



คู่มือการจัดการเดสก์ท็อป

Business Desktops

หมายเลขประจำสินค้าของเอกสาร:312947-281

มีนาคม 2003

คู่มือนี้จะแสดงคำอธิบายและคำแนะนำเกี่ยวกับการใช้คุณสมบัติการรักษาความปลอดภัยและการจัดการอัจฉริยะซึ่งติดตั้งไว้ในคอมพิวเตอร์บางรุ่น

© 2002 บริษัท Hewlett-Packard

© 2002 บริษัท Hewlett-Packard Development, L.P.

HP, Hewlett Packard, และโลโก้ Hewlett-Packard เป็นเครื่องหมายการค้าของบริษัท Hewlett-Packard ในประเทศสหรัฐอเมริกา และประเทศอื่นๆ

Compaq และ โลโก้ Compaq เป็นเครื่องหมายการค้าของ Hewlett-Packard Development Company, L.P. ในประเทศสหรัฐอเมริกา และประเทศอื่นๆ

Microsoft, MS-DOS, Windows และ Windows NT เป็นเครื่องหมายการค้าของ Microsoft Corporation ในประเทศสหรัฐอเมริกา และประเทศอื่นๆ

ชื่อผลิตภัณฑ์อื่นๆ ที่กล่าวถึงในที่นี้อาจเป็นเครื่องหมายการค้าของบริษัทที่เป็นเจ้าของ

Hewlett-Packard Company ไม่ต้องการรับผิดชอบต่อความผิดพลาดทางเทคนิค การแก้ไข การละเลย หากมีอยู่ในที่นี้ หรือต่อความเสียหายอันเกิดจากอุบัติเหตุ หรือเป็นสาเหตุจากประสิทธิภาพหรือการใช้วัสดุนี้ ข้อมูลในเอกสารนี้จัดทำให้ "ตามที่ เป็นอยู่" โดยไม่มีการรับประกันไม่ว่าในเรื่องใดๆ รวมถึง แต่ไม่จำกัดเฉพาะ กับการรับประกันโดยนัยของสินค้า และความเหมาะสมสำหรับจุดมุ่งหมายเฉพาะอย่าง และสามารถเปลี่ยนแปลงได้โดยไม่ต้องแจ้งให้ทราบล่วงหน้า การรับประกันสำหรับผลิตภัณฑ์ของ HP จะกำหนดไว้ในข้อความการรับประกันอย่างจำกัดที่ให้มาพร้อมกับผลิตภัณฑ์ ข้อความในที่นี้จะไม่มีผลเป็นการรับประกันเพิ่มเติมใดๆ ทั้งสิ้น เอกสารนี้ประกอบไปด้วยข้อมูลเฉพาะอย่างซึ่งได้รับการคุ้มครองโดยลิขสิทธิ์ ห้าม นำเอกสารนี้ และบางส่วนของเอกสารนี้ ไปทำการถ่ายเอกสาร ทำซ้ำ หรือแปลไป เป็นภาษาอื่นๆ โดยไม่ได้รับอนุญาตเป็นลายลักษณ์อักษรจากบริษัท Hewlett-Packard



คำเตือน:ข้อความในลักษณะนี้หมายถึง การไม่ปฏิบัติตามอาจเป็นผลให้เกิด การบาดเจ็บหรือเสียชีวิต



ข้อควรระวัง:ข้อความในลักษณะนี้หมายถึง การไม่ปฏิบัติตามอาจเป็นผลให้ เกิดความเสียหายต่ออุปกรณ์หรือสูญเสียข้อมูล

คู่มือการจัดการเดสก์ทอป

Business Desktops

พิมพ์ครั้งแรก (มีนาคม 2003)

หมายเลขประจำสินค้าของเอกสาร:312947-281

สารบัญ

คู่มือ การ จัด การ เดสก์ทอป

การ ตั้ง ค่า เริ่ม ต้น และ การ เริ่ม ใช้ งาน	2
การ ติด ตั้ง ระบบ ระยะ ไกล.....	3
การอัปเดตและ การ จัดการ ซอฟต์แวร์	4
Altiris eXpress	4
Altiris eXpress PC Transplant Pro	5
ซอฟต์แวร์ การ จัด การ ไคล เอนต์ ของ HP	6
การ จัด การ ซอฟต์แวร์ ของ ระบบ	6
HP Proactive Notification (HPPN)	7
ActiveUpdate	7
การ แฟลช ROM	8
การ แฟลช ROM ระยะ ไกล.....	8
บล็อก การบูต ROM FailSafe.	9
การถอดแบบการ ตั้ง ค่า	11
ปุ่ม เปิด ปิด แบบ สอง สถานะ	12
การ จัดการ พลังงาน	13
ไซท์เว็ลด์ ไซด์เว็ป	14
ความ ร่วม มือ และ พันธมิตร	14
การ ควบคุม ทรัพย์สิน และ การ รักษา ความ ปลอดภัย	15
การ ป้องกัน ด้วย รหัส ผ่าน.....	18
การ กำหนด รหัส ผ่าน สำหรับ การ ตั้ง ค่า โดย ใช้ โปรแกรม การ ตั้ง ค่า คอมพิวเตอร์.....	19
การ กำหนด รหัส ผ่าน เมื่อ เปิด เครื่อง โดย ใช้ โปรแกรม การ ตั้ง ค่า คอมพิวเตอร์	20

DriveLock	24
Smart Cover Sensor	26
Smart Cover Lock	27
Master Boot Record Security	30
ก่อนที่จะแบ่งพาร์ติชันหรือฟอร์แมตดิสก์ที่ใช้บูตในปัจจุบัน	32
การล็อคด้วยสายเคเบิล	32
เทคโนโลยีตรวจสอบลายนิ้วมือ	33
การแจ้งข้อผิดพลาดและการเรียกคืนข้อมูลระบบ	34
ระบบป้องกันไครฟ์	34
แหล่งจ่ายไฟที่ทนต่อไฟกระชาก	34
เซ็นเซอร์อุณหภูมิ	34

ดรรชนี

คู่มือการจัดการเดสก์ทอป

ระบบจัดการอัจฉริยะ Intelligent Manageability ของ HP เป็นโซลูชันมาตรฐานสำหรับการจัดการและควบคุมระบบเดสก์ทอป เวิร์กสเตชัน และคอมพิวเตอร์โน้ตบุ๊ก ในสภาวะการทำงานในเน็ตเวิร์ค HP เป็นผู้ริเริ่มระบบจัดการเดสก์ทอปในปี 1995 ด้วยการเปิดตัว คอมพิวเตอร์ที่มีระบบการจัดการเดสก์ทอปอย่างเต็มรูปแบบเป็นครั้งแรก HP เป็นเจ้าของสิทธิบัตรเทคโนโลยีระบบการจัดการนี้ นับแต่นั้นมา HP ก็ได้กลายเป็นผู้นำในการพัฒนามาตรฐานและโครงสร้างพื้นฐานที่จำเป็นต่อการใช้งาน, การตั้งค่า และการจัดการเดสก์ทอป, เวิร์กสเตชัน และคอมพิวเตอร์โน้ตบุ๊กอย่างมีประสิทธิภาพ HP ได้ร่วมมือกับผู้ให้โซลูชันซอฟต์แวร์ชั้นนำในอุตสาหกรรมอย่างใกล้ชิดเพื่อสร้างความมั่นใจในการใช้งานร่วมกันระหว่างระบบจัดการอัจฉริยะและผลิตภัณฑ์เหล่านี้ ระบบจัดการอัจฉริยะนี้จึงเป็นแง่มุมสำคัญของพันธมิตรสัญญาที่เรามีให้คุณ ด้วยโซลูชัน PC Lifecycle ซึ่งจะช่วยเหลือคุณในสี่ขั้นตอนหลักของวงจรการใช้งานระบบคอมพิวเตอร์ อันได้แก่การวางแผน การนำไปใช้ การจัดการ และการเปลี่ยนแปลง

คู่มือนี้เป็นการสรุปความสามารถและคุณสมบัติขององค์ประกอบหลัก 7 ประการของการจัดการเดสก์ทอป

- การตั้งค่าเริ่มต้นและการเริ่มใช้งาน
- การติดตั้งระบบระยะไกล
- การอัปเดตและการจัดการซอฟต์แวร์
- การแฟลช ROM
- ความร่วมมือและพันธมิตร
- การควบคุมทรัพย์สินและการรักษาความปลอดภัย
- การแจ้งข้อผิดพลาดและการเรียกคืนข้อมูลระบบ



การสนับสนุนคุณสมบัติต่างๆ ที่กล่าวถึงในคู่มือนี้อาจแตกต่างกันไปในเครื่องคอมพิวเตอร์และซอฟต์แวร์แต่ละรุ่น

การตั้งค่าเริ่มต้นและการเริ่มใช้งาน

เครื่องคอมพิวเตอร์ของคุณจะมีการติดตั้งอิมเมจของซอฟต์แวร์ระบบไว้แล้ว หลังจากกระบวนการ "แยก" ซอฟต์แวร์ เครื่องคอมพิวเตอร์ก็จะพร้อมสำหรับการใช้งาน

คุณอาจต้องการแทนที่อิมเมจของซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าด้วยระบบและซอฟต์แวร์ชุดที่กำหนดขึ้นเอง มีหลายวิธีที่สามารถทำได้ เช่น:

- ติดตั้งซอฟต์แวร์เพิ่มเติมหลังจากที่แยกอิมเมจของซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าแล้ว
- การใช้เครื่องมือติดตั้งซอฟต์แวร์ เช่น Altiris eXpress เพื่อแทนที่ซอฟต์แวร์ที่ติดตั้งไว้ล่วงหน้าด้วยอิมเมจของซอฟต์แวร์ตามที่คุณเลือก
- การใช้กระบวนการลอกแบบดิสก์เพื่อคัดลอกเนื้อหาของฮาร์ดไดรฟ์หนึ่งไปยังอีกไดรฟ์หนึ่ง

วิธีการเริ่มต้นใช้งานที่ดีที่สุดขึ้นอยู่กับสถานะและกระบวนการด้านสารสนเทศของคุณ หัวข้อ PC Deployment ในเว็บไซต์ Solutions and Services

(<http://www.compaq.com/solutions/pcsolutions>) จะมีข้อมูลที่สามารถช่วยให้คุณเลือกวิธีการเริ่มต้นใช้งานที่เหมาะสมที่สุด

ซีดี *Restore Plus!* การตั้งค่าจากระบบ และฮาร์ดแวร์ที่พร้อมสำหรับ ACPI จะมีความช่วยเหลือสำหรับการเรียกคืนซอฟต์แวร์ระบบการจัดการการตั้งค่าและการแก้ไขปัญหา รวมทั้งการจัดการพลังงาน

การติดตั้งระบบระยะไกล

การติดตั้งระบบระยะไกลช่วยให้คุณเริ่มต้นและติดตั้งระบบโดยใช้ซอฟต์แวร์และการตั้งค่าที่อยู่ในเซิร์ฟเวอร์ของระบบเครือข่าย โดยการเริ่มต้น Preboot Execution Environment (PXE) คุณสมบัตินี้เป็นเครื่องมือในการติดตั้งระบบและการตั้งค่า และสามารถใช้ในการทำงานต่อไปนี้:

- การฟอร์แมตฮาร์ดไดรฟ์
- การเริ่มต้นใช้งานอิมเมจของซอฟต์แวร์ในเครื่องคอมพิวเตอร์ส่วนบุคคลตั้งแต่หนึ่งเครื่องขึ้นไป
- การติดตั้งแอปพลิเคชันหรือไดรเวอร์
- การอัปเดตระบบปฏิบัติการ, แอปพลิเคชัน หรือไดรเวอร์

เมื่อต้องการเริ่มต้นการติดตั้งระยะไกล ให้กด **F12** เมื่อข้อความ F12 = Network Service Boot ปรากฏขึ้นที่มุมขวาล่างของหน้าจอโลโก้ HP จากนั้น ปฏิบัติตามคำแนะนำบนหน้าจอเพื่อ ดำเนินการต่อ

HP และ Altiris, Inc. ได้ร่วมมือกันในการพัฒนาเครื่องมือที่จะช่วยให้การใช้งานและการจัดการระบบคอมพิวเตอร์เป็นไปได้อย่างขึ้นและใช้เวลาน้อยลง อีกทั้งเพื่อลดค่าใช้จ่ายที่เกิดขึ้น และทำให้เครื่องคอมพิวเตอร์ของ HP เป็นเครื่องคอมพิวเตอร์ไคลเอนต์ที่มีความสามารถในการจัดการสูงสุดสำหรับสภาวะการทำงานในองค์กร

การอัปเดตและการจัดการซอฟต์แวร์

HP มีเครื่องมือหลายอย่างในการจัดการและการอัปเดตซอฟต์แวร์ในเครื่องเดสก์ท็อปและเวิร์กสเตชัน เช่น Altiris eXpress; Altiris eXpress PC Transplant Pro; HP Client Manager Software, Altiris eXpress solution; System Software Manager; HP Proactive Notification และ ActiveUpdate

Altiris eXpress

HP และ Altiris ได้ขยายความร่วมมือในการให้บริการโซลูชันชั้นนำของอุตสาหกรรมซึ่งลดความซับซ้อนในการจัดการฮาร์ดแวร์และซอฟต์แวร์สำหรับเดสก์ท็อป, โน้ตบุ๊ก, อุปกรณ์พกพา และเซิร์ฟเวอร์ตลอดอายุการใช้งาน Altiris eXpress ช่วยให้ผู้บริหารระบบสามารถสร้างและใช้งานอิมเมจของซอฟต์แวร์ที่เป็นมาตรฐานองค์กรที่สามารถกำหนดขึ้นเองได้อย่างรวดเร็วสำหรับเครื่องคอมพิวเตอร์ในเน็ตเวิร์กตั้งแต่หนึ่งเครื่องขึ้นไปโดยใช้อินเทอร์เฟซ ซึ่งการใช้งานจะง่ายพอๆ กับโปรแกรม Windows Explorer Altiris eXpress สนับสนุน Preboot Execution Environment (PXE) เมื่อใช้ Altiris eXpress และคุณสมบัติการติดตั้งระบบระยะไกลของHP ผู้บริหารระบบจะไม่ต้องเข้าทำงานที่เครื่องคอมพิวเตอร์แต่ละเครื่องเพื่อเริ่มใช้อิมเมจของซอฟต์แวร์อีกเลย

โซลูชันของ Altiris eXpress มอบวิธีที่มีประสิทธิภาพและได้ผลในการทำให้ขั้นตอนและพื้นที่ที่มีปัญหาภายในสถานะ IT ของคุณเป็นไปโดยอัตโนมัติ โครงสร้างพื้นฐานทางเว็บของ Altiris eXpress ช่วยให้คุณสามารถจัดการระบบของคุณได้ทุกที่ ทุกเวลา แม้กระทั่งจากเครื่องคอมพิวเตอร์พกพา iPAQ!

โซลูชันของ Altiris eXpress มีรูปแบบเป็น โมดูลาร์และสามารถเพิ่มเติมเพื่อขยายขอบเขตความต้องการในระดับ workgroup ไปสู่ระดับองค์กร ทั้งนี้ โดยที่โซลูชันดังกล่าวได้รวมเข้ากับเครื่องมือการจัดการไคลเอนต์ของธุรกิจอื่น และเป็นส่วนเสริมของ Microsoft BackOffice/SMS

โซลูชันส่วนขยายของ Altiris eXpress มุ่งเน้นขอบเขตด้าน IT ที่สำคัญ 4 ส่วน คือ:

- การนำไปใช้และการเปลี่ยนรุ่น
- การจัดการซอฟต์แวร์และระบบปฏิบัติการ
- การจัดการรายการสิ่งของและทรัพย์สิน
- การช่วยเหลือและการแก้ไขปัญหา

Altiris eXpress จะสามารถติดตั้งอิมเมจของซิสต์ที่ประกอบด้วยระบบปฏิบัติการ แอปพลิเคชัน และ โปรแกรมโคลนของ Altiris eXpress ภายในเวลาเพียงไม่กี่นาทิต โดยไม่ต้องใช้แผ่นดิสเก็ตต์สำหรับบูตแยกต่างหาก ด้วย Altiris eXpress ผู้บริหารระบบเครือข่ายจะสามารถ:

- สร้างอิมเมจใหม่หรือแก้ไขอิมเมจเดิม หรือลอกแบบเครื่องคอมพิวเตอร์ในเน็ตเวิร์กซึ่งอาจมีอิมเมจที่เหมาะสมที่สุด
- สร้างอิมเมจของซิสต์ที่กำหนดเองเป็นจำนวนเท่าใดก็ได้ สำหรับเวิร์กกรุ๊ปหลายแบบ
- แก้ไขไฟล์อิมเมจ เปลี่ยนแปลงไฟล์โดยไม่ต้องเริ่มต้นใหม่ทุกครั้ง ซึ่งทำได้เช่นนี้ เป็นเพราะ Altiris eXpress เก็บไฟล์ในรูปแบบเดิม คือ NTFS, FAT16 หรือ FAT32
- สร้าง “New PC Event” ซึ่งก็คือ Script ที่จะทำงานโดยอัตโนมัติเมื่อมีการเพิ่มเครื่องคอมพิวเตอร์ในเครือข่าย สคริปต์นี้อาจใช้ในการฟอร์แมตฮาร์ดไดรฟ์ แฟลช ROM BIOS และติดตั้งอิมเมจซอฟต์แวร์แบบมาตรฐาน
- กำหนดการทำงานกลุ่มเครื่องคอมพิวเตอร์

นอกจากนี้ Altiris eXpress ยังมีคุณสมบัติในการกระจายซอฟต์แวร์ซึ่งใช้งานง่าย คุณสามารถใช้ Altiris eXpress เพื่ออัปเดตระบบปฏิบัติการและซอฟต์แวร์จากคอนโซลส่วนกลาง เมื่อใช้ร่วมกับโปรแกรมจัดการซอฟต์แวร์ระบบ หรือ HP Client Manager Altiris eXpress ยังสามารถ อัปเดต ROM BIOS และซอฟต์แวร์ดีไวซ์ไดรเวอร์ได้อีกด้วย

หากต้องการข้อมูลเพิ่มเติม โปรดเยี่ยมชมเว็บไซต์

<http://www.compaq.com/easydeploy>

Altiris eXpress PC Transplant Pro

Altiris eXpress PC Transplant Pro ช่วยให้คุณสามารถเปลี่ยนรุ่นของเครื่องคอมพิวเตอร์ได้โดยไม่ต้องเปลี่ยนแปลงค่าใดๆ โดยจะรักษาการตั้งค่า การปรับแต่ง และข้อมูลเดิม ดังนั้นคุณสามารถเปลี่ยนรุ่นของเครื่องคอมพิวเตอร์จากเก่าเป็นใหม่ได้อย่างรวดเร็วและง่ายดาย การอัปเดตจะใช้เวลาเป็นนาทีแทนที่จะเป็นชั่วโมงหรือเป็นวัน โดยที่เดสก์ท็อปและแอปพลิเคชันจะใช้งานได้ตามที่ผู้ใช้ต้องการ

สำหรับรายละเอียดเพิ่มเติมเกี่ยวกับการดาวน์โหลดโปรแกรมสำหรับประเมินผลการทำงาน 30 วันแบบเต็มรูปแบบ โปรดเยี่ยมชมเว็บไซต์

<http://www.compaq.com/easydeploy>

ซอฟต์แวร์การจัดการไคลเอนต์ของ HP

ซอฟต์แวร์การจัดการไคลเอนต์ของ HP (HP CMS) ผนวกเทคโนโลยีระบบจัดการอัจฉริยะของ HP ไว้ใน Altiris eXpress เพื่อให้คุณสมบัติการจัดการฮาร์ดแวร์ที่ดีขึ้นสำหรับอุปกรณ์ของ HP ซึ่งรวมถึง:

- การดูรายละเอียดรายการฮาร์ดแวร์สำหรับการจัดการทรัพย์สิน
- การตรวจสอบและวินิจฉัยความสมบูรณ์ของเครื่องคอมพิวเตอร์
- การแจ้งการเปลี่ยนแปลงในสถานะการทำงานของฮาร์ดแวร์ได้อย่างทันท่วงที
- การรายงานรายละเอียดที่สำคัญๆ ของธุรกิจ เช่น เครื่องคอมพิวเตอร์ที่มีการแจ้งเตือนเกี่ยวกับอุณหภูมิ การแจ้งเตือนเกี่ยวกับหน่วยความจำ และอื่นๆ ที่สามารถเข้าถึงได้ทางเว็บ

■ การอัปเดตซอฟต์แวร์ระบบระยะไกล เช่น ดีไวซ์ไดรเวอร์ และ ROM BIOS สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการจัดการไคลเอนต์ของ HP โปรดเยี่ยมชมเว็บไซต์ <http://www.compaq.com/easydeploy>

การจัดการซอฟต์แวร์ของระบบ

การจัดการซอฟต์แวร์ระบบ (System Software Manager - SSM) เป็นยูทิลิตี้สำหรับการอัปเดตซอฟต์แวร์ของระบบในเครื่องคอมพิวเตอร์หลายเครื่องในคราวเดียวกัน เมื่อรันในเครื่องคอมพิวเตอร์ โปรแกรม SSM จะตรวจหาเวอร์ชันของฮาร์ดแวร์และซอฟต์แวร์ จากนั้นจะอัปเดตซอฟต์แวร์ที่เหมาะสมจากหน่วยเก็บข้อมูลกลาง ซึ่งเรียกว่าหน่วยเก็บไฟล์ เวอร์ชันของไดรเวอร์ ที่โปรแกรม SSM สนับสนุนจะถูกแสดงด้วยไอคอนพิเศษบนเว็บไซต์ดาวน์โหลดไดรเวอร์ และบนซิติ Support Software หากต้องการดาวน์โหลด ยูทิลิตี้ หรือรับข้อมูลเพิ่มเติมเกี่ยวกับ SSM โปรดเยี่ยมชมเว็บไซต์

<http://www.compaq.com/im/ssmwp.html>

HP Proactive Notification (HPPN)

โปรแกรม HP Proactive Notification ใช้เว็บไซต์ที่มีความปลอดภัย Subscriber's Choice เพื่อให้บริการต่อไปนี้อย่างอัตโนมัติและทันเหตุการณ์:

- ส่งอีเมลแจ้งการเปลี่ยนแปลงเกี่ยวกับผลิตภัณฑ์ (Product Change Notification - PCN) เพื่อแจ้งให้คุณทราบถึงการเปลี่ยนแปลงของฮาร์ดแวร์และซอฟต์แวร์ในคอมพิวเตอร์และเซิร์ฟเวอร์ส่วนใหญ่ที่ใช้ในธุรกิจล่วงหน้าถึง 60 วัน
- ส่งอีเมลซึ่งมีข่าวสารสำหรับลูกค้า (Customer Bulletins), คำแนะนำสำหรับลูกค้า (Customer Advisories), บันทึกสำหรับลูกค้า (Customer Notes), ข่าวสารด้านความปลอดภัย (Security Bulletins) และการแจ้งข่าวไดรเวอร์สำหรับคอมพิวเตอร์และเซิร์ฟเวอร์ส่วนใหญ่ที่ใช้ในธุรกิจ

คุณเป็นผู้ให้ข้อมูลของคุณเองเพื่อให้แน่ใจว่าคุณจะได้รับแต่ข้อมูลซึ่งตรงกับสภาพแวดล้อมทางเทคโนโลยีสารสนเทศของคุณ โปรดเยี่ยมชมเว็บไซต์ต่อไปนี เพื่อรับข้อมูลเพิ่มเติมเกี่ยวกับ HPPN และสร้างข้อมูลส่วนตัวของคุณ:

<http://www.hp.com/united-states/subscribe/>

ActiveUpdate

ActiveUpdate คือ แอปพลิเคชันที่ยึดไคลเอนต์เป็นหลักของ HP ไคลเอนต์ ActiveUpdate จะรันบนระบบของคุณและใช้รูปแบบที่ผู้ใช้กำหนดเองของคุณเพื่อความนำโหลดโปรแกรมอัปเดตซอฟต์แวร์สำหรับคอมพิวเตอร์และเซิร์ฟเวอร์ส่วนใหญ่ที่ใช้ในธุรกิจโดยอัตโนมัติและทันที่

โปรดเยี่ยมชมเว็บไซต์ต่อไปนี เพื่อรับข้อมูลเพิ่มเติมเกี่ยวกับ ActiveUpdate, ความนำโหลดแอปพลิเคชัน และ สร้างข้อมูลส่วนตัวของคุณ:

<http://www.compaq.com/activeupdate>

การแฟลช ROM

เครื่องคอมพิวเตอร์ของคุณมาพร้อมกับหน่วยความจำ ROM ที่สามารถกำหนดโปรแกรมใหม่ได้ (หน่วยความจำแบบอ่านได้อย่างเดียว) เมื่อคุณกำหนดรหัสผ่านสำหรับการตั้งค่าในยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10) คุณสามารถป้องกัน ROM จากการอัปเดตหรือแทนที่โดยไม่ได้ตั้งใจได้ ซึ่งเป็นสิ่งสำคัญในการทำงานที่สมบูรณ์ของ เครื่องคอมพิวเตอร์ หากคุณต้องการอัปเดต ROM คุณ สามารถ:

- สั่งซื้อดิสก์เก็ต ROMPaq™ จาก HP
- ดาวน์โหลดอิมเมจ ROMPaq ล่าสุดจาก <http://www.hp.com/support>



ข้อควรระวัง: เพื่อการป้องกัน ROM ในระดับสูงสุด โปรดตรวจสอบว่าคุณได้กำหนดรหัสผ่านสำหรับการตั้งค่าไว้ ซึ่งรหัสนี้จะป้องกันการอัปเดต ROM โดยไม่ได้รับอนุญาต ผู้บริหารระบบสามารถใช้ System Software Manager กำหนดรหัสผ่านสำหรับการตั้งค่าให้กับคอมพิวเตอร์เครื่องหนึ่งหรือหลายเครื่องได้พร้อมๆ กัน หากต้องการข้อมูลเพิ่มเติม โปรดเยี่ยมชมเว็บไซต์ <http://www.compaq.com/im/ssmwp.html>

การแฟลช ROM ระยะไกล

การแฟลช ROM จากระยะไกลจะช่วยให้ผู้บริหารระบบสามารถอัปเดต ROM ในเครื่องคอมพิวเตอร์ของ HP ระยะไกลได้อย่างปลอดภัย โดยตรงจากคอนโซลการจัดการเน็ตเวิร์กส่วนกลาง ซึ่งจะช่วยให้ผู้บริหารระบบ สามารถทำงานนี้ได้ จากระยะไกล กับเครื่องคอมพิวเตอร์หลายเครื่องในขณะเดียวกัน ทำให้การตั้งค่าระบบมีความสม่ำเสมอและมีการควบคุมอิมเมจ PC ROM ของ HP ผ่านเครือข่ายได้ดียิ่งขึ้น นอกจากนี้ยังส่งผลให้ประสิทธิภาพการทำงานสูงขึ้น และลดค่าใช้จ่ายในการครอบครองอีกด้วย



เครื่องคอมพิวเตอร์จะต้องเปิด หรือได้รับการเปิดระบบ โดยใช้การเปิดจากระยะไกล เพื่อที่จะใช้คุณสมบัติการแฟลช ROM จากระยะไกล

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการแฟลช ROM ระยะไกล โปรดดูในส่วน HP Client Manager Software หรือ System Software Manager ที่ <http://www.compaq.com/easydeploy>

บล็อกการบูต ROM FailSafe

บล็อกการบูต ROM FailSafe ช่วยให้สามารถเรียกคืนระบบในกรณีที่การแฟลช ROM ล้มเหลว ซึ่งเกิดขึ้นไม่บ่อยนัก เช่น กรณีเกิดไฟฟ้าดับ ขณะที่กำลังอัปเดต ROM บล็อกการบูตนี้เป็น ส่วนที่ได้รับการป้องกันการแฟลชใน ROM ซึ่งจะตรวจสอบการแฟลช ROM เมื่อเปิดเครื่องคอมพิวเตอร์

- หาก ROM ของระบบถูกต้อง ระบบจะเริ่มดำเนินการทำงานตามปกติ
- หาก ROM ไม่ผ่านการตรวจสอบ บล็อกการบูต FailSafe จะทำงานสนับสนุนเพียงพอที่จะเริ่มต้นระบบจากดิสเก็ตต์ ROMPaq ซึ่งจะตั้งโปรแกรม ROM ของระบบด้วยอิมเมจที่ถูกต้อง

“เมื่อบล็อกการบูตตรวจพบว่า ROM ของระบบไม่ถูกต้อง ไฟสถานะเปิดปิดของระบบจะกระพริบเป็นสีแดง 8 ครั้ง ห่างกันครั้งละหนึ่งวินาที แล้วเว้น 2 วินาที และจะมีเสียงเตือน 8 ครั้งติดต่อกัน ข้อความ Boot Block recovery mode จะปรากฏบนหน้าจอ (เฉพาะบางรุ่น)


ในการเรียกข้อมูลระบบกลับคืนหลังจากเข้าสู่โหมดเรียกคืนบล็อกการบูต ให้ดำเนินการตามขั้นตอนต่อไปนี้:

1. หากมีดิสเก็ตต์อยู่ในไดรฟ์ ให้นำดิสเก็ตต์ออกและปิดเครื่อง
2. ใส่แผ่นดิสเก็ตต์ ROMPaq เข้าในไดรฟ์
3. เปิดเครื่องคอมพิวเตอร์
4. หากไม่มีดิสเก็ตต์ ROMPaq ระบบจะให้คุณใส่แผ่นดิสเก็ตต์และเริ่มระบบใหม่
5. หากมีการกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ ไฟสัญญาณ Caps Lock จะติดและระบบจะให้คุณใส่รหัสผ่าน
6. ป้อนรหัสผ่านสำหรับการตั้งค่า
7. หากระบบสามารถเริ่มต้นจากแผ่นดิสเก็ตต์ และตั้งโปรแกรม ROM ได้สำเร็จ ไฟสัญญาณทั้งสามดวงบนแป้นพิมพ์จะสว่างขึ้น และระบบจะส่งสัญญาณเสียงที่เบากว่าๆ ค้างขึ้น เพื่อแจ้งว่าการดำเนินการเสร็จสมบูรณ์
8. นำแผ่นดิสเก็ตต์ออกและปิดเครื่อง
9. เปิดเครื่องอีกครั้งเพื่อเริ่มดำเนินการทำงาน

ตารางต่อไปนี้จะแสดงรูปแบบสัญญาณไฟบนแป้นพิมพ์รูปแบบต่างๆ จากบล็อกการบูต (เมื่อต่อแป้นพิมพ์แบบ PS/2 เข้ากับเครื่อง) และอธิบายความหมายและการปฏิบัติที่สัมพันธ์กับรูปแบบนั้น

รูปแบบสัญญาณไฟบนแป้นพิมพ์ที่บล็อกการบูต ROM ใช้

โหมด Failsafe Boot Block	สีของไฟ สัญญาณบน แป้นพิมพ์	แป้นพิมพ์ ลักษณะของ สัญญาณไฟ	สภาวะ/ข้อความ
Num Lock	เขียว	สว่าง	ไม่มีแผ่นดิสเก็ตต์ ROMPaq หรือมีแต่ไม่ถูกต้อง หรือไดรฟ์ไม่พร้อมทำงาน
Caps Lock	เขียว	สว่าง	บ่อนรหัสผ่าน
Num, Caps, Scroll Lock	เขียว	สว่างและดับ 2 ครั้ง (พร้อมด้วย สัญญาณเสียงยาว 1 ครั้งและสั้น 3 ครั้ง)	การแฟลช ROM ล้มเหลว
Num, Caps, Scroll Lock	เขียว	สว่าง	การแฟลชบล็อกการบูต ROM เสร็จสมบูรณ์ ปิดเครื่อง แล้วเปิดเครื่องอีกครั้งเพื่อรีบูต

 สัญญาณไฟเพื่อการวินิจฉัยจะไม่กะพริบบนแป้นพิมพ์แบบ USB

การถอดแบบการตั้งค่า

วิธีนี้ช่วยให้ผู้บริหารระบบสามารถคัดลอกการตั้งค่าของเครื่องคอมพิวเตอร์ไปยังเครื่องคอมพิวเตอร์อื่นซึ่งเป็นรุ่นเดียวกันได้อย่างง่ายดาย ซึ่งทำให้การตั้งค่าในระบบคอมพิวเตอร์หลายเครื่องเป็นไปอย่างรวดเร็วและสอดคล้องกันมากขึ้น การถอดแบบการตั้งค่า:

1. เข้าสู่เมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
2. คลิก **File > Save to Diskette** ปฏิบัติตามคำแนะนำบนหน้าจอ



ต้องใช้ดิสเก็ตต์ไดรฟ์หรืออุปกรณ์สื่อข้อมูลแฟลชแบบ USB ที่สนับสนุน เช่น DiskOnKey

3. ในการจำลองค่า ให้คลิก **File > Restore from Diskette** และปฏิบัติตามคำแนะนำบนหน้าจอ

Altiris eXpress, System Software Manager และ PC Transplant จะช่วยให้การคัดลอกการตั้งค่าและค่าเฉพาะต่างๆ จากคอมพิวเตอร์เครื่องหนึ่งไปยังอีกเครื่องหนึ่งหรือหลายเครื่องทำได้โดยง่าย หากต้องการข้อมูลเพิ่มเติม โปรดเยี่ยมชมเว็บไซต์ <http://www.compaq.com/easydeploy>

ปุ่มเปิดปิดแบบสองสถานะ

เมื่อใช้คุณสมบัติ Advanced Configuration and Power Interface (ACPI) ในระบบปฏิบัติการ Windows 98, Windows 2000, และ Windows XP ปุ่มเปิดปิดจะสามารถทำงานเป็นปุ่มเปิด/ปิดตามปกติหรือเป็นปุ่มพักการทำงานก็ได้ คุณสมบัติการพักการทำงานมีได้เป็นการปิด เครื่องคอมพิวเตอร์อย่างสมบูรณ์ แต่จะทำให้เครื่องคอมพิวเตอร์เข้าสู่โหมดสแตนด์บายซึ่งใช้พลังงานน้อย ซึ่งทำให้คุณสามารถหยุดการทำงานของเครื่องโดยไม่ต้องปิดแอปพลิเคชันต่างๆ และสามารถกลับมาใช้งานในสถานะเดิมได้อย่างรวดเร็วโดยไม่สูญเสียข้อมูล

ในการเปลี่ยนการตั้งค่าปุ่มเปิดปิด ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. ใน Windows 2000 ให้คลิกปุ่ม **Start** แล้วเลือก **Settings > Control Panel > Power Options**

ใน Windows XP ให้คลิกปุ่ม **Start Button**, แล้วเลือก **Control Panel > Performance and Maintenance > Power Options**

2. ใน **Power Options Properties** ให้เลือกแถบ **Advanced**

3. ในส่วน **Power Button** ให้เลือกการตั้งค่าปุ่มเปิดปิดตามต้องการ

หลังจากที่ตั้งค่าปุ่มเปิดปิดให้ทำงานเป็นปุ่มพักการทำงานแล้ว ให้กดปุ่มเปิดปิดเพื่อนำคอมพิวเตอร์เข้าสู่สถานะการใช้พลังงานน้อย (พักการทำงาน) กดปุ่มอีกครั้งเพื่อออกจากสถานะพักการทำงานและกลับสู่การใช้พลังงานเต็มอัตรา เมื่อต้องการปิดเครื่องคอมพิวเตอร์โดยสมบูรณ์ ให้กดปุ่มเปิดปิดค้างไว้เป็นเวลา 4 วินาที



ข้อควรระวัง:อย่าใช้ปุ่มเปิดปิดเพื่อปิดเครื่อง เว้นแต่ในกรณีที่ระบบไม่ตอบสนองต่อคำสั่ง การปิดเครื่องโดยไม่ผ่านระบบปฏิบัติการอาจทำให้ฮาร์ดไดรฟ์เสียหายหรือสูญเสียข้อมูล

การจัดการพลังงาน

การจัดการพลังงานเป็นคุณสมบัติที่ช่วยประหยัดพลังงานโดยการปิดอุปกรณ์บางอย่างของเครื่องคอมพิวเตอร์ ในระหว่างที่ไม่ได้ใช้งาน เพื่อเป็นการประหยัดพลังงานโดยไม่ต้องปิดเครื่อง

เมื่อใช้คุณสมบัติ Advanced Configuration and Power Interface (ACPI) ในระบบปฏิบัติการ Windows 98, Windows 2000, Windows Millennium และ Windows XP คุณสามารถเปิดใช้คุณสมบัติ, กำหนดเวลา (ระยะเวลาที่อุปกรณ์ไม่มีการทำงานก่อนจะปิดอุปกรณ์) หรือ ระบุการใช้งานอุปกรณ์ โดยใช้ระบบปฏิบัติการ

1. ใน Windows 2000 ให้คลิกปุ่ม **Start** แล้วเลือก **Settings > Control Panel > Power Options**

ใน Windows XP ให้คลิกปุ่ม **Start Button**, แล้วเลือก **Control Panel > Performance and Maintenance > Power Options**

2. ใน **Power Options Properties** ให้เลือกแถบ **Power Schemes**
3. เลือกการตั้งค่าการใช้พลังงานตามต้องการ

ใช้ Display Properties เพื่อกำหนด แก๊งไข หรือยกเลิกการใช้การตั้งค่าโปรแกรมการจัดการพลังงานสำหรับจอภาพ ในการเข้าสู่ Display Properties ให้คลิกปุ่มขวาของเมาส์ที่เดสก์ทอปของ **Windows** แล้วเลือก **Properties**

ไซท์เว็ลด์ไวด์เว็บ

วิศวกรของ HP ได้ทดสอบและปรับปรุงซอฟต์แวร์ที่ HP และผู้ผลิตรายอื่นผลิตขึ้น และพัฒนาซอฟต์แวร์สนับสนุนสำหรับระบบปฏิบัติการเพื่อให้คุณมั่นใจถึงประสิทธิภาพ, ความเข้ากันได้ และเสถียรภาพสูงสุดสำหรับ เครื่องคอมพิวเตอร์ของ HP

เมื่อมีการเปลี่ยนไปยังระบบปฏิบัติการใหม่หรือระบบปฏิบัติการที่ปรับปรุงใหม่ จะต้องใช้ซอฟต์แวร์สนับสนุนที่ได้รับการออกแบบมาสำหรับระบบนั้น โดยเฉพาะหากคุณต้องการใช้ Microsoft Windows รุ่นต่างจากที่ติดตั้งไว้ในเครื่องคอมพิวเตอร์ คุณจะต้องติดตั้งไดรเวอร์และยูทิลิตี้ในเวอร์ชันที่ตรงกัน เพื่อให้แน่ใจว่าคุณสมบัติต่างๆ ได้รับการสนับสนุนและทำงานได้อย่างถูกต้อง

HP ช่วยให้การค้นหา, การเข้าใช้, การประเมิน และการติดตั้งซอฟต์แวร์สนับสนุนเวอร์ชันล่าสุดเป็นไปได้ง่ายขึ้น คุณสามารถดาวน์โหลดซอฟต์แวร์ได้จาก

<http://www.hp.com/support>

เว็บไซต์นี้ประกอบด้วยดีไวซ์ไดรเวอร์, ยูทิลิตี้ และอิมเมจของ ROM ที่แฟลชได้ในเวอร์ชันล่าสุด ซึ่งจำเป็นสำหรับใช้งานระบบปฏิบัติการ Microsoft Windows รุ่นล่าสุด ในเครื่องคอมพิวเตอร์ HP ของคุณ

ความร่วมมือและพันธมิตร

โซลูชันการจัดการของ HP ผนวกเอาการจัดการระบบอื่นๆ ไว้ด้วย และมีหลักการจากมาตรฐานต่างๆ เช่น:

- อินเทอร์เน็ตการจัดการเดสก์ทอป (DMI) 2.0
- เทคโนโลยี Wake on LAN
- ACPI
- SMBIOS
- การสนับสนุน Pre-boot Execution (PXE)

การควบคุมทรัพย์สินและการรักษาความปลอดภัย

คุณสมบัติการควบคุมทรัพย์สินได้รับการผนวกเข้ากับคอมพิวเตอร์เพื่อให้ข้อมูลการควบคุมทรัพย์สินที่สำคัญซึ่งสามารถจัดการได้โดยใช้ HP Insight Manager, HP Client Manager หรือแอปพลิเคชันการจัดการระบบอื่นๆ การทำงานร่วมกันของคุณสมบัติการควบคุมทรัพย์สินและผลิตภัณฑ์เหล่านี้ได้อย่างสมบูรณ์แบบโดยอัตโนมัติจะช่วยให้คุณเลือกเครื่องมือในการจัดการที่เหมาะสมกับสภาวะการทำงานของคุณมากที่สุด และสามารถใช้ประโยชน์จากเครื่องมือที่มีอยู่เดิมได้อย่างคุ้มค่า

นอกจากนี้ HP ยังมีโซลูชันที่หลากหลายสำหรับควบคุมการเข้าถึงส่วนประกอบและข้อมูลที่สำคัญต่างๆ คุณสมบัติการรักษาความปลอดภัย อย่างเช่น Smart Cover Sensor และ Smart Cover Lock ซึ่งมีให้ในผลิตภัณฑ์บางรุ่น จะช่วยป้องกันการเข้าถึงส่วนประกอบภายในของ PC ได้ และด้วยการตัดการทำงานของพอร์ตขนาน อนุกรม หรือ USB หรือตัดการทำงานในการบูตจากสื่อบุคจะช่วยให้คุณป้องกันการเข้าถึงข้อมูลที่สำคัญได้ การแจ้งเตือนของตัวตรวจสอบการเปลี่ยนหน่วยความจำและ Smart Cover Sensor สามารถส่งต่อถึงแอปพลิเคชันการจัดการระบบเพื่อแจ้งให้คุณทราบถึงการบุกรุกองค์ประกอบภายในได้อย่างทันที่




Smart Cover Sensor และ Smart Cover Lock เป็นอุปกรณ์เสริมในบางระบบ

ใช้ยูทิลิตีต่อไปนี้เพื่อรักษาความปลอดภัยสำหรับเครื่องคอมพิวเตอร์ HP ของคุณ:


- หากการตั้งค่าเครื่องท้องถิ่น ให้ใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์ *คู่มือยูทิลิตีการตั้งค่าคอมพิวเตอร์ (F10)* ซึ่งมาพร้อมกับเครื่องคอมพิวเตอร์เพื่อคู่มือและคำแนะนำเพิ่มเติมเกี่ยวกับการใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์
- สำหรับการตั้งค่าระยะไกล ให้ใช้ HP Client Manager หรือ System Software Manager ซอฟต์แวร์นี้จะช่วยให้คุณใช้งานและควบคุมการรักษาความปลอดภัยได้อย่างแน่นอนและทั่วถึงจากยูทิลิตีคำสั่ง(Command Line) ที่ง่ายดาย

ตารางและหัวข้อต่อไปนี้จะกล่าวถึงคุณสมบัติการจัดการด้านความปลอดภัยของเครื่องคอมพิวเตอร์โดยใช้ยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10) ที่เครื่องคุณ


ภาพรวมของคุณสมบัติการรักษาความปลอดภัย

คุณสมบัติ	วัตถุประสงค์	วิธีการใช้งาน
การควบคุมการบูตจากสื่อที่ถอดเข้าออกได้	ป้องกันการบูตจากไดรฟ์สื่อที่ถอดเข้าออกได้	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
การควบคุมอินเตอร์เฟซอนุกรมขนาน USB หรืออินฟราเรด	ป้องกันการถ่ายโอนข้อมูลผ่านทางอินเตอร์เฟซอนุกรมขนาน USB (Universal Serial Bus) หรืออินฟราเรด	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
รหัสผ่านเมื่อเปิดเครื่อง	ป้องกันการเข้าใช้คอมพิวเตอร์โดยไม่มีรหัสผ่าน ซึ่งสามารถใช้ได้ทั้งกับการเริ่มต้นการทำงานของคอมพิวเตอร์ครั้งแรกและการเริ่มการทำงานใหม่	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
รหัสผ่านสำหรับการตั้งค่า	ป้องกันการตั้งค่าคอมพิวเตอร์ใหม่ (การใช้ยูทิลิตี้การตั้งค่าคอมพิวเตอร์) โดยไม่มีรหัสผ่าน	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
DriveLock	ป้องกันการเข้าถึงข้อมูลในบางฮาร์ดไดรฟ์โดยไม่ได้รับอนุญาต คุณสมบัตินี้มีในคอมพิวเตอร์บางรุ่นเท่านั้น	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าคอมพิวเตอร์ โปรดดูที่ คู่มือยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10) การใช้คุณสมบัติการรักษาความปลอดภัยอาจต่างกันไป ทั้งนี้ขึ้นอยู่กับวิธีการตั้งค่าเครื่องคอมพิวเตอร์ของคุณ		

ภาพรวมของคุณสมบัติการรักษาความปลอดภัย(ต่อ)

คุณสมบัติ	วัตถุประสงค์	วิธีการใช้งาน
Smart Cover Sensor	แจ้งให้ทราบเมื่อฝาครอบหรือแผงปิดด้านข้างถูกถอดออก สามารถกำหนดให้ต้องใช้รหัสผ่านสำหรับการตั้งค่าเพื่อ เริ่มการทำงานของคอมพิวเตอร์ใหม่ หลังจากที่มีการถอดฝาครอบหรือแผงปิดด้านข้างของเครื่อง หากต้องการข้อมูลเพิ่มเติมเกี่ยวกับคุณสมบัตินี้ โปรดดูที่ <i>คู่มือฮาร์ดแวร์</i> ในซีดี <i>Documentation Library</i> สำหรับคุณสมบัตินี้มีในคอมพิวเตอร์บางรุ่นเท่านั้น	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
Master Boot Record Security	อาจช่วยป้องกันการเปลี่ยนเรคคอร์ดการบูตหลักของดิสก์ที่จับคู่ในปัจจุบันโดยไม่ตั้งใจหรือการเปลี่ยนแปลงโดยประสงค์ร้าย เป็นวิธีการเรียกคืน MBR ที่ "ทราบว่าจะใช้ได้เป็นครั้งสุดท้าย"	จากเมนูยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)
การแจ้งเตือนการเปลี่ยนแปลงหน่วยความจำ	ตรวจจับว่ามีการเพิ่ม ลด หรือนำหน่วยความจำออกจากระบบ และแจ้งผู้ใช้และผู้บริหารระบบ	สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้การแจ้งเตือนหน่วยความจำ โปรดดูข้อมูลแบบออนไลน์ใน <i>คู่มือการจัดการอัจฉริยะ</i>
 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าคอมพิวเตอร์ โปรดดูที่ <i>คู่มือยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)</i> การใช้คุณสมบัติการรักษาความปลอดภัยอาจต่างกันไป ทั้งนี้ขึ้นอยู่กับ การตั้งค่าเครื่องคอมพิวเตอร์ของคุณ		

ภาพรวมของคุณสมบัติการรักษาความปลอดภัย(ต่อ)

คุณสมบัติ	วัตถุประสงค์	วิธีการใช้งาน
ป้ายแสดงความเป็นเจ้าของ	แสดงข้อมูลการเป็นเจ้าของ ตามที่ผู้ บริหารระบบกำหนดขึ้น ระหว่างการ เริ่มต้นระบบ (ป้องกันตัวรหัสผ่าน สำหรับการตั้งค่า)	จากเมนูยูทิลิตี้การตั้งค่า คอมพิวเตอร์ (F10)
การล็อกด้วยสายเคเบิล	ป้องกันการเข้าถึงภายในเครื่อง คอมพิวเตอร์ เพื่อป้องกันการเปลี่ยน แปลงการตั้งค่าหรือการถอดส่วน ประกอบต่างๆ สามารถใช้ยึด คอมพิวเตอร์เข้ากับวัตถุที่แน่นหนา เพื่อป้องกันขโมย	ติดตั้งตัวล็อกสายเคเบิลเพื่อยึด คอมพิวเตอร์เข้ากับวัตถุที่แน่น หนา
ห้วงรักษาความปลอดภัย	ป้องกันการเข้าถึงภายในเครื่อง คอมพิวเตอร์ เพื่อป้องกันการเปลี่ยน แปลงการตั้งค่าหรือการถอดส่วน ประกอบต่างๆ	ติดตั้งตัวล็อกในห้วงรักษาความ ปลอดภัยเพื่อป้องกันการแก้ไขการ ตั้งค่าหรือการถอดส่วนประกอบ ต่างๆ
 สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าคอมพิวเตอร์ โปรดดูที่ <i>คู่มือยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)</i> การใช้คุณสมบัติการรักษาความปลอดภัยอาจต่างกันไป ทั้งนี้ขึ้นอยู่กับวิธีการตั้งค่าเครื่องคอมพิวเตอร์ของคุณ		

การป้องกันด้วยรหัสผ่าน

รหัสผ่านเมื่อเปิดเครื่องจะป้องกันการใช้คอมพิวเตอร์โดยไม่ได้รับอนุญาตด้วยการ
ให้ผู้ป้อนรหัสผ่านเพื่อเข้าใช้แอปพลิเคชันหรือข้อมูลทุกครั้งที่เปิดหรือเริ่มระบบ
ใหม่ ส่วนรหัสผ่านสำหรับการตั้งค่าซึ่งป้องกันการเข้าใช้โปรแกรมการตั้งค่า
คอมพิวเตอร์จะสามารถใช้แทนรหัสผ่านเมื่อเปิดเครื่องได้ ซึ่งหมายความว่า เมื่อ
ระบบให้ผู้ป้อนรหัสผ่านเมื่อเปิดเครื่อง การป้อนรหัสผ่านสำหรับการตั้งค่าแทนจะมี
ผลเช่นเดียวกัน

คุณสามารถกำหนดรหัสผ่านสำหรับการตั้งค่าของคอมพิวเตอร์ทั้งเน็ตเวิร์ก ซึ่งทำ
ให้ผู้บริหารระบบสามารถล็อกอินเข้าสู่เครื่องคอมพิวเตอร์ทุกเครื่องเพื่อดำเนินการ
ซ่อมบำรุง โดยไม่ต้องทราบรหัสผ่านเมื่อเปิดเครื่อง แม้ว่า จะมีการกำหนดไว้ก็ตาม

การกำหนดรหัสผ่านสำหรับการตั้งค่าโดยใช้โปรแกรมการตั้งค่าคอมพิวเตอร์

การกำหนดรหัสผ่านสำหรับการตั้งค่าจากโปรแกรมการตั้งค่าคอมพิวเตอร์จะป้องกันการแก้ไขการตั้งค่าของเครื่องคอมพิวเตอร์ (การใช้ชุดคีย์การตั้งค่าคอมพิวเตอร์ (F10)) หากไม่ได้ป้อนรหัสผ่าน

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านล่างของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ชุดคีย์นี้

3. เลือก **Security** จากนั้นเลือก **Setup Password** และปฏิบัติตามคำแนะนำบนหน้าจอ
4. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

การกำหนดรหัสผ่านเมื่อเปิดเครื่องโดยใช้โปรแกรมการตั้งค่าคอมพิวเตอร์

การกำหนดรหัสผ่านเมื่อเปิดเครื่องในโปรแกรมการตั้งค่าคอมพิวเตอร์จะป้องกันการเข้าใช้เครื่องคอมพิวเตอร์เมื่อเปิดระบบ หากไม่ได้ป้อนรหัสผ่าน เมื่อกำหนดรหัสผ่านเมื่อเปิดเครื่องแล้ว โปรแกรมการตั้งค่าคอมพิวเตอร์จะแสดงตัวเลือก Password ได้เมนู Security ตัวเลือกรหัสผ่านรวมถึงการรับรหัสผ่านเมื่อวอร์มบูต (Password Prompt on Warm Boot) หากเลือก Password Prompt on Warm Boot จะต้องมีการป้อนรหัสผ่านทุกครั้งที่ยืดเครื่องคอมพิวเตอร์

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านขวาของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตีนี้

3. เลือก **Security** จากนั้นเลือก **Power-On Password** และปฏิบัติตามคำแนะนำบนหน้าจอ
4. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

การป้อนรหัสผ่านเมื่อเปิดเครื่อง

ในการป้อนรหัสผ่านเมื่อเปิดเครื่อง ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

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



พิมพ์รหัสผ่านที่ถูกต้อง และด้วยเหตุผลด้านความปลอดภัย ตัวอักษรที่คุณพิมพ์จะไม่ปรากฏบนหน้าจอ

หากคุณป้อนรหัสผ่านไม่ถูกต้อง ไอคอนรูปกุญแจจะปรากฏขึ้น ให้ลองพิมพ์อีกครั้ง หากใส่รหัสผ่านผิดติดต่อกันสามครั้ง คุณจะต้องปิดเครื่องคอมพิวเตอร์ แล้วเปิดใหม่อีกครั้งก่อนที่จะดำเนินการต่อ

การป้อนรหัสผ่านสำหรับการตั้งค่า

หากมีการกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ในคอมพิวเตอร์ ระบบจะให้คุณป้อนรหัสผ่านดังกล่าวทุกครั้งที่รีน โปแกรมการตั้งค่าคอมพิวเตอร์

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ในวินโดวส์ ให้คลิก **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 = Setup ปรากฏขึ้นที่มุมด้านขวาล่างของหน้าจอ ให้กดปุ่ม **F10**



หากคุณไม่ได้กดปุ่ม **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตีนี้

3. เมื่อไอคอนรูปกุญแจปรากฏบนหน้าจอ ให้พิมพ์รหัสผ่านสำหรับการตั้งค่า และกด **Enter**



พิมพ์รหัสผ่านที่ถูกต้อง และด้วยเหตุผลด้านความปลอดภัย ตัวอักษรที่คุณพิมพ์จะไม่ปรากฏบนหน้าจอ

หากคุณป้อนรหัสผ่านไม่ถูกต้อง ไอคอนรูปกุญแจจะปรากฏขึ้น ให้ลองพิมพ์อีกครั้ง หากใส่รหัสผ่านผิดติดต่อกันสามครั้ง คุณจะต้องปิดเครื่องคอมพิวเตอร์ แล้วเปิดใหม่อีกครั้งก่อนที่จะดำเนินการต่อ

การเปลี่ยนรหัสผ่านเมื่อเปิดเครื่องหรือรหัสผ่านสำหรับการตั้งค่า

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer** ในการเปลี่ยนรหัสผ่านสำหรับการตั้งค่า ให้รันโปรแกรมการตั้งค่าคอมพิวเตอร์
2. เมื่อไอคอนรูปกุญแจปรากฏขึ้น ให้พิมพ์รหัสผ่านปัจจุบัน ตามด้วยเครื่องหมายทับ (/) หรือตัวคั่นอื่น จากนั้นพิมพ์รหัสผ่านใหม่ ตามด้วยเครื่องหมายทับ (/) หรือตัวคั่นอื่น และรหัสผ่านใหม่อีกครั้งตามที่แสดงต่อไปนี้:
รหัสผ่านปัจจุบัน/รหัสผ่านใหม่/รหัสผ่านใหม่



พิมพ์รหัสผ่านที่ถูกต้อง และด้วยเหตุผลด้านความปลอดภัย ตัวอักษรที่คุณพิมพ์จะไม่ปรากฏบนหน้าจอ

3. กดปุ่ม **Enter**

รหัสผ่านใหม่จะมีผลเมื่อคุณเปิดเครื่องในครั้งถัดไป



โปรดดูหัวข้อ "อักขระที่ใช้เป็นตัวคั่นในแป้นพิมพ์ของชาติต่างๆ" ในบทนี้ เพื่อข้อมูลเพิ่มเติมเกี่ยวกับตัวคั่นอื่นๆ นอกจากนี้ คุณสามารถเปลี่ยนรหัสผ่านเมื่อเปิดเครื่องและรหัสผ่านสำหรับการตั้งค่าโดยใช้ตัวเลือก Security ในโปรแกรมการตั้งค่าคอมพิวเตอร์

การลบรหัสผ่านเมื่อเปิดเครื่องหรือรหัสผ่านสำหรับการตั้งค่า

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer** ในการลบรหัสผ่านสำหรับการตั้งค่า ให้รันโปรแกรมการตั้งค่าคอมพิวเตอร์
2. เมื่อไอคอนรูปกุญแจปรากฏขึ้น ให้พิมพ์รหัสผ่านปัจจุบันตามด้วยเครื่องหมายทับ (/) หรือตัวคั่นอื่นตามที่แสดงดังนี้:
รหัสผ่านปัจจุบัน/
3. กดปุ่ม **Enter**



โปรดดูหัวข้อ "อักขระที่ใช้เป็นตัวคั่นในแป้นพิมพ์ของชาติต่างๆ" เพื่อข้อมูลเพิ่มเติมเกี่ยวกับอักขระที่ใช้เป็นตัวคั่น นอกจากนี้ คุณสามารถเปลี่ยนรหัสผ่านเมื่อเปิดเครื่องและรหัสผ่านสำหรับการตั้งค่าโดยใช้ตัวเลือก Security ในโปรแกรมการตั้งค่าคอมพิวเตอร์

อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ

การออกแบบแป้นพิมพ์จะเป็นไปตามมาตรฐานของแต่ละประเทศ รูปแบบการพิมพ์และเป็นตัวอักษรที่ใช้สำหรับการเปลี่ยนหรือลบรหัสผ่านจะขึ้นอยู่กับแป้นพิมพ์ที่มาพร้อมกับคอมพิวเตอร์

อักขระที่ใช้เป็นตัวคั่นบนแป้นพิมพ์ของแต่ละชาติ

อาราบิก	/	กรีก	-	รัสเซีย	/
เบลเยียม	=	ฮิบรู	.	สโลวาเกีย	-
BHCSY*	-	ฮังการี	-	สเปน	-
บราซิล	/	อิตาลี	-	สวีเดน/ฟินแลนด์	/
จีน	/	ญี่ปุ่น	/	สวิส	-
เช็ก	-	เกาหลี	/	ไทย	/
เดนมาร์ก	-	ลาตินอเมริกา	-	ตุรกี	.
ฝรั่งเศส	!	นอร์เวย์	-	อังกฤษแบบ สหราชอาณาจักร	/
ฝรั่งเศสแบบ แคนาดา	é	โปแลนด์	-	อังกฤษแบบ สหรัฐอเมริกา	/
เยอรมัน	-	โปรตุเกส	-		

* สำหรับบอสเนีย-เฮอร์เซโกวีนา โครเอเชีย สโลวาเนีย และยูโกสลาเวีย

การยกเลิกรหัสผ่าน

หากคุณลืมรหัสผ่าน คุณจะไม่สามารถเข้าใช้เครื่องคอมพิวเตอร์ได้ หากต้องการคำแนะนำเกี่ยวกับการยกเลิกรหัสผ่าน โปรดดู [คู่มือการแก้ไขปัญหา](#)

DriveLock

ตัวล็อกไดรฟ์ (DriveLock) เป็นคุณสมบัติการรักษาความปลอดภัยที่ป้องกันการเข้าใช้ข้อมูลในฮาร์ดไดรฟ์ที่กำหนด ตัวล็อกไดรฟ์เป็นส่วนเสริมของโปรแกรมการตั้งค่าคอมพิวเตอร์ คุณสมบัตินี้จะมีอยู่ในคอมพิวเตอร์บางรุ่น และจะใช้ได้เมื่อมีฮาร์ดไดรฟ์ที่สามารถใช้คุณสมบัตินี้ได้เท่านั้น

ตัวล็อกไดรฟ์เป็นคุณสมบัติสำหรับผู้ใช้ HP ที่ให้ความสำคัญสูงสุดในการป้องกันข้อมูล ซึ่งในกรณีนี้ มูลค่าของฮาร์ดไดรฟ์และการสูญเสียข้อมูลในไดรฟ์เปรียบเทียบไม่ได้กับแลกกับกับความเสียหายที่อาจเกิดขึ้นจากการล้วงละเมิดเข้าใช้ข้อมูลสำคัญ โดยไม่ได้รับอนุญาต และเพื่อเพิ่มความยืดหยุ่นในกรณีที่คุณลืมรหัสผ่าน โดยยังคงระดับการรักษาความปลอดภัยไว้นั้น คุณสมบัติตัวล็อกไดรฟ์ของ HP จึงใช้รูปแบบการป้องกันด้วยรหัสผ่านสองค่า รหัสผ่านชุดหนึ่งจะถูกกำหนดและใช้โดยผู้บริหารระบบ ส่วนอีกชุดหนึ่งจะถูกกำหนดและใช้โดยผู้ใช้ทั่วไป และจะไม่มี "หนทางพิเศษ" สำหรับ ปลดล็อกไดรฟ์หารหัสผ่านทั้งสองค่าสูญหายไป ดังนั้น คุณสมบัติตัวล็อกไดรฟ์จะปลอดภัยที่สุดในกรณีที่มีการจำลองข้อมูลในไดรฟ์ไปยังระบบข้อมูลขององค์กร หรือมีการสำรองข้อมูลอย่างสม่ำเสมอ

ในกรณีที่ไม่สามารถจำรหัสผ่านทั้งสองค่าของตัวล็อกไดรฟ์ ฮาร์ดไดรฟ์นั้น ก็จะใช้ไม่ได้อีกต่อไป ทางเลือกนี้อาจเสี่ยงเกินไปสำหรับผู้ใช้ที่ไม่มีความจำเป็นต้องใช้การป้องกันในระดับนี้ แต่สำหรับผู้ใช้ที่มีความจำเป็น ความเสี่ยงนี้อาจคุ้มค่าเมื่อคำนึงถึงข้อมูลที่เก็บรักษาในไดรฟ์

การใช้ตัวล็อกไดรฟ์

ตัวเลือก DriveLock จะปรากฏอยู่ในเมนู Security ในการตั้งค่าคอมพิวเตอร์ ผู้ใช้จะเห็นตัวเลือกในการกำหนดรหัสผ่านหลักหรือใช้งานคุณสมบัติตัวล็อกไดรฟ์ และจะต้องป้อนรหัสผ่านสำหรับผู้ใช้ ซึ่งจะ สามารถใช้คุณสมบัตินี้ได้ และเนื่องจากการกำหนดค่าของตัวล็อกไดรฟ์ในครั้งแรกมักกระทำโดยผู้บริหารระบบ ดังนั้นจึงควรกำหนดรหัสผ่านหลักก่อน ทั้งนี้ ผู้บริหารระบบควรกำหนดรหัสผ่านหลักไว้ ไม่ว่า จะต้องการใช้คุณสมบัติตัวล็อกไดรฟ์ หรือไม่ก็ตาม เพื่อที่ผู้บริหารระบบจะสามารถแก้ไขการตั้งค่าตัวล็อกไดรฟ์ได้หากมีการล็อกไดรฟ์ในอนาคต เมื่อกำหนดรหัสผ่านหลักแล้ว ผู้บริหารระบบสามารถใช้คุณสมบัตินี้ หรือเลือกที่จะไม่ใช่คุณสมบัตินี้ก็ได้

หากมีฮาร์ดไดรฟ์ที่ถูกล็อก กระบวนการ POST จะให้คุณป้อนรหัสผ่านเพื่อปลดล็อกไดรฟ์ หากมีการกำหนดรหัสผ่านเมื่อเปิดเครื่องไว้ และรหัสผ่านนั้นตรงกับรหัสผ่านสำหรับผู้ใช้งานของตัวล็อกไดรฟ์ กระบวนการ POST จะไม่ให้คุณป้อนรหัสผ่านอีกครั้ง แต่หากไม่มีการกำหนดรหัสผ่านเมื่อเปิดเครื่องไว้ ผู้ใช้จะต้องป้อนรหัสผ่านสำหรับตัวล็อกไดรฟ์ โดยสามารถใช้ได้ทั้งรหัสผ่านหลักและรหัสผ่านสำหรับผู้ใช้งาน ผู้ใช้สามารถป้อนรหัสผ่านได้เพียงสองครั้ง หากรหัสผ่านไม่ถูกต้องทั้งสองครั้ง กระบวนการ POST จะดำเนินการต่อ แต่จะไม่สามารถเข้าสู่ข้อมูลในไดรฟ์ดังกล่าวได้

การใช้งานตัวล็อกไดรฟ์

การใช้งานตัวล็อกไดรฟ์เหมาะสมที่สุดกับสภาพแวดล้อมแบบองค์กร ซึ่งผู้บริหารระบบจะจัดให้ผู้ใช้งานฮาร์ดไดรฟ์ multibay สำหรับใช้กับคอมพิวเตอร์บางเครื่อง และผู้บริหารระบบจะต้องตั้งค่าฮาร์ดไดรฟ์ multibay ซึ่งรวมถึงการกำหนดรหัสผ่านหลักของตัวล็อกไดรฟ์ด้วย ในกรณีที่ผู้ใช้ลืมรหัสผ่านสำหรับผู้ใช้งาน หรือเมื่อมีการเปลี่ยนมือผู้ใช้ คุณสามารถใช้รหัสผ่านหลักเพื่อรีเซ็ตรหัสผ่านสำหรับผู้ใช้งานและสามารถใช้งานไดรฟ์ได้อีกครั้ง

ผู้บริหารระบบที่เลือกใช้คุณสมบัตินี้ควรกำหนดนโยบายภายในองค์กรสำหรับการกำหนดและเก็บรักษาการรหัสผ่านหลัก เพื่อป้องกันเหตุการณ์ที่ผู้ใช้อาจงุนงงหรือมีได้ใจกำหนดรหัสผ่านทั้งสองชุดก่อนที่จะออกจากองค์กร ซึ่งหากเป็นเช่นนั้น จะต้องมีการเปลี่ยนฮาร์ดไดรฟ์ใหม่ เพราะจะไม่สามารถใช้งานฮาร์ดไดรฟ์นี้ได้อีก และเช่นเดียวกัน หากไม่มีการกำหนดรหัสผ่านหลักไว้ ผู้บริหารระบบอาจไม่สามารถเข้าสู่ฮาร์ดไดรฟ์ได้ และจะไม่สามารถดำเนินการตรวจสอบซอฟต์แวร์ที่ไม่ได้รับอนุญาตได้ตามปกติ รวมถึงฟังก์ชันการควบคุมทรัพย์สินและการสนับสนุนอื่นๆ ด้วย


ทั้งนี้ ไม่แนะนำให้ใช้คุณสมบัติตัวล็อกไดรฟ์สำหรับผู้ใช้งานที่ไม่มีความจำเป็นต้องใช้ระบบรักษาความปลอดภัยที่เข้มงวดเช่นนี้ ผู้ใช้ในกลุ่มนี้รวมถึงผู้ใช้คอมพิวเตอร์ส่วนบุคคล หรือผู้ใช้ที่ไม่ได้เก็บข้อมูลสำคัญไว้ในฮาร์ดไดรฟ์เป็นประจำ สำหรับผู้ใช้งานเหล่านี้ การสูญเสียฮาร์ดไดรฟ์เนื่องจากการลืมรหัสผ่านทั้งสองชุดจะไม่มีผลกับการใช้ตัวล็อกไดรฟ์เพื่อป้องกันข้อมูล คุณสามารถจำกัดการเข้าใช้โปรแกรมการตั้งค่าคอมพิวเตอร์และตัวล็อกไดรฟ์ด้วยรหัสผ่านสำหรับการตั้งค่า โดยผู้บริหารระบบสามารถกำหนดรหัสผ่านสำหรับการตั้งค่าขึ้นโดยไม่ให้ผู้ใช้งานทราบรหัสผ่านนั้น ก็จะยังสามารถจำกัดการใช้งานตัวล็อกไดรฟ์ได้

Smart Cover Sensor

Smart Cover Sensor ซึ่งมีให้ในบางรุ่น เป็นเทคโนโลยีการผสมผสาน ระหว่าง ฮาร์ดแวร์และซอฟต์แวร์ ซึ่งใช้สำหรับการแจ้งเมื่อมีการเปิดฝาครอบหรือแผงปิด ด้านข้างของเครื่อง โดยมีระดับการป้องกัน สามระดับ ดังที่จะอธิบายในตารางต่อไปนี้

ระดับการป้องกันของ Smart Cover Sensor

ระดับ	การตั้งค่า	คำอธิบาย
ระดับ 0	Disabled (ไม่ใช้งาน)	ไม่ใช้งาน Smart Cover Sensor (ค่าดีฟอลต์)
ระดับ 1	Notify User (แจ้งผู้ใช้)	เมื่อเริ่มระบบคอมพิวเตอร์ใหม่ หน้าจอจะแสดงข้อความแจ้งว่ามีการเปิดฝาครอบเครื่องหรือแผงปิดด้านข้าง
ระดับ 2	Setup Password (รหัสผ่านสำหรับการตั้งค่า)	เมื่อเริ่มระบบคอมพิวเตอร์ใหม่ หน้าจอจะแสดงข้อความแจ้งว่ามีการเปิดฝาครอบเครื่องหรือแผงปิดด้านข้าง คุณจะต้องป้อนรหัสผ่านสำหรับการตั้งค่าเพื่อดำเนินการต่อ

 การตั้งค่าเหล่านี้สามารถเปลี่ยนแปลงได้โดยใช้โปรแกรมการตั้งค่าคอมพิวเตอร์ สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการตั้งค่าคอมพิวเตอร์ โปรดดูที่ คู่มือยูทิลิตี้การตั้งค่าคอมพิวเตอร์ (F10)

การกำหนดระดับการป้องกันของ Smart Cover Sensor

ในการกำหนดระดับการป้องกันของ Smart Cover Sensor โปรดปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านขวาของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตีนี้

3. เลือก **Security** จากนั้นเลือก **Smart Cover** และปฏิบัติตามคำแนะนำบนหน้าจอ
4. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

Smart Cover Lock

Smart Cover Lock เป็นล๊อคฝาปิดเครื่องที่ควบคุมด้วยซอฟต์แวร์ซึ่งมีอยู่ในคอมพิวเตอร์ HP บางรุ่น ล๊อคนี้จะป้องกันการเข้าถึงส่วนประกอบภายในเครื่องโดยไม่ได้รับอนุญาต คอมพิวเตอร์จะส่งถึงมือคุณ โดยที่ Smart Cover Lock อยู่ในตำแหน่งปลดล๊อค



ข้อควรระวัง: เพื่อการป้องกันสูงสุด โปรดตรวจสอบว่าคุณได้กำหนดรหัสผ่านสำหรับการตั้งค่าแล้ว รหัสผ่านสำหรับการตั้งค่าจะป้องกันการเข้าใช้ยูทิลิตีการตั้งค่าคอมพิวเตอร์โดยไม่ได้รับอนุญาต



Smart Cover Lock เป็นอุปกรณ์เสริมในบางระบบ

การล๊อคด้วย Smart Cover Lock

ในการใช้และล๊อค Smart Cover Lock ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านขวาล่างของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตีนี้

3. เลือก **Security** แล้วเลือก **Smart Cover** และเลือกตัวเลือก **Locked**
4. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

การปลดล๊อค Smart Cover Lock

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านขวาล่างของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตีนี้

3. เลือก **Security > Smart Cover > Unlocked**
4. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

การใช้กุญแจ Smart Cover FailSafe

หากคุณใช้งาน Smart Cover Lock และไม่สามารถป้อนรหัสผ่านเพื่อยกเลิกการทำงานของล็อก คุณจะต้องใช้กุญแจ Smart Cover FailSafe เพื่อเปิดฝาเครื่อง คุณจะต้องใช้กุญแจในกรณีต่อไปนี้:

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



ข้อควรระวัง: กุญแจ Smart Cover FailSafe เป็นอุปกรณ์พิเศษที่สามารถสั่งซื้อได้จาก HP โปรดเตรียมพร้อมโดยการสั่งซื้อกุญแจนี้ก่อนเกิดความจำเป็นต้องใช้งาน จากตัวแทนจำหน่ายหรือผู้ให้บริการที่ได้รับอนุญาต

หากต้องการขอรับกุญแจ FailSafe ให้ดำเนินการอย่างใดอย่างหนึ่งต่อไปนี้:

- ติดต่อผู้ให้บริการหรือตัวแทนจำหน่ายที่ได้รับอนุญาตของ HP
- ติดต่อหมายเลขที่เหมาะสมตามที่ระบุในใบรับประกัน

สำหรับข้อมูลเพิ่มเติมเกี่ยวกับการใช้กุญแจ Smart Cover FailSafe โปรดดูจาก *คู่มืออ้างอิงฮาร์ดแวร์*

Master Boot Record Security

เรคคอร์ดการบูตหลัก (MBR) ประกอบด้วยข้อมูลที่จำเป็นต่อการบูตจากดิสก์และการเข้าใช้ข้อมูลในดิสก์นั้น การป้องกันเรคคอร์ดการบูตหลักจะป้องกันการเปลี่ยนแปลงแก้ไข MBR โดยไม่ตั้งใจหรือโดยไม่ปรารถนาดี เช่น กรณีที่เกิดจากไวรัสคอมพิวเตอร์หรือการใช้ยูทิลิตีดิสก์ที่ไม่ถูกต้อง นอกจากนี้ ยังใช้ในการเรียกคืน MBR ที่ "ทราบว่าจะใช้ได้เป็นครั้งล่าสุด" หากระบบพบว่า MBR มีการเปลี่ยนแปลงเมื่อเริ่มระบบใหม่

ในการใช้การป้องกัน MBR ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านขวาของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ย่อข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตีนี้

3. เลือก **Security > Master Boot Record Security > Enabled**
4. เลือก **Security > Save Master Boot Record**
5. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

เมื่อใช้การป้องกัน MBR แล้ว BIOS ของระบบจะป้องกันไม่ให้เกิดการเปลี่ยนแปลงแก้ไข MBR สำหรับดิสก์ที่บูตในปัจจุบันในขณะที่อยู่ใน MS-DOS หรือ Windows Safe Mode



ระบบปฏิบัติการส่วนใหญ่จะควบคุมการเข้าใช้ MBR ของดิสก์ที่บูตปัจจุบัน และ BIOS จะไม่สามารถป้องกันการเปลี่ยนแปลงในขณะที่ระบบปฏิบัติการทำงานอยู่

ทุกครั้งที่เปิดเครื่องหรือเริ่มระบบใหม่ BIOS จะเปรียบเทียบ MBR ของดิสก์ที่บูตปัจจุบันกับ MBR ที่บันทึกไว้ก่อนหน้านี้ หากพบการเปลี่ยนแปลงในกรณีที่บันทึกไว้ เดียวกันกับที่บันทึกไว้ก่อนหน้านี้ ข้อความต่อไปนี้จะปรากฏขึ้น

1999—Master Boot Record has changed. (มีการเปลี่ยนแปลงเรคคอร์ดการบูตหลัก)

Press any key to enter Setup to configure MBR Security. (กดปุ่มใดๆ เพื่อเข้าสู่การตั้งค่าเพื่อกำหนดค่าการรักษาความปลอดภัย MBR)

และในการเข้าสู่โปรแกรมการตั้งค่าคอมพิวเตอร์ คุณจะต้อง

- บันทึก MBR ของดิสก์ที่ใช้บูตปัจจุบัน
- เรียกคืน MBR ที่บันทึกไว้ก่อนหน้านี้ หรือ
- เลิกใช้คุณสมบัติการป้องกัน MBR

หากมีการกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ คุณจะต้องทราบรหัสผ่านนั้น หากตรวจพบการเปลี่ยนแปลง และหากดิสก์ที่ใช้บูตไม่ใช่ดิสก์เดียวกันกับของ MBR เดิมที่บันทึกไว้ ข้อความต่อไปนี้จะปรากฏขึ้น:

2000—Master Boot Record Hard Drive has changed. (ฮาร์ดไดรฟ์ Master Boot Record มีการเปลี่ยนแปลง)

Press any key to enter Setup to configure MBR Security. (กดปุ่มใดๆ เพื่อเข้าสู่การตั้งค่าเพื่อกำหนดค่าการรักษาความปลอดภัย MBR)

และในการเข้าสู่โปรแกรมการตั้งค่าคอมพิวเตอร์ คุณจะต้อง

- บันทึก MBR ของดิสก์ที่ใช้บูตปัจจุบัน
- เลิกใช้คุณสมบัติการป้องกัน MBR

หากมีการกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ คุณจะต้องทราบรหัสผ่านนั้น หาก MBR ที่บันทึกไว้ก่อนหน้านี้เกิดความเสียหาย ซึ่งอาจไม่เกิดขึ้นบ่อยนัก ข้อความต่อไปนี้จะปรากฏขึ้น:

1998—Master Boot Record has been lost. (Master Boot Record สูญหาย)

Press any key to enter Setup to configure MBR Security. (กดปุ่มใดๆ เพื่อเข้าสู่การตั้งค่าเพื่อกำหนดค่าการรักษาความปลอดภัย MBR)

และในการเข้าสู่โปรแกรมการตั้งค่าคอมพิวเตอร์ คุณจะต้อง

- บันทึก MBR ของดิสก์ที่ใช้บูตปัจจุบัน
- เลิกใช้คุณสมบัติการป้องกัน MBR

หากมีการกำหนดรหัสผ่านสำหรับการตั้งค่าไว้ คุณจะต้องทราบรหัสผ่านนั้น

ก่อนที่จะแบ่งพาร์ติชันหรือฟอร์แมตดิสก์ที่ใช้บูตในปัจจุบัน

ตรวจสอบว่าได้เลิกใช้คุณสมบัติการป้องกัน MBR ก่อนที่คุณจะเปลี่ยนแปลงการแบ่งพาร์ติชันหรือก่อนที่จะฟอร์แมตดิสก์ ยูทิลิตี้สำหรับดิสก์บางชนิด เช่น FDISK และ FORMAT จะพยายามอัปเดต MBR หากคุณใช้คุณสมบัติการป้องกัน MBR ขณะที่เปลี่ยนแปลงการแบ่งพาร์ติชันหรือฟอร์แมต คุณอาจได้รับข้อความแสดงข้อผิดพลาดจากยูทิลิตี้ของดิสก์ หรือได้รับคำเตือนจากโปรแกรมการป้องกัน MBR ในครั้งถัดไปที่เปิดเครื่องหรือ เริ่มระบบใหม่ ในการเลิกใช้การป้องกัน MBR ให้ปฏิบัติตามขั้นตอนต่อไปนี้:

1. เปิดหรือเริ่มต้นระบบคอมพิวเตอร์ใหม่ หากคุณอยู่ใน Windows คลิกที่ **Start > Shut Down > Restart the Computer**
2. เมื่อข้อความ F10 Setup ปรากฏขึ้นที่มุมด้านขวาของหน้าจอ ให้กดปุ่ม **F10** กด **Enter** เพื่อข้ามหน้าจอเริ่มต้น หากจำเป็น



หากคุณไม่ได้กด **F10** ในขณะที่ข้อความดังกล่าวปรากฏขึ้น คุณจะต้องเริ่มการทำงานของคอมพิวเตอร์ใหม่เพื่อเข้าสู่ยูทิลิตี้

3. เลือก **Security > Master Boot Record Security > Disabled**
4. ก่อนออกจากโปรแกรม ให้คลิก **File > Save Changes** และ **Exit**

การล๊อคด้วยสายเคเบิล

แผงด้านหลังของเครื่องคอมพิวเตอร์สามารถรองรับการล๊อคด้วยสายเคเบิลเพื่อยึดคอมพิวเตอร์ไว้กับที่

สำหรับคำแนะนำพร้อมภาพประกอบ โปรดดูที่ *คู่มืออ้างอิงฮาร์ดแวร์* ในซีดี *Documentation Library*

เทคโนโลยีตรวจสอบลายนิ้วมือ

เพื่อตัดปัญหาในการป้อนรหัสผ่านสำหรับผู้ใช้งาน เทคโนโลยีตรวจสอบลายนิ้วมือของ HP ได้เพิ่มความปลอดภัยให้กับระบบเน็ตเวิร์ค ทำให้ขั้นตอนการลงทะเบียนเข้าใช้งานง่ายขึ้น และลดค่าใช้จ่ายที่เกี่ยวข้องกับการจัดการเน็ตเวิร์คขององค์กรลง โดยมีราคาที่เหมาะสม ไม่เป็นเพียงทางเลือกสำหรับองค์กรที่มีการป้องกันด้วยเทคโนโลยีระดับสูงอีกต่อไป



การรองรับเทคโนโลยีตรวจสอบลายนิ้วมือจะต่างกันไปในแต่ละรุ่น

หาข้อมูลเพิ่มเติม ดูได้ที่เว็บไซต์:

<http://www.compaq.com/solutions/security>

การแจ้งข้อผิดพลาดและการเรียกคืนข้อมูลระบบ

การแจ้งข้อผิดพลาดและการเรียกคืนข้อมูลระบบเป็นการผสมผสานเทคโนโลยีของฮาร์ดแวร์และซอฟต์แวร์เข้าด้วยกันเพื่อป้องกันการสูญเสียข้อมูลสำคัญ และลดเวลาซ่อมบำรุงที่ไม่ได้วางแผนไว้

เมื่อเกิดข้อผิดพลาด คอมพิวเตอร์จะแสดงข้อความแจ้งเตือนภายใน ซึ่งประกอบด้วยคำอธิบายข้อผิดพลาดและการดำเนินการที่แนะนำ จากนั้นคุณสามารถดูสถานะปัจจุบันของระบบโดยใช้โปรแกรม HP Client Manager หากคอมพิวเตอร์นั้นเชื่อมต่อกับเครือข่ายที่จัดการโดย HP Insight Manager, HP Client Manager หรือแอปพลิเคชันจัดการระบบอื่นๆ คอมพิวเตอร์จะแจ้งข้อผิดพลาดไปยังแอปพลิเคชันจัดการระบบด้วยเช่นกัน

ระบบป้องกันไดรฟ์

ระบบป้องกันไดรฟ์ (DPS) เป็นเครื่องมือในการวินิจฉัยซึ่งมีอยู่ในฮาร์ดไดรฟ์ที่ติดตั้งในเครื่องคอมพิวเตอร์ HP บางรุ่น DPS ได้รับการออกแบบมาเพื่อช่วยวินิจฉัยปัญหาที่อาจส่งผลให้ต้องมีการเปลี่ยนฮาร์ดไดรฟ์โดยไม่มีอยู่ในเงื่อนไขการรับประกัน

ในการผลิตเครื่องคอมพิวเตอร์ HP จะมีการทดสอบฮาร์ดไดรฟ์ที่ติดตั้งด้วย DPS และจะมีการบันทึกข้อมูลสำคัญไว้อย่างถาวรในไดรฟ์นั้นๆ และทุกครั้งที่รัน DPS ผลการทดสอบจะถูกบันทึกลงในฮาร์ดไดรฟ์ ผู้ให้บริการของคุณสามารถใช้ข้อมูลนี้เพื่อช่วยวินิจฉัยปัญหาที่ทำให้คุณต้องรันซอฟต์แวร์ DPS หากต้องการคำแนะนำเกี่ยวกับการใช้ DPS โปรดดู [คู่มือการแก้ไขปัญหา](#)

แหล่งจ่ายไฟที่ทนต่อไฟกระชาก

แหล่งจ่ายไฟที่ทนต่อกระแสไฟฟ้ากระชากจะให้ความมั่นใจมากขึ้นเมื่อคอมพิวเตอร์พบการกระชากของกระแสไฟซึ่งไม่อาจคาดการณ์ได้ แหล่งจ่ายไฟนี้ได้รับการปรับระดับเพื่อให้ทนต่อกระแสไฟฟ้ากระชากถึง 2000 โวลต์โดยไม่ทำให้เกิดการขัดข้องหรือสูญเสียข้อมูล

เซ็นเซอร์อุณหภูมิ

เซ็นเซอร์อุณหภูมิเป็นคุณสมบัติด้านฮาร์ดแวร์และซอฟต์แวร์ที่ติดตามอุณหภูมิภายในของเครื่องคอมพิวเตอร์ โดยคุณสมบัตินี้จะแสดงข้อความเตือนเมื่ออุณหภูมิไม่อยู่ในช่วงปกติ ซึ่งทำให้คุณมีเวลาดำเนินการตามความเหมาะสมก่อนที่จะส่วนประกอบภายในจะเสียหายหรือก่อนที่ข้อมูลจะสูญหายไป

ข

ข้อควรระวัง 8

การรักษาความปลอดภัย โดย ล็อกฝาปิดเครื่อง 27
กุญแจ FailSafe 29

ค

คิสก์, การ ลอกแบบ 2

คิสก์ ที่ สามารถ บูต ได้, ข้อมูล สำคัญ 32

ก

การจัด การ ซอฟต์แวร์ ของ ระบบ (SSM) 6

การจัด การ โคล เอ็นต์ ของ HP 6

การจัดการ พลังงาน 13

การ ตั้ง ค่า

กำหนด เวลา 13

Smart Cover Sensor 27

การ ตั้ง ค่า ปุ่ม เปิด ปิด 12

การ ตั้ง ค่า ความ ปลอดภัย, การ ตั้ง ค่า 15

การ ตั้ง ค่า เริ่ม ต้น 2

การ ตั้ง ค่า, การ จำลอง 11

การ ตั้ง ค่า, เริ่ม ต้น 2

การ ติด ตั้ง ระยะ ไกล 3

การ ติด ตั้ง ระบบ ระยะ ไกล, การ ใช้ งาน 3

การ ฟอรัมเมต คิสก์, ข้อมูล สำคัญ 32

การ กำหนด พารามิเตอร์ของ คิสก์, ข้อมูล สำคัญ 32

การ กำหนด

รหัส ผ่าน สำหรับการ ตั้ง ค่า 19, 21

การ ปลด ล็อก Smart Cover Lock 28

การ ประหยัด พลังงาน 13

การ ประหยัด พลังงาน, การ ตั้ง ค่า สำหรับ 13

การ ป้องกัน ฮาร์ดไดรฟ์ 34

การ ป้องกัน ROM 8

การ ป้องกัน ROM, ข้อ ควร ระวัง 8

การ ป้อน

รหัส ผ่าน เมื่อ เปิด เครื่อง 20

รหัส ผ่าน สำหรับการ ตั้ง ค่า 21

การ ควบคุม การ เข้า ใช้ คอมพิวเตอร์ 15

การ ควบคุม ทรัพย์สิน 15

การ เข้า ใช้ คอมพิวเตอร์, การ ควบคุม 15

การ แจ้ง ข้อ ผิด พลาด 34

การ แฟลช ROM ระยะ ไกล 8

การ ยก เลิก รหัส ผ่าน 23

การ เปลี่ยน ระบบ ปฏิบัติ การ, ข้อมูล สำคัญ 14

การ เปลี่ยน รหัส ผ่าน 22

การ เรียก คืน ข้อมูล ระบบ 9

การ เรียก คืน ข้อมูล, ซอฟต์แวร์ 2

การ ล็อก ด้วย สาย เคเบิล 32

การ ล็อก ด้วย Smart Cover Lock 28

การ รักษา ความ ปลอดภัย ด้วย รหัส ผ่าน 18

การ รักษา ความ ปลอดภัย โดย ล็อค ฝา ปิด เครื่อง, ข้อ
 ควร ระวัง 27

การ รักษา ความ ปลอดภัย, เรค คอร์ด การบูต หลัก 30

การ ลบ รหัส ผ่าน 22

การ ตั้ง ชื่อ กุแฉ FailSafe 29

กุแฉ FailSafe

 ชื่อ ควร ระวัง 29

 การ ตั้ง ชื่อ 29

กุแฉ Smart Cover FailSafe, การ ตั้ง ชื่อ 29

การอัปเกรด ROM 8

กำหนด เวลา, การ ตั้ง ค่า 13

ซ

ซอฟต์แวร์

 การ จัดการ พลังงาน 13

 การ ติด ตั้ง ระบบ ระยะ ไกล 3

 การ ควบคุม ทรัพย์สิน 15

 การ แจ็ง ชื่อ ผิด พลาด และ การ เรียก คีน ข้อมูล

 ระบบ 34

 การ แฟลช ROM ระยะ ไกล 8

 การ เรียก คีน ข้อมูล 2

 การ รวม 2

 การอัปเดต หลายๆ เครื่อง 6

 ระบบ ป้อง กัน ไดรฟ์ 34

 Altiris eXpress 4

 ยูทิลิตี้ การ ตั้ง ค่า คอมพิวเตอร์ 11

 Master Boot Record Security 30

 บล็อค การบูต FailSafe 9

 System Software Manager 6

ซอฟต์แวร์ ที่ กำหนด ขึ้น เอง 2

ป

ปุ่ม เปิด ปิด

 การ ตั้ง ค่า 12

ปุ่ม เปิด ปิด แบบ สอง สถานะ 12

ปุ่ม เปิด ปิด, สอง สถานะ 12

ค

คุณสมบัติ การ รักษา ความ ปลอดภัย, ตาราง 16

ล

ไดรฟ์ , การ ป้องกัน 34

ระบบ ปฏิบัติ การ, ข้อ มูล สำคั เกี่ยว กับ 14

เซ็นเซอร์ อุณหภูมิ 34

เครื่อง มือ การ เริ่ม ใช้งาน, ซอฟต์แวร์ 2

เครื่อง มือ การ ลอก แบบ, ซอฟต์แวร์ 2

เครื่อง มือ ใน การ วินิจฉัย สำ หรับ ฮาร์ดไดรฟ์ 34

เทคโนโลยี ตรวจสอบ ลาย นิ้ว มือ 33

เว็บไซต์

 www.compaq.com 8, 14

 www.compaq.com/activeupdate 7

 www.compaq.com/easydeploy 5, 6, 8, 11

 www.compaq.com/im/ssmwp.html 6, 8

 www.compaq.com/solutions/pcsolutions 2

 www.compaq.com/solutions/security 33

 www.hp.com/united-states/subscribe 7

ล็อค ฝา ปิด เครื่อง, smart 27

ActiveUpdate 7

แหล่ง จ่าย ไฟ ที่ ทน ต่อ ไฟ กระชาก 34

แหล่ง จ่าย ไฟ, ทน ต่อ ไฟ กระชาก 34

รหัสผ่าน

- การ ตั้ง ค่า 19
- การ กำหนด 21
- การ ยกเลิก 23
- การ เปลี่ยน 22
- การ ลบ 22
- เปิด เครื่อง 20

รหัสผ่าน เมื่อ เปิด เครื่อง

- การ ป้อน 20
- การ เปลี่ยน 22
- การ ลบ 22

รหัสผ่าน สำหรับการ ตั้ง ค่า

- การ กำหนด 19
- การ ป้อน 21
- การ เปลี่ยน 22
- การ ลบ 22

แอคเดรส World Wide Web ที่ เว็บไซต์

Altiris eXpress 4

Altiris eXpress PC Transplant Pro 5

ยูทิลิตี้ การ ตั้ง ค่า คอมพิวเตอร์ 11

ห

ส้าน ไฟ บน แป้น พิมพ์, ROM, ตาราง 10

ฮ

อักขระ ที่ ใช้ เป็น ตัว คั่น บน แป้น พิมพ์ ของ แต่ละ ชาติ
23

อักขระ ที่ ใช้ เป็น ตัว คั่น บน แป้น พิมพ์, แต่ละ ชาติ 23

อักขระ ที่ ใช้ เป็น ตัว คั่น, ตาราง 23

อินเทอร์เน็ต แอคเดรส, ดู เว็บไซต์

อุณหภูมิ ภายใน ของ เครื่อง คอมพิวเตอร์ 34

อุณหภูมิ, ภายใน คอมพิวเตอร์ 34

อิมเมจของ ซอฟต์แวร์ ที่ ติด ตั้ง ไว้ ล่วง หน้า 2

ฮาร์ดไดรฟ์, เครื่อง มือ ใน การ วินิจฉัย 34

บ

บล็อก การบูต FailSafe 9

ม

Master Boot Record Security, การ ตั้ง ค่า 30

ป

Preboot Execution Environment (PXE) 3

PXE (Preboot Execution Environment) 3

ร

ROM, การอัปเกรด 8

ROM, ไม่ ถูก ต้อง 9

ROM ของ ระบบ ไม่ ถูก ต้อง 9

ROM ส้าน ไฟ บน แป้น พิมพ์, ตาราง 10

ส

Smart Cover Lock

การ ปลด ล็อก 28

การ ล็อก 28

Smart Cover Sensor

การ ตั้ง ค่า 27

ระดับ การ ป้องกัน 26

SSM (การ จัด การ ซอฟต์แวร์ ของ ระบบ) 6

ู

URL (เว็บไซต์) ที่ เว็บไซต์