคุม และสร้างรายงานสรุปสำหรับการทดสอบที่ล้มเหลว

ระบบป้องกันไดรฟ์

ระบบป้องกันไดรฟ์ (DPS) เป็นเครื่องมือในการวินิจฉัยที่มีอยู่ในฮาร์ดไดรฟ์ที่ติดตั้งในเครื่องคอมพิวเตอร์ HP บางรุ่น DPS ได้รับการออกแบบมาเพื่อช่วยวินิจฉัยปัญหาที่อาจส่งผลให้ต้องมีการเปลี่ยนฮาร์ดไดรฟ์โดยไม่อยู่ในเงื่อนไขการรับประกัน

ในการผลิตเครื่องคอมพิวเตอร์ HP จะมีการทดสอบฮาร์ดไดรฟ์ที่ถูกติดตั้งด้วย DPS และจะมีการบันทึกข้อมูลสำคัญไว้อย่างถาวรในไดรฟ์นั้นๆ และทุกครั้งที่รัน DPS ผลการทดสอบจะถูกบันทึกลงในฮาร์ดไดรฟ์ ผู้ให้บริการของคุณสามารถใช้ข้อมูลนี้เพื่อช่วยวินิจฉัยปัญหาที่ทำให้คุณต้องรันซอฟต์แวร์ DPS โปรดดูคำแนะนำเกี่ยวกับการใช้ DPS ใน *คู่มือการแก้ไขปัญหา*

แหล่งจ่ายไฟที่ทนต่อไฟกระชาก

แหล่งจ่ายไฟภายในที่ทนต่อกระแสไฟฟ้ากระชากจะให้ความมั่นใจมากขึ้นเมื่อคอมพิวเตอร์พบการกระชากของกระแสไฟซึ่งไม่อาจคาดการณ์ได้ แหล่งจ่ายไฟนี้ได้รับการปรับระดับเพื่อให้ทนต่อกระแสไฟฟ้ากระชากถึง 2000 โวลต์โดยไม่ทำให้เกิดการขัดข้องหรือสูญเสียข้อมูล

เซ็นเซอร์อุณหภูมิ

เซ็นเซอร์อุณหภูมิเป็นคุณสมบัติด้านฮาร์ดแวร์และซอฟต์แวร์ที่ติดตามอุณหภูมิภายในของเครื่องคอมพิวเตอร์ โดยคุณสมบัตินี้จะแสดงข้อความเตือนเมื่ออุณหภูมิไม่อยู่ในช่วงปกติ ซึ่งทำให้คุณมีเวลาดำเนินการตามความเหมาะสมก่อนที่ส่วนประกอบภายในจะเสียหายหรือก่อนที่ข้อมูลจะสูญหายไป

ข้อควรระวัง: สภาวะอุณหภูมิสูงอาจสร้างความเสียหายแก่ระบบหรือทำให้ข้อมูลสูญหาย

ดัชนี