Settings”面板的“Service Control”栏的“Service”列表中可以改变Secure It Easy服务的运行状态（包括自动、手动、禁止等）。在默认状态下，其处于自动运行状态，点击“Stop”按钮可以停止该服务（图6）。

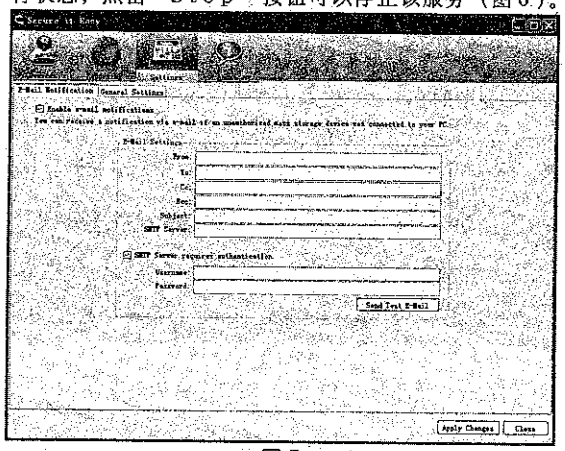

图5

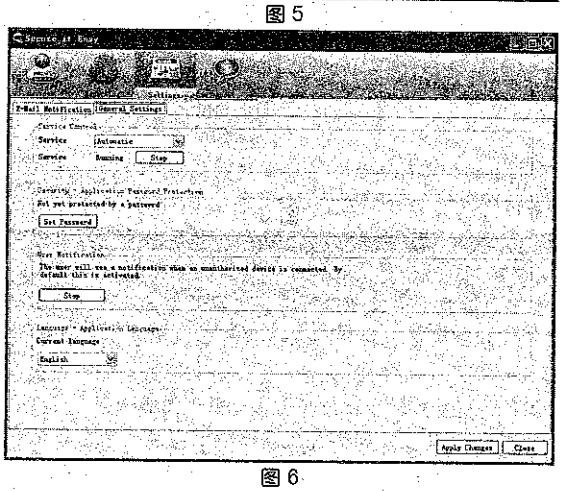

图6

在“Security—Application Password Protection”栏中点击“Set Password”按钮，可以为Secure It Easy设置管理密码，这样在打开其管理窗口时就必须输入预设的密码，防止对其进行配置操作，这样可以有效的防止其他人随意更改USB设备的使用状态。在默认状态下，当插入USB设备时，Secure It Easy都会弹出拦截信息，这在很大程度上会“暴露”其“行踪”，在“User Notication”栏中点击“Stop”按钮，可以取消其信息提示功能，便于增强其运行的隐蔽性。为了加强对USB设备使用的情况进行统计，Secure It Easy提供了日志记录功能，可以精确的记录所有USB设备的使用情况。在Secure It Easy管理窗口工具栏中点击“Report”按钮，在“Log File”面板的日志列表中显示了所有USB设备的使用情况，包括连接的时间、描述信息、VID、PID、串行号、计算机名称、帐户信息、动作（包括连接、激活、禁用等状态）等信息，让我们可以对本机上USB设备的使用情况一目了然（图7）。在“Log Size Limit”栏中可以设置日志文件的大小，选择“By Days”项，可以按照日、月、星期、年份为单位设置日志记录的有效期。选择“By Size”项，可以按照容量的大小（包括KB、MB、TB等单位）来设置日志文件的大小。如果选择“Disabled”项，表示日志文件的大小不受任何限制。点击“Clear Log”按钮可以清空日志信息。在“Export Log”栏中可以设置日志文件的导出路径，点击“Export”按钮将日志文件导出后单独保存。

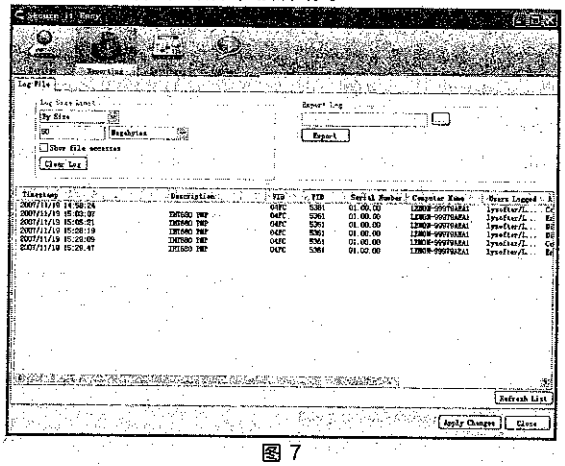

图7

三、使用MyUSBOnly为USB端口加密

MyUSBOnly可以将自身添加到系统启动项中，这样可以跟随系统自动运行。MyUSBOnly的运行机制比较特殊，其采用了和大多数防火墙软件类似的黑白名单管理机制，对于经过认证的USB设备将其添加到白名单中，对于禁用的USB设备将其添加到黑名单中。在系统托盘中的MyUSBOnly图标的右键菜单中选择“General Setup”项，在弹出的MyUSBOnly登录对话框中输入密码（初始密码为“0000”），在MyUSBOnly管理窗口左侧点击“Device Whitelist”项（图8），在右侧窗口可以执行USB设备的认证操作，点击“Start Detect”按钮，然后插上所需的USB设备，点击“Detect”按钮，在认证列表中即可显示当前连接的所有USB设备，选中允许正常使用的USB设备的名称，点击“Add to Whitelist”按钮，即可将其添加到“Device Name Whitelist”列表中，该列表中的所有设备都可以正常使用，之外的USB设备则禁止使用。最后点击“Save”按钮保存白名单设备。然后重新连接通过认证的USB设备，就可以正常加载使用了。按照上述方法，你可以非常方便的管理USB设备。

在MyUSBOnly管理窗口左侧点击“General Setup”项，在右侧窗口的“Setup Window Access Password”栏中可以更改MyUSBOnly的登录密码，这样就可以禁止其他人随意更改你的USB设备白名单。默认情况下，在系统托盘中会显示MyUSBOnly的图

标，为了加强其运行的隐蔽性，可以取消“Display tray icon”项的选择，这样可以让MyUSBOnly图标从在系统托盘中消失（图9）。当然你也可以随时点击“Ctrl＋F5”热键来打开其管理窗口。取消“Instant prompt for unknown USB storage device”项的选择，可以在连接USB设备时，禁止MyUSBOnly弹出相关的提示信息。这样，MyUSBOnly就可以悄无声息的禁用该USB设备，从表面上给人造成系统出错或者USB端口损坏的假象。

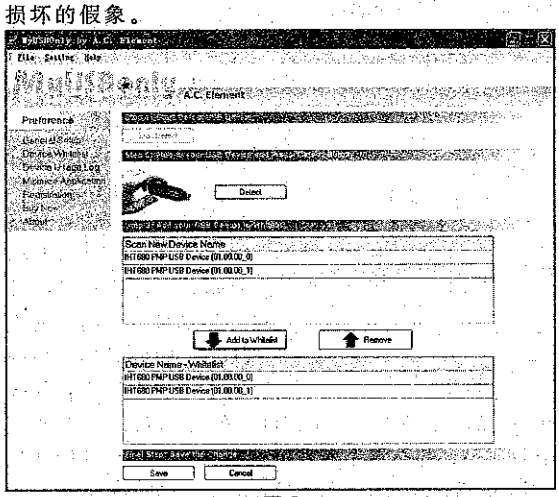

图8

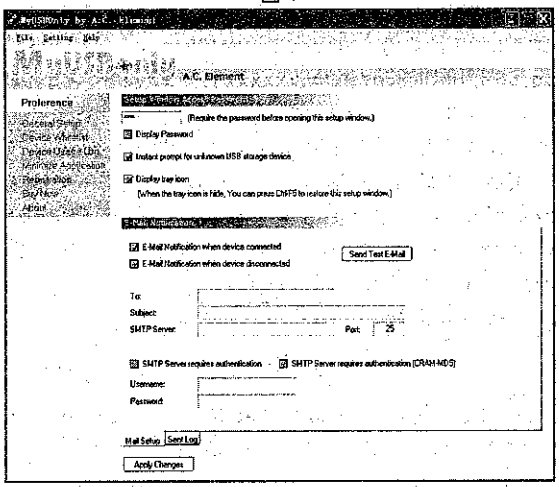

图9

MyUSBOnly不仅可以监视USB设备的使用情况，还可以同时向你发送报警邮件。在“E-Mail Notication”栏中勾选“E-Mail Notification when device connected”和“E-Mail Notification when device disconnected”项；表示当连接或者移除USB设备时，可以向预设的邮箱发送报警邮件。在其下可以设置收件人地址、邮件主题、SMTP服务器地址，勾选“SMTP Server requires authercation”项，可以设置SMTP服务器的帐户名称和密码信息，点击“Send Test E_Mail”按钮，可以发送测试邮件。当然，你可以随时打开“Sent Log”面板，在其中查看所有发送的报警邮件信息。最后点击“Apply Changes”按钮保存配置。为了便于统计USB设备的使用情况，在MyUSBOnly管理窗口左侧点击“Device Usage Log”项，在右侧窗口中显示完整的日志信息，依次包括USB设备的名称、分配的盘符、采取的动作（连接或者拔出）、是否经过MyUSBOnly的认证、连接或者拔出的时间等。让你能够清晰的了解USB设备连接使用情况。

四、使用Driver Block为移动设备加锁

同以上软件相比，Driver Block是一款小巧精悍的移动设备管理工具，能够很方便的激活或者禁用所有的移动存储设备。在Driver Block安装程序的“Input administrator password”窗口中勾选“Conceal password while typing”项，表示不显示输入的密码信息，在“Input Password”和“Repeat Password”栏中输入密码，点击OK按钮即会打开“Input Supervisor password”窗口，在其中可以设置超级用户密码，这样如果忘记了管理密码，还可以使用超级用户密码为Driver Block解锁。在任务栏系统托盘中双击Drive Blocker图标，在主窗口的“Removable Drives Status”栏中显示“Locked”字样（图10），表示当前的所有移动存储设备全部处于锁定状态，不管连接任何移动存储设备，Drive Blocker都会抢在Windoww对其正常加载使用前禁用该设备。同时造成Windows无法正常管理可移动存储设备的情况，系统会弹出“拒绝访问”的警告窗口，这样其他人就无法在本机上使用移动存储设备了。当你想使用移动存储设备时，可以在Drive Blocker主窗口的“Password”栏中输入管理密码或者超级用户密码，点击“Unlock Drives”按钮，在“Removable Drives Status”栏中显示“Unlocked”信息，表示解除了移动存储设备的锁定状态，然后就可以正常连接和使用各种移动存储设备了。当点击“Lock Drives”按钮，可以重新锁定所有的移动存储设备。Drive Blocker采用了特殊的进程保护机制，别人无法在Windows的任务管理器中终结其运行。在默认情况下，Drive Blocker将自身添加到系统启动项中，可以跟随系统自动运行。如果需要卸载Drive Blocker，必须在其管理窗口中点击菜单“Files”→“Uninstall Driver Block”项，输入正确的管理密码或者超级用户密码后，才可以将其彻底卸载。

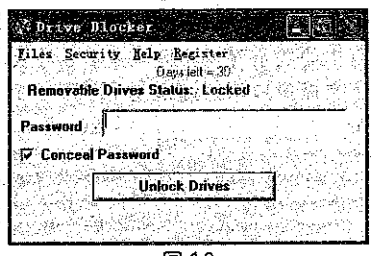

图10

（本文所涉及到的Secure Endpoint USB、Secure It Easy、MyUSBOnly和Driver Block已收录到光盘中）