Vista BitLocker

磁盘加密向导

Vista BitLocker 磁盘加密向导

BitLocker 是微软 Vista 企业版和旗舰版（Vista Enterprise and Ultimate）中的一个功能，可以加密系统磁盘。这一点在 Windows 之前的版本中，如果没有第三方产品是不可能实现的。为了使用 BitLocker，需要有可信平台模块（Trusted Platform Module，TPM）硬件的系统，1.2 版本或者更好的。现在有些 PC 厂商已经开始支持了，虽然需要额外付费。

但是如果想要在没有 TPM 的系统上使用 BitLocker 应该怎么办呢？

本技术指南将介绍如何启动 BitLocker，并在没有 TPM 的电脑上运行的方法，以及没有它的时候需要什么，应该怎么做以及可以获得的结果等。

BitLocker 加密简介

BitLocker 是微软 Vista 企业版和旗舰版中的一个功能，可以加密系统磁盘。为了使用 BitLocker，需要有可信平台模块（Trusted Platform Module，TPM）硬件的系统，1.2 版本或者更好的。大部分的电脑都没有 TPM，而且还不能在增加 TPM。

- BitLocker 加密没有 TPM 的 Vista 之一：简介

BitLocker 加密准备工作

在没有 TPM 的 Vista 中，如果要使用 BitLocker 加密系统磁盘，应该首先做以下准备：了解你的硬件，需要有可移动 USB 存储设备和可以从 USB 设备启动系统的 BIOS；配置磁盘；编辑本地策略。本部分将分步介绍这些准备工作。

- BitLocker 加密没有 TPM 的 Vista 之二：了解硬件

- BitLocker 加密没有 TPM 的 Vista 之三：配置磁盘
- BitLocker 加密没有 TPM 的 Vista 之四：编辑本地策略

BitLocker 加密过程

经过上面的步骤，就做好了开始使用 BitLocker 做磁盘加密的准备。要准备好，BitLocker 加密磁盘这个过程需要很长时间，可能要几个小时，这取决于磁盘上数据的多少。以下分为十个步骤详细介绍。

- BitLocker 加密没有 TPM 的 Vista 之五：开始 BitLocker 加密

BitLocker 加密没有 TPM 的 Vista 之一：简介

BitLocker 是微软 Vista 企业版和旗舰版（Vista Enterprise and Ultimate）中的一个功能，可以加密系统磁盘。这一点在 Windows 之前的版本中，如果没有第三方产品是不可能实现的。为了使用 BitLocker，需要有可信平台模块（Trusted Platform Module，TPM）硬件的系统，1.2 版本或者更好的。现在有些 PC 厂商已经开始支持了，虽然需要额外付费。

但是如果想要在没有 TPM 的系统上使用 BitLocker 应该怎么办呢？大部分的电脑——特别是大部分现有的电脑——都没有 TPM，而且还不能在电脑上增加 TPM。它可能是系统设计的一部分，也可能不是。

还好，微软已经把一些产品植入到 BitLocker 中了，使其可以在没有 TPM 的系统上使用。在这一系列文章中，我将介绍如何启动 BitLocker，并在没有 TPM 的电脑上运行的方法，以及没有它的时候需要什么，应该怎么做以及可以获得的结果等。

注意：*在对磁盘上的数据进行完全备份前，不要执行这些步骤！* 这个过程完全是自己主导的，很可能会出现一些错误。如果磁盘上有一些不可替代的内容，在加密磁盘前先进行备份。

（作者：Serdar Yegulalp　译者：Tina Guo　来源：TechTarget 中国）

BitLocker 加密没有 TPM 的 Vista 之二：了解硬件

在没有 TPM 的 Vista 中，使用 BitLocker 加密系统磁盘所需要的基本的硬件要求如下：

1. 可移动 USB 存储设备。我也说过，如果没有 TPM 系统，使用 BitLocker 的第二种方法是使用写入到移动 USB 闪存的加密密钥。

2. 可以从 USB 设备启动系统的 BIOS。带有 BitLocker 密钥的 USB 设备必须连接，并且在系统第一次启动的时候必须可以通过 BIOS 可读；这就是 BitLocker 需要系统可以从 USB 设备启动并工作的原因。

注意：对有些电脑来说，可能通过集线器插入 USB 设备，并且仍然可以在导入的时候在电脑上可见。但是，不是总是可以。如果你的系统使用外部集线器，可能你就想要实验一下，查看导入的时候可以看到那些端口。

如果你的电脑没有 TPM，而且不能从 USB 设备启动，仍然可以使用 BitLocker，但是会有些繁琐。BitLocker 可以通过 48 位数字的恢复密码，可以在启动系统的时候使用。不能手动设置恢复密码，而且它的长度也不是用户可以设置的，所以把恢复密码当作启动电脑的标准方法有些困难。

（作者：Serdar Yegulalp 译者：Tina Guo 来源：TechTarget 中国）

BitLocker 加密没有 TPM 的 Vista 之三：配置磁盘

为了在系统上安装 BitLocker，Vista 的启动文件必须在独立的位置。需要在安装前通过创建至少两个区来设置：大约 2G 的启动区和全面的系统区。需要独立的启动区是为了允许启动文件自己不要加密。微软的设置 BitLocker 指南详细描述了这一过程。

为了可以在使用 Vista 的系统上使用 BitLocker，需要使用 Vista 企业版和旗舰版（Vista Enterprise and Ultimate）的附加软件之一，就是 **BitLocker Drive Preparation Tool**。Drive Preparation Tool 可以允许用户准备只有一个分区的系统，或者不兼容的分区设置来使用 BitLocker。Preparation Tool 通过在现有系统分区（通常命名是磁盘：S）的终端创建新的启动分区，并在这里复制启动负载，并把这个分区设置为可以启动的。一旦安装完成，通过 Microsoft Update，启动就相当容易了：

1. 点击“**开始**”并在搜索框中键入 BitLocker。
2. 点击 **BitLocker Drive Preparation Tool**。
3. 点击“**我接受**”来接受专利使用权转让协议。
4. 根据提示，创建新的系统启动区。在这个过程中需要重启电脑。

如果已经运行了 Vista 系统，想要在上面增加 BitLocker，这个功能就会让事情变得简单，而不需要卸载系统。重新分区，并重装 Vista。

（作者：Serdar Yegulalp　译者：Tina Guo　来源：TechTarget 中国）

BitLocker 加密没有 TPM 的 Vista 之四：编辑本地策略

在默认情况下，BitLocker 只能在拥有 TPM 的时候才能起作用；如果没有 TPM，它也不会出现。这种设备是作为 Group Policy 限制而强制实施的，所以需要编辑 Group Policy，做些更改。

1. 点击**开始，运行**。
2. 键入 **gpedit.msc**，回车。这样就可以触发 UAC 确认警告。点击“**确认**”继续。
3. 继续进行 **Local Computer Policy、Computer Configuration、 Administrative Templates、Windows Components、BitLocker Drive Encryption**。
4. 双击**控制面板设置**：激活高级启动选型，然后点击“**激活**”激活策略上的变更。
5. 在 **Allow BitLocker without a compatible TPM** 窗口应该自动核对，如果不是，就勾选。
6. 点击确定。
7. 关闭 Group Policy 编辑器。
8. 退出，再登录使变更生效。

注意，在 BitLocker Drive Encryption 策略控制台中还有一些其它的选项，例如选择磁盘加密方法，或者选择是否把 BitLocker 密钥备份到 Active Directory 域名中。

（作者：Serdar Yegulalp 译者：Tina Guo 来源：TechTarget 中国）

BitLocker 加密没有 TPM 的 Vista 之五：开始 BitLocker 加密

在重启后，你就做好了开始使用 BitLocker 做磁盘加密的准备。要准备好，这个过程需要很长时间，可能要几个小时，这取决于磁盘上数据的多少。虽然如此，电脑在这个过程中还是可以用的——只是可能很慢。我的建议是在加密完成前不要使用电脑做任何事情。

开始加密过程：

1. 点击**开始**，在搜索框中键入 **BitLocker**。选择“**BitLocker 加密磁盘**”（页可以从控制面板中启动 BitLocker。）
2. 这时应该查看可以使用 BitLocker 加密的磁盘数列表（特别是 C 盘）。如果你看到了黄色的警告——例如，这是警告说没有 TPM 硬盘——然后回来确定已经正确的执行了前面的设置。
3. 点击系统磁盘（通常还是 C 盘）的“**打开 BitLocker**”，然后开始配置磁盘的 BitLocker。
4. 下面就会出现一系列的选项：在没有附加密钥的情况下使用 BitLocker，**在每次启动的时候都要求 PIN，并在每次启动的时候要求启动 USB 密钥。**只有最后一条（要**求启动 USB 密钥**）都应该高亮，所以点击开始。
5. 应该显示“**保存启动密钥**”。插入用以存储 TPM 密钥的 USB 可移动磁盘，并等待它的驱动器名在窗口中显示。（如果没有显示驱动器名，就不能杯格式化。）
6. 点击“**保存**”来保存启动密钥。
7. 然后就可以看到不同位置上保存 BitLocker 恢复密码的选项：文件夹、USB 驱动或者打印的文件。暂时要保存至少两份恢复密码；之后可以做更多的备份，或者删除现在的备份。
8. 在下一页就会有运行 BitLocker 检查的选项。这需要重新启动并确保 BitLocker 启动密钥可以在启动的时候阅读。如果你不能确定系统是否支持通过 USB 启动，可

以运行这个测试。系统可以重新启动，如果测试不成功，就会在下次 Vista 启动的时候受到警告。如果发生了，加密后启动系统的唯一的方法是使用恢复密码。

注意：可以把恢复密码保存到存储启动密约的 USB 设备中，但是这样做不太好。如果别人使用了 USB 设备，这个人就不需要启动使用设备你的电脑就知道如何攻击它。

注意之二：如果可以不要在不启动 Vista 的别的时候，使用启动密约。我认为可以在创建了启动密钥后启动写保护，这样就没有副作用了。而且还不能用以作其他事情，否则可能会对它造成破坏。

9. 这时就会出现实际启动加密过程的选项。在作的时候，就可以看到进程条，如果需要可以暂停或者恢复加密过程。在加密完成前不要关机或者重启系统。

10. 当完成加密后，可以重启电脑。之后在每次启动的时候，都必须插入 USB 密钥，并在启动的时候可见，或者会提示你键入恢复密码在继续。

注意：如果不能检查 BitLocker，而且想要加密磁盘，就需要重新执行这些步骤，并选择运行 BitLocker 检查。还有，要确保通过 USB 端口连接的磁盘可以在启动的时候首先被阅读。

（作者：Serdar Yegulalp　译者：Tina Guo　来源：TechTarget 中国）