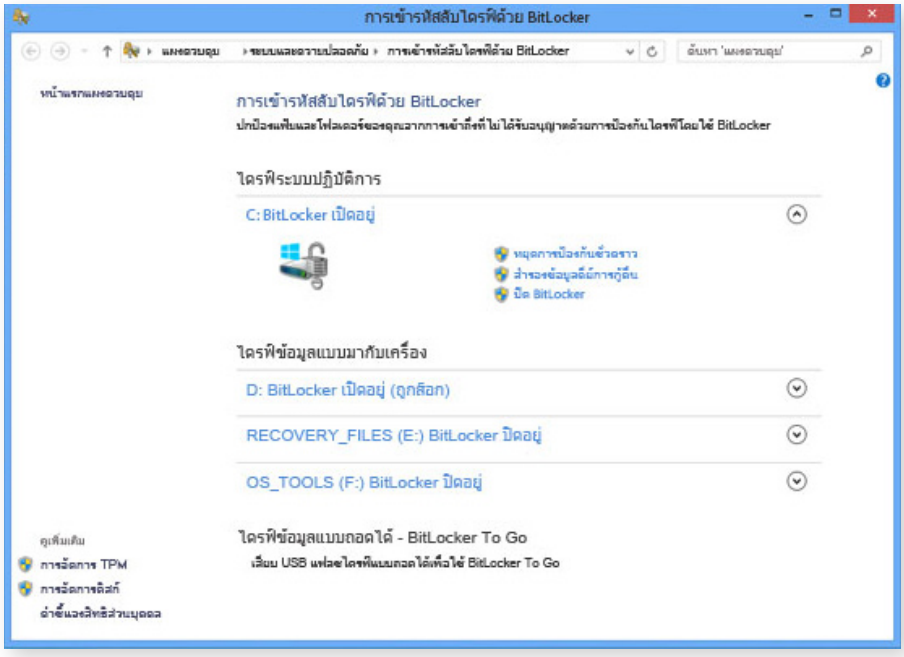
คุณสมบัติใหม่ของ BitLocker บน Windows 8 และ Windows Server 2012



BitLocker เป็นคุณสมบัติที่ช่วยป้องกันการเข้าถึงข้อมูลสำคัญจากผู้ที่ไม่มีสิทธิ์ โดยการเข้ารหัสข้อมูลที่เก็บอยู่ในไดรฟ์หรือพาร์ติชั่นด้วยรหัสผ่านตามที่ผู้ใช้กำหนด ไมโครซอฟท์เริ่มนำ BitLocker มาใช้ครั้งแรกใน Windows Vista ซึ่งในเวอร์ชั่นแรกนั้นสามารถทำการเข้ารหัสได้เฉพาะดิสก์ไดรฟ์ในส่วนที่ใช้เก็บข้อมูล หรือที่ติดตั้ง Windows อยู่เท่านั้น หลังจากนั้นใน Windows Vista SP1 ได้ปรับปรุง BitLocker ให้สนับสนุนการเข้ารหัสดิสก์ไดรฟ์ทั้งลูกได้ ต่อมาใน Windows 7 ได้เพิ่มคุณสมบัติ BitLocker to Go สำหรับใช้เข้ารหัสข้อมูลที่เก็บอยู่ในอุปกรณ์เก็บข้อมูลแบบพกพา เช่น ยูเอสบีแฟลชไดรฟ์ และฮาร์ดไดรฟ์แบบต่อภายนอก เป็นต้น และมาถึง Windows 8 และ Windows Server 8 คุณสมบัติ BitLocker ได้รับการปรับปรุงการทำงานให้มีความสามารถเพิ่มขึ้นในหลายด้าน ดังนี้

การทำโพรวิชั่นนิงของ BitLocker

ใน Windows 7 และ Windows Vista ผู้ใช้จะจัดเตรียมคุณสมบัติ BitLocker ได้หลังจากทำการติดตั้งระบบปฏิบัติการแล้วโดยใช้การติดต่อผ่านทางบรรทัดคำสั่ง manage-bde หรือทางระบบติดต่อผู้ใช้ของ Control Panel แต่ใน Windows 8 นั้นสามารถจัดเตรียมการเข้ารหัสได้ตั้งแต่ในระหว่างการติดตั้งระบบปฏิบัติการ

โดยใน Windows 8 ผู้ดูแลระบบสามารถเปิดใช้งาน BitLocker ได้ก่อนที่จะทำการติดตั้งระบบปฏิบัติการจาก Windows Preinstallation Environment (WinPE) ซึ่งจะทำการเข้ารหัสไดรฟ์ที่ถูกฟอร์แมตก่อนที่จะเริ่มกระบวนการติดตั้ง Windows หากเป็นการเข้ารหัสเฉพาะพื้นที่ดิสก์ที่มีการใช้งานเท่านั้น (Used Disk Space Only) จะทำให้กระบวนการติดตั้ง Windows ใช้เวลาเพิ่มขึ้นจากการติดตั้งแบบปกติเพียงไม่กี่วินาทีเท่านั้น

ในการตรวจสอบสถานะ BitLocker ของส่วนต่างๆ ในดิสก์ไดรฟ์นั้น ผู้ดูแลระบบสามารถดูสถานะของไดรฟ์ผ่านทางแผงควบคุม BitLocker หรือ Windows Explorer เมื่อไดรฟ์ถูกจัดเตรียมไว้ล่วงหน้าสำหรับ BitLocker จะแสดงสถานะเป็น “Waiting For Activation” พร้อมกับไอคอนตกใจสีเหลืองในแผงควบคุม โดยสถานะนี้หมายความว่ามีเพียงเครื่องป้องกันที่ถูกนำมาใช้เพื่อการเข้ารหัสของส่วนต่างๆ ในดิสก์ไดรฟ์เท่านั้น ในกรณีนี้ที่มีบางส่วนยังไม่ได้ได้รับการป้องกันก็จำเป็นต้องเพิ่มคีย์ความปลอดภัยให้กับส่วนนั้นเพื่อให้ไดรฟ์ได้รับการคุ้มครองอย่างเต็มที่

ผู้ดูแลระบบสามารถใช้แผงควบคุม เครื่องมือ manage-bde หรือ WMI API เพื่อเพิ่มตัวป้องกันคีย์ที่เหมาะสมและก่อนที่สถานะของโวลุ่มจะได้รับการอัพเดต ตารางต่อไปนี้แสดงให้เห็นถึงตัวป้องกันคีย์ที่เหมาะสมที่สามารถเพิ่มให้กับไดรฟ์ที่ได้รับการจัดเตรียมไว้ล่วงหน้าเพื่อการป้องกันด้วย BitLocker

การเข้ารหัสเฉพาะพื้นที่ดิสก์ที่มีการใช้งานเท่านั้น

ใน Windows 8 นั้น BitLocker เสนอวิธีการเข้ารหัสข้อมูล 2 แบบ คือ การเข้ารหัสเฉพาะพื้นที่ดิสก์ที่มีการใช้งานเท่านั้น (Used Disk Space Only) และการเข้ารหัสดิสก์ทั้งลูก (Full volume encryption) โดยการเข้ารหัสแบบแรกจะเป็นการเข้ารหัสเฉพาะบล็อคที่ถูกใช้งานบนดิสก์เป้าหมายทั้งลูกเท่านั้นจึงทำงานได้เร็วกว่า

เมื่อมีการจัดเตรียม BitLocker ในระหว่างการติดตั้งใช้งาน Windows การเข้ารหัสแบบเฉพาะพื้นที่ดิสก์ที่มีการใช้งานจะยอมให้ BitLocker ใช้เวลาเข้ารหัสไดรฟ์ก่อนจะทำการติดตั้งระบบปฏิบัติการสั้นกว่าส่วนการเข้ารหัสดิสก์ทั้งก้อนนั้นจะทำการเข้ารหัสดิสก์ไดรฟ์ทั้งส่วนที่มี

ประเภทของไดรฟ์	ตัวป้องกันคีย์
ระบบปฏิบัติการ	TPM TPM+PIN Startup Key (สำหรับระบบที่ไม่มี TPM) รหัสผ่าน (สำหรับระบบที่ไม่มี TPM)
ไดรฟ์ข้อมูลแบบติดตั้งกับที่	ปลดล็อกโดยอัตโนมัติ รหัสผ่าน สมาร์ทการ์ด
ไดรฟ์ข้อมูลแบบถอดได้	รหัสผ่าน สมาร์ทการ์ด

และไม่มีข้อมูลแบบเดียวกับใน Windows 7 และ Windows Vista

ทั้งนี้ ผู้ดูแลระบบสามารถใช้การตั้งค่านโยบายกลุ่มใหม่ในการเลือกรูปแบบการเข้ารหัสว่าจะใช้แบบเข้ารหัสเฉพาะพื้นที่ดิสก์ที่มีการใช้งาน หรือเข้ารหัสทั้งหมดก็ได้ โดยการตั้งค่านโยบายกลุ่มสำหรับ BitLocker Drive Encryption จะเก็บอยู่ที่ \Computer Configuration\ Administrative Templates\Windows Components\Bitlocker Drive Encryption path of Local Computer Policy and Domain Computer Policy

โดยมีนโยบายกลุ่มให้เลือก 3 ค่าดังนี้

- Fixed Data Drives\Enforce drive encryption type on fixed data drives
- Operating System Drives\Enforce drive encryption type on operating system drives
- Removable Data Drives\Enforce drive encryption type on removable data drives

การเปลี่ยนพินและรหัสผ่านของผู้ใช้ทั่วไป

ยอมให้ผู้ใช้ทั่วไป (Standard user) สามารถทำการเปลี่ยนพิน (PIN) หรือรหัสผ่านของ BitLocker บนโวลุ่มระบบปฏิบัติการและรหัสผ่านของ BitLocker บนโวลุ่มข้อมูลได้ ซึ่งจะช่วยลดภาระงานของทีมให้บริการช่วยเหลือลง

ตามปกติแล้วการกำหนดค่า BitLocker สำหรับไดรฟ์ระบบปฏิบัติการนั้นต้องใช้สิทธิ์ระดับผู้ดูแลระบบ และในองค์กรที่คอมพิวเตอร์ถูกการจัดการโดยเจ้าหน้าที่ด้านไอทีจะไม่ให้สิทธิ์ระดับผู้ดูแลระบบแก่ผู้ใช้มาตรฐาน ทำให้การปรับใช้ตัวเลือกการป้องกัน TPM + PIN กับเครื่องคอมพิวเตอร์จำนวนมากทำได้ยาก แต่ใน Windows 8 แม้ว่าการกำหนดค่า BitLocker จะยังคงต้องใช้สิทธิ์ระดับผู้ดูแลระบบ แต่โดยเริ่มต้นแล้วผู้ใช้งานปกติได้รับอนุญาตให้เปลี่ยนพิน หรือรหัสผ่านของ BitLocker สำหรับโวลุ่มระบบปฏิบัติการ หรือรหัสผ่านของ BitLocker สำหรับโวลุ่มข้อมูล ซึ่งจะช่วยให้ผู้ใช้มาตรฐานสามารถเลือกพิน และรหัสผ่านที่สามารถจดจำได้ง่ายกว่าการจำพินและรหัสผ่านที่กำหนดให้โดยเจ้าหน้าที่ด้านไอที

อย่างไรก็ตาม การที่ผู้ใช้สามารถเลือกใช้รหัสผ่านและพินได้เองอาจทำให้เกิดการเลือกใช้รหัสผ่านหรือพินที่มีจุดอ่อนและคาดเดาได้ง่าย ซึ่งอาจถูกโจมตีโดยใช้วิธีแบบพจนานุกรม และวิศวกรรมทางสังคมได้ ดังนั้นควรบังคับใช้การกำหนดรหัสผ่านที่มีซับซ้อนและพินที่เป็นไปตามนโยบายกลุ่มผ่านทางการกำหนดนโยบายกลุ่มเพื่อช่วยให้แน่ใจว่าผู้ใช้จะเลือกกำหนดรหัสผ่านและพินได้อย่างเหมาะสมและปลอดภัย

ในการเปลี่ยนพิน หรือรหัสผ่านของ BitLocker นั้นผู้ใช้มาตรฐานจะต้องป้อนพิน หรือรหัสผ่านปัจจุบันสำหรับไดรฟ์ หากผู้ใช้ป้อนพินหรือรหัสผ่านปัจจุบันไม่ถูกต้องเกิน 5 ครั้ง ผู้ใช้มาตรฐานจะไม่สามารถที่จะเปลี่ยนพิน หรือรหัสผ่านของ BitLocker โดยค่าเคาน์เตอร์จะรีเซตเป็น “0” เมื่อคอมพิวเตอร์ถูกรีสตาร์ทหรือผู้ดูแลระบบทำการรีเซต

ในกรณีที่ไม่ต้องการให้ผู้ใช้มาตรฐานเปลี่ยนพินหรือรหัสผ่านของ BitLocker ได้เอง ผู้ดูแลระบบสามารถปิดออปชั่นได้ผ่านทางการตั้งค่านโยบายกลุ่ม Disallow standard users from changing the PIN ซึ่งเก็บอยู่ที่ \Computer Configuration\ Administrative Templates\Windows Components\BitLocker Drive Encryption\ Operating System Drives โดยใช้เครื่องมือ Group Policy Editor

Network Unlock:

Windows Server 8 จะเพิ่มออปชั่นชื่อ Network Unlock ซึ่งเป็นตัวป้องกัน BitLocker ตัวใหม่สำหรับดิสก์ไดรฟ์ที่ใช้ติดตั้งระบบปฏิบัติการ ซึ่งทำให้การจัดการเซิร์ฟเวอร์และเดสก์ท็อปที่มีการเปิดใช้ BitLocker ในสภาพแวดล้อมแบบโดเมนทำได้ง่ายขึ้น โดยการจัดเตรียมการปลดปลดล็อคดิสก์ไดรฟ์โดยอัตโนมัติเมื่อรีบูทระบบและเชื่อมต่อผ่านระบบเครือข่ายแบบสายที่มีความน่าเชื่อถือ อย่างไรก็ตามคุณสมบัตินี้ต้องใช้ฮาร์ดแวร์ไคลเอ็นต์ที่รองรับไดรเวอร์ DHCP ในเฟิร์มแวร์ UEFI

รองรับฮาร์ดไดรฟ์ที่ถูกเข้ารหัสสำหรับ Windows

ก่อนหน้านี้ BitLocker นั้นจะจัดเตรียมการเข้ารหัสดิสก์ไดรฟ์ที่ใช้เก็บข้อมูล และระบบปฏิบัติการ Windows แบบ Full Volume Encryption (FVE) แต่ใน Windows 8 นั้น BitLocker ที่มีฟังก์ชั่น Encrypted Hard Drive ซึ่งสนับสนุนการเข้ารหัสฮาร์ดไดรฟ์ทั้งลูก (Full Disk Encryption-FDE) ได้ ซึ่งเป็นการเข้ารหัสในระดับบล็อคข้อมูลของฮาร์ดดิสก์ทางกายภาพทำให้มีประสิทธิภาพการทำงานมากขึ้นเนื่องจากเป็นการเข้ารหัสบนตัวฮาร์ดแวร์ที่ไม่ขึ้นกับตัวควบคุมการจัดเก็บบนฮาร์ดไดรฟ์

Windows 8 สนับสนุนฮาร์ดไดรฟ์ที่ถูกเข้ารหัสแบบเนทีฟในระบบปฏิบัติการผ่านทางกลไกดังนี้

- **Identification:** Windows 8 จะสามารถระบุได้ว่าไดรฟ์ใดถูกเข้ารหัสแบบ Encrypted Hard Drive
- **Activation:** เครื่องมือจัดการดิสก์ของ Windows 8 จะสามารถเปิดการใช้งาน สร้าง และแมพส่วนของดิสก์ไดรฟ์เป็นช่วง/กลุ่มตามความเหมาะสม
- **Configuration:** Windows 8 จะสร้างและแมพส่วนต่างๆ ของดิสก์ไดรฟ์โวลุ่มเป็นช่วง/กลุ่มตามความเหมาะสม
- **API:** Windows 8 ได้เตรียม API สนับสนุนแอพพลิเคชั่นสำหรับจัดการฮาร์ดไดรฟ์ที่ถูกเข้ารหัสไว้อย่างอิสระจาก BitLocker Drive Encryption
- **BitLocker:** ผู้ใช้สามารถใช้แผงควบคุม BitLocker ในการจัดการฮาร์ดไดรฟ์ที่ถูกเข้ารหัสไว้ในลักษณะเดียวกันกับการจัดการการเข้ารหัสส่วนต่างๆ ของดิสก์ไดรฟ์ทั้งหมดได้