



鼎昌外存设备访问监控平台

(mobile Storage Media Management DC-SMM)

使 用 手 册

郑州鼎昌计算机科技有限公司

目录

前言	3
第一章 产品简介	3
1.1 产品介绍	4
1.2 产品功能	4
1.3 产品优势	6
第二章 安装、卸载	7
2.1 服务端安装	8
2.2 客户端安装	13
2.3 卸载	13
2.3.1 服务端卸载	14
2.3.2 客户端卸载	16
第三章 管理员使用指南	17
3.1 登陆及配置	17
3.1.1 登陆	17
3.1.2 修改密码	18
3.2 主界面介绍	20
3.2.1 设备管理	20
3.2.2 使用记录	21
3.2.3 分组管理	21
3.3 操作指南	21
3.3.1 分组管理	21
3.3.2 设备管理	29
3.3.3 使用记录	37
第四章 用户使用指南	41
4.1 内部安全 U 盘的使用	44
4.2 外部安全 U 盘的使用	46
第五章 联系我们	50

前言

一、目的

编写本使用说明书的目的是充分叙述本软件所能实现的功能及其运行环境，以便使用者了解本软件的使用范围和使用方法。

二、用户手册的使用

第一章 产品简介

第二章 安装、生成、启动

第三章 管理员使用指南

第四章 用户使用指南

三、阅读说明

【注意】需要着重指出，以便提醒用户在实际操作中谨慎应对、处理的情况。

【说明】对一些问题或者情况所做出的解释和说明。

【建议】为发挥更好的使用效果，体现本产品的优异性能而给出意见或建议。

第一章 产品简介

1.1 产品介绍

在我国，政府部门、企事业单位已经越来越多地使用 USB 外存设备来传输文件，但在此过程中也存在相当大的安全隐患，因此加强对 USB 外存设备的管理也成为我们防范信息泄漏工作重中之重。

鼎昌科技针对当前企事业单位对外存设备安全隐患的迫切需求，自主研发了集外存设备管理、外存设备登记、操作记录登记于一体的“鼎昌外存设备访问监控平台”，该系统可根据管理员制定的策略分类管理外存设备，有效保证了信息的安全性。

1.2 产品功能

➤ 设备登记

外存设备必须经过注册认证才能使用，未认证的外存设备在内部不能使用。

- 建立外设与人员对应关系，方便对设备使用者的监管；
- 设备统一管理和控制；
- 方便查询和随时设置设备的使用权限。

➤ 设备在内部使用控制

外存设备未经许可无法在内部计算机上使用，必要时可以在指定计算机上使用。

用外存设备，通过设置外存设备使用权限和范围，控制设备在内部的使用。

- 防止外存设备任意访问他人或其他部门机器；
- 防止内部信息未经许可被拷贝。

➤ 设备在外部使用控制

设置外存设备在外部使用权限，外存设备未经许可无法在外部计算机上使用；根据选择的安全策略，划分安全区与普通区，经过授权的设备在外部使用，其操作全部保存有操作记录，追踪设备的外部使用情况。

- 防止外存设备在外部任意使用；
- 防止将涉密数据未经允许通过外存设备流出。

➤ 设备在内部可使用范围控制

外存设备经过登记，内部使用时需要设置外存设备在内部的使用范围，只能在自己所属的范围内使用，超出规定范围无法使用。

- 重要部门或机器不允许外存设备随意访问；
- 防止任意外存设备接触重要涉密文件信息。

➤ 日志审计

外存设备所有使用、操作都留有详细记录，便于对外存设备使用情况进行安全审计。

- 通过查看使用记录，分析是否存在泄密隐患；
- 数据泄露时可以分析查询日志，查找根源，确定泄密事件，追踪泄密责任。

➤ 分组管理

人员分组、机器分组可按照单位内部组织结构进行统一管理。

1.3 产品优势

※ 简单的操作界面

向导式工作模式，友好的提醒界面，用户可轻松上手。

※ 灵活的系统设置

通过系统设置可对所管理的每一个外设进行设置，权限包括只读、读写、禁止访问、访问期限、使用范围、外部使用划分安全区与普通区等。

※ 真正的设备监控

底层驱动开发，从外设接入系统开始，直到外设离开系统，实行全程监控。

※ 完善的操作记录

可以监控记录每次设备从进入系统到退出系统全过程的操作，包括进入、退出系统的时间、复制、删除等所有进行的操作。

※ 丰富的查询与报表

可以查询某个存储设备某段时间的使用情况，可以查找某个文件被哪些存储设备拷贝过，查询结果可以按照制定的字段输出。

第二章 安装、卸载

产品安装前准备

鼎昌外存设备访问监控平台包含服务端和客户端，正常使用必须遵循以下最低配置的软硬件环境。

服务端配置环境

CPU	Intel 奔腾 1.6GHZ 以上处理器
内存	2G
硬盘	400G
操作系统	Windows Server 2000 、 Windows Server 2003 及 Windows xp ；
监视器应用件	246 色，最小分辨率 800*600 像素
应用软件	IE6.0 以上
硬件接口	USB2.0

客户端配置环境

CPU	Intel 奔腾 1.6GHZ 以上处理器
内存	2G
硬盘	40G
操作系统	Windows Server 2000 、 Windows Server 2003 及

	Windows xp ;
监视器应用件	246 色，最小分辨率 800*600 像素
硬件接口	USB2.0

注意：

- 1.服务端在安装完成后会自动释放客户端程序。
- 2.安装前请卸载鼎昌外存设备访问监控平台原有版本，并删除原有文件目录。
- 3.安装前确认安装机器是否安装有 mysql 数据库，如果原来机器安装有 mysql 数据库，需知道 mysql 数据库密码。如果没有安装，鼎昌外存设备访问监控平台自行安装，mysql 数据库默认用户名 root，密码：dc123.

2.1 服务端安装

双击服务端安装程序 USBSetup.exe，解压安装包如图 2-1 所示：

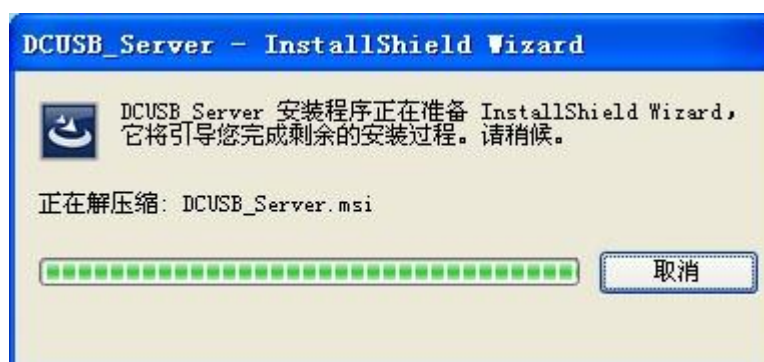


图 2-1

进行安装，进入欢迎界面，如图 2-2 所示：



图 2-2

单击“下一步”，同意鼎昌软件使用协议，出现如图 2-3 所示：

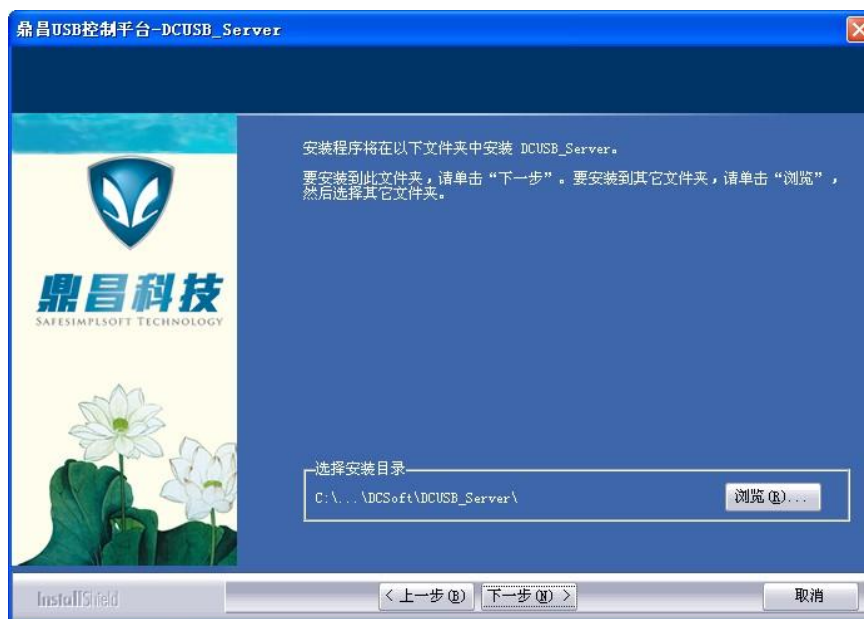


图 2-3

单击“浏览”可以更改其安装路径，如图 2-3 所示：



图 2-3

选择需要安装的路径，单击确定，单击“下一步”，选择安装 Mysql 数据库、控制程序、释放客户端安装包，如图 2-4 所示：



图 2-4

单击“下一步”，如图 2-5 所示：



图 2-5

单击“安装”，如图 2-6 所示：

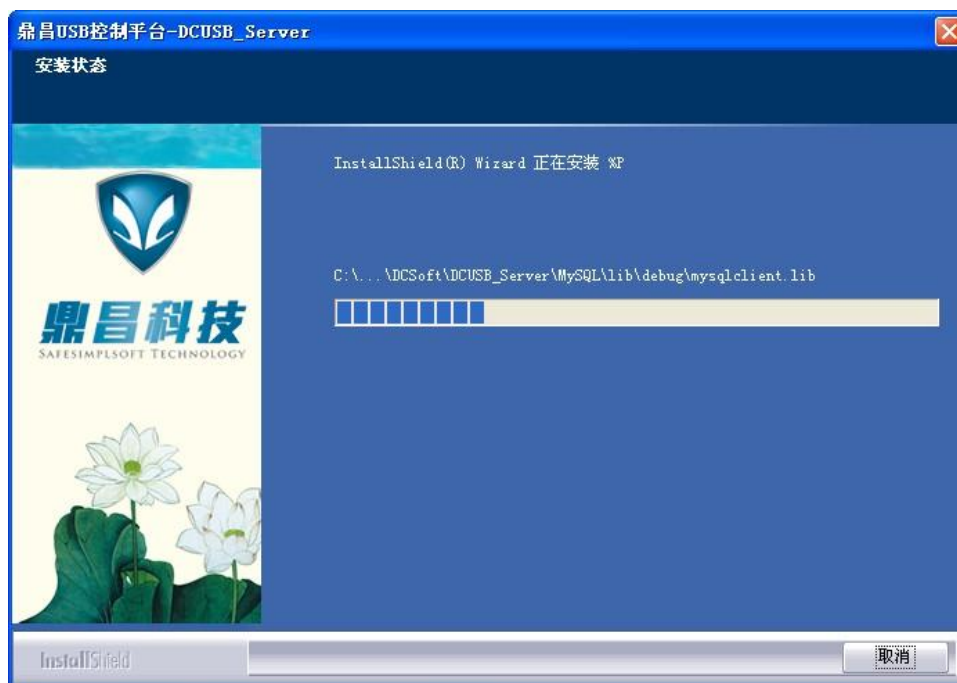


图 2-6

完成安装，如图 2-7 所示：



图 2-7

安装界面消失，桌面生成“USB 控制”、“安全 U 盘”两个图标，如图 2-8 所示：



图 2-8

开始菜单的程序中生成服务端及安全 U 盘，如图 2-9 所示：



图 2-9

同时生成和释放客户端安装程序，如图 2-10 所示：

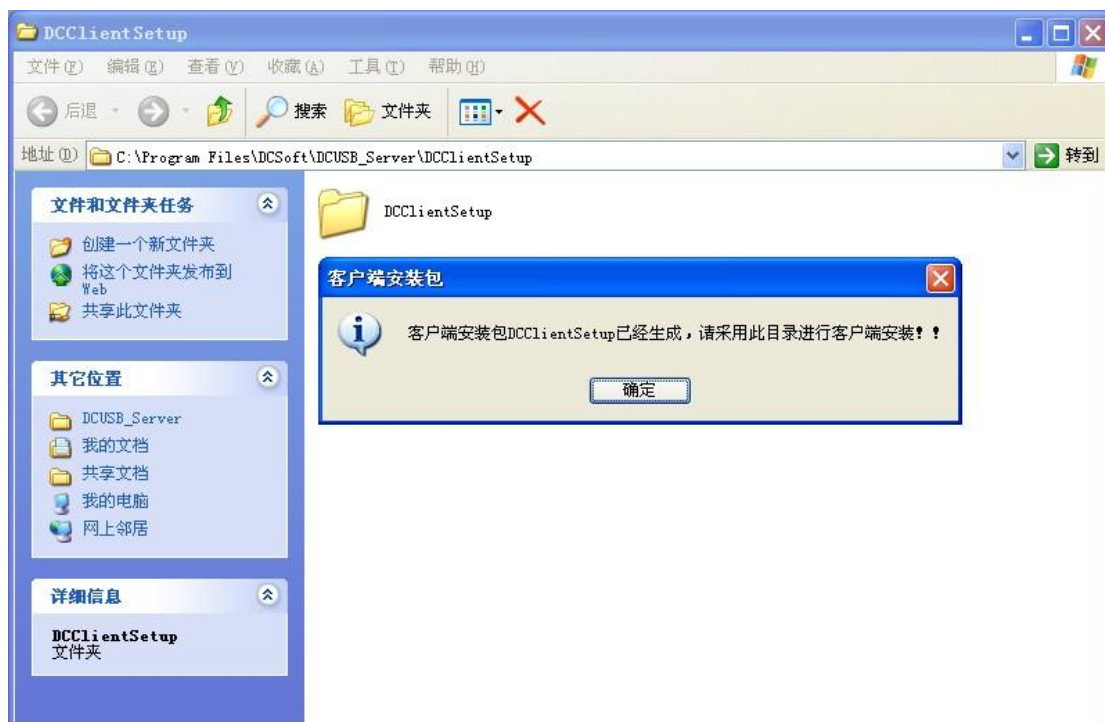


图 2-10

2.2 客户端安装

服务端安装完成后释放到桌面上的客户端安装包“DCClientSetup”（位服务端安装目录下），将此文件夹发送到需要安装客户端的机器上，双击 ClientSetup.exe 进行安装，具体操作步骤可参考服务端安装过程。

2.3 卸载

本程序自带有卸载程序，软件卸载时需要输入卸载密码。

注意：

软件卸载密码默认为 dingchangkeji，用户需要设置卸载密码时，请与鼎昌科技技术部联系。

2.3.1 服务端卸载

单击“开始->程序->DCSoft->USB_Server->USB 卸载”如图 2-11 所示：

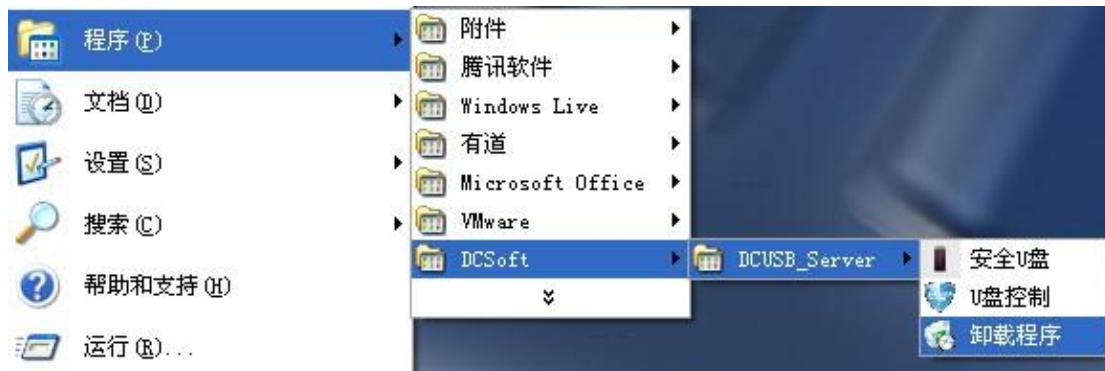


图 2-11

单击“卸载程序”后出现如图 2-12

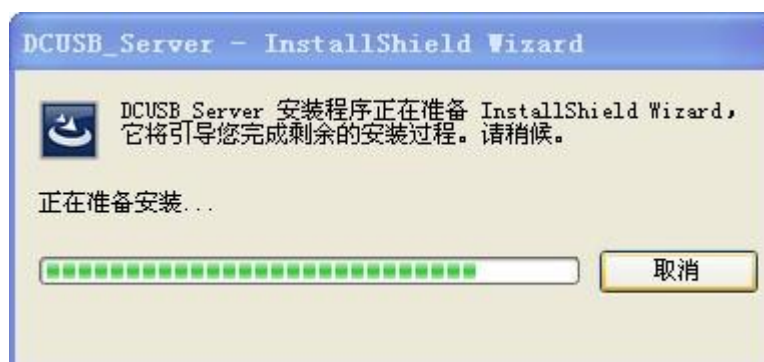


图 2-12

在等待几秒钟后，如图 2-13 所示：



图 2-13

输入正确的卸载密码，确定方可允许卸载。单击“下一步”，开始卸载，如图 2-14 所示：



图 2-14

单击“下一步”，开始卸载。

2.3.2 客户端卸载

单击“开始->程序->DCSoft->USB_Client->卸载 USB”，如图 2-15 所示：



图 2-15

单击“卸载程序”，接下来的步骤参考服务端卸载步骤。

第三章 管理员使用指南

3.1 登陆及配置

3.1.1 登陆

登陆方式有两种：

第一种：双击桌面快捷图标“USB 控制.exe”，出现登陆界面，如图 3-1 所示：



图 3-1 登陆

第二种：点击“开始->程序->DCSoFe->DCUSB_Server->USB 控制.exe”。

输入正确的密码用户名和密码，点击“登陆”即可登陆。

注意：登录前，首先要插入加密锁，否则在登录系统时会出现提示，如图 3-2

所示：

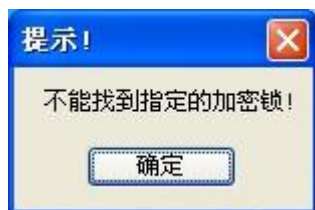


图 3-2 加密锁检测

【说明】

该系统初始用户名为 admin，密码为“4000013851”，请登录时及时修改密码。

3.1.2 修改密码

为了保证系统的安全性，建议管理员首次登录时修改密码，单击“修改密码”出现修改密码对话框，如图 3-3 所示：



图 3-3 修改密码

输入原有密码，然后根据要求输入新密码和重复新密码，新密码长度不小于 5 位。如果密码长度小于 5 位，出现提示，如图 3-4 所示：

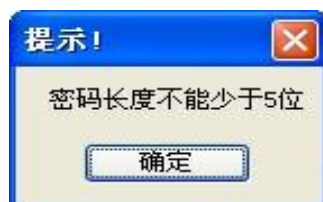


图 3-4 密码长度检测

设置数据库连接信息，点击“测试连接”，如图 3-5 所示：



图 3-5 数据库连接

点击“确认”，如图 3-6 所示：



图 3-6 保存成功

3.2 主界面介绍



图 3-7 主界面

3.2.1 设备管理

设备管理包括设备登记和已登记设备信息两部分内容。

(1) 设备登记

当插入 USB 外存设备时，系统自动显示设备信息，管理员可以设置设备内部使用权限的读写权限、设置设备的持有者、有效期限及使用范围，外部使用权限的普通区与安全区划分以监控传操作记录。

(2) 已登记设备信息

显示所有登记过的设备信息、当前插入设备信息。

3.2.2 使用记录

显示所有已登记设备的使用记录，包含人员分组、持有者、操作类型、操作时间、厂商代号、产品代号、序列号、目标机器名、目标机器 IP 地址、目标机器 MAC 地址、目标机器硬盘序列号、目标机器分组。

3.2.3 分组管理

分组管理包括人员分组和机器分组两部分内容。

(1) 人员分组

可以进行添加分组、添加人员，更改人员分组、删除。

(2) 机器分组

可以进行添加分组、搜索机器、更改机器分组、删除。

3.3 操作指南

在进行设备管理前首先需要设置分组。

3.3.1 分组管理

一、人员分组：

包括的主要内容是：部门的添加，人员添加、删除、修改，如图 3-8 所示：

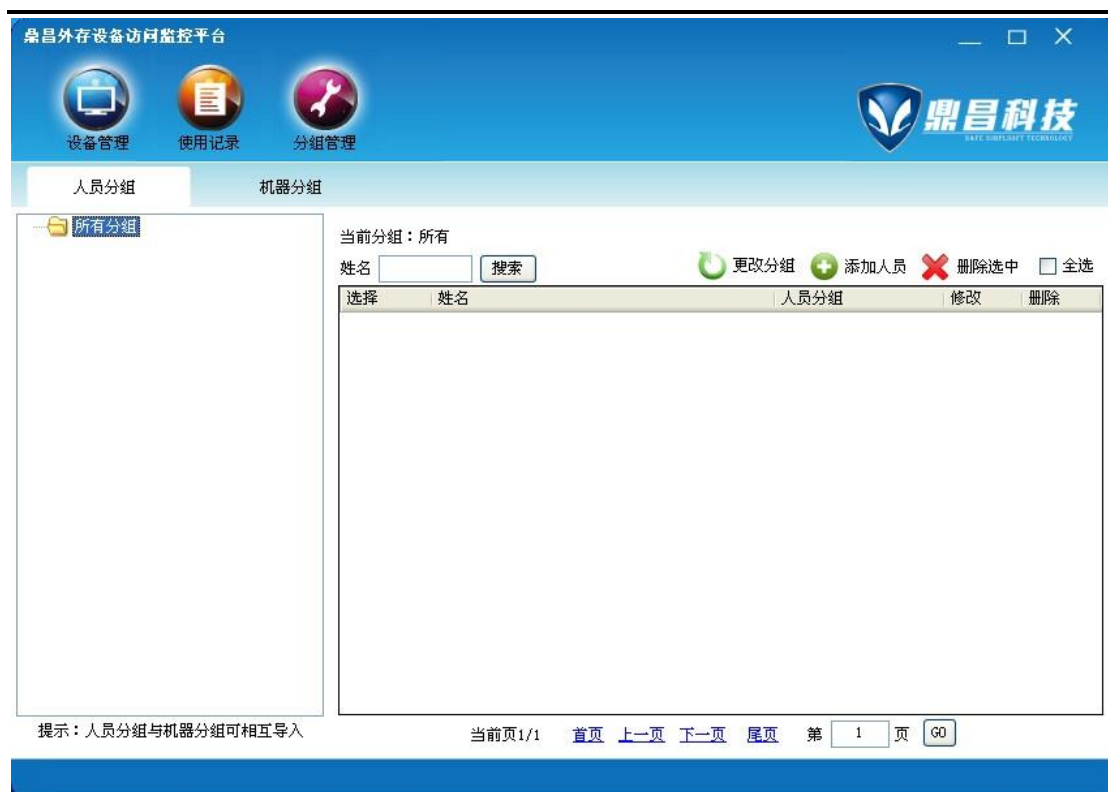


图 3-8 人员分组界面

1、添加分组

右击所有分组，可以添加分组，或从机器分组导入。添加新的分组时，在分组名输入框中输入组名，如图 3-9 所示：



图 3-9 添加分组

单击确定，提示新分组添加成功，如图 3-10 所示：

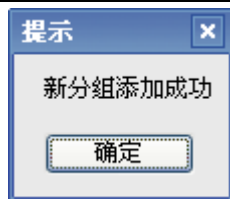


图 3-10 添加成功提示

同时，可以右击选择需要修改或删除的分组，单击右键选择“删除分组”，可以实现对分组的删除，同样选择“修改分组”时实现对分组名称的修改，如图 3-11 所示：

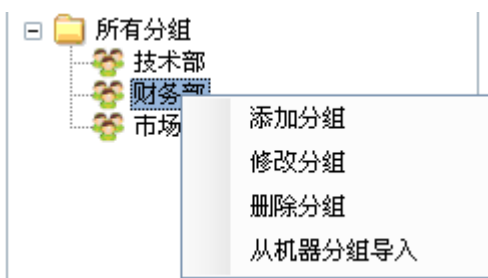
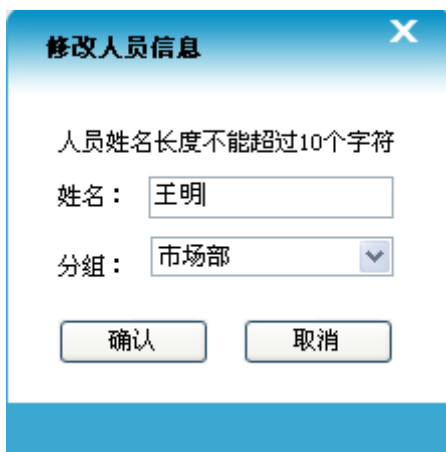


图 3-11 管理分组界面

2、添加人员

单击添加人员，出现修改人员信息界面，添加人员姓名，选择分组，如图 3-12 所示：



3-12 添加人员信息

确认后，出现人员信息添加成功的提示，并添加成功，如图 3-13 所示：

当前分组：人力资源部

姓名

☐ 全选


选择	姓名	人员分组	修改	删除
<input type="checkbox"/>	王明	市场部		

当前页 1/1 [首页](#) [上一页](#) [下一页](#) [尾页](#) 第 页

图 3-13 添加成功

对人员进行更改分组操作有两种方法：

(1) 批量修改：选中需要修改分组的人员对应的复选框，然后点击更改分组，进行修改；

(2) 单个修改：点击需要修改分组的人员所在行中的  图标，进行单个修改，如图 3-14 所示：

更改分组

选择分组：


市场部


确认

取消

3-14 人员信息更改分组

对人员进行删除操作有两种方法：

(1) 批量删除：选中需要删除的人员信息对应的复选框，点击  删除选中 进行批量删除；

(2) 单个删除：单击删除人员所在行中的  图标，进行单个删除，如图 3-15 所示：



3-15 人员信息删除

二、机器分组

1、添加分组

如同人员分组的操作进行添加。(注：机器分组中的部门和人员分组的部门可以进行相互导入)

首先我们把人员分组中的部门导入到机器分组中，右击所有分组，选择从人员分组中导入，如图 3-16 所示：



图 3-16 选择人员分组导入

出现导入分组界面，选择要导入的部门，点击确认导入，如图 3-17 所示：



3-17 导入分组

导入分组后，如图 3-18 所示：

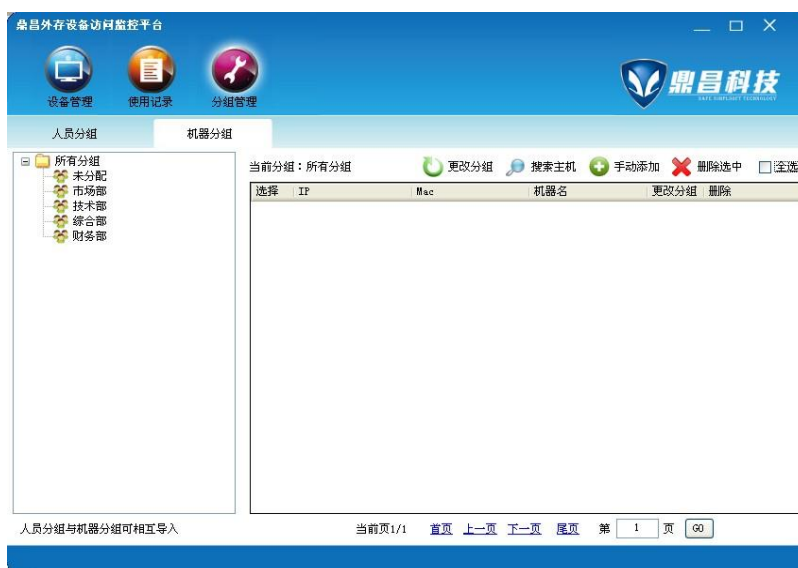


图 3-18 导入分组组主页面

2、添加主机

点击搜索主机，出现搜索主机界面，选择需要添加机器所属网络，设置相应的网卡。单击“开始搜索”，系统自动检测网络中的主机，如图 3-19 所示：



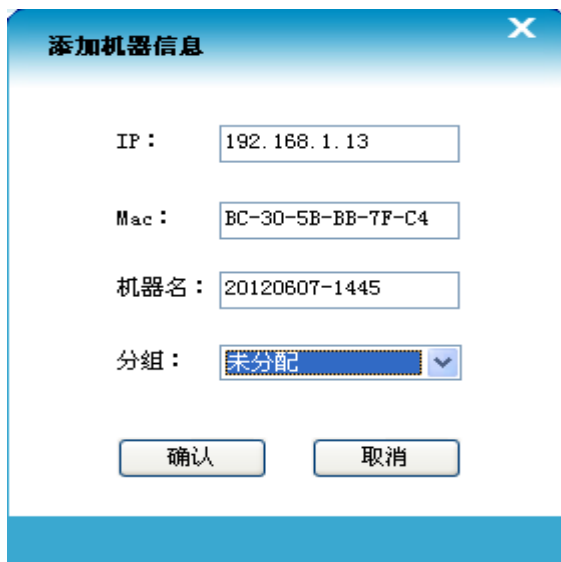
图 3-19 搜索主机

在所搜索的主机信息中选择需要添加的主机，在主机勾选框前打钩。也可以通过全选，批量选定，如图 3-20 所示：



图 3-20 添加主机

也可以手动添加，点击“手动添加”出现添加机器信息界面，如图 3-21 所示：



添加机器信息

IP: 192.168.1.13

Mac: BC-30-5B-BB-7F-C4

机器名: 20120607-1445

分组: 未分配

确认 取消

图 3-21 手工添加机器信息

在输入框输入需要添加的 IP，点击“确认”按钮，可出现搜索到的 mac 及机器名，选择分组，单击“确定”即可，提示机器添加成功，如图 3-22 所示：



图 3-22



机器添加到所有分组中，可以进行更改分组，如图 3-23、3-24 所示：



图 3-23 更改分组



图 3-24 更改分组

同时，也可以选择需要移除的机器名，点击  删除选中 进行删除，也可以单击 ，进行单个删除。

3.3.2 设备管理

1、设备登记

插入 USB 设备，点击刷新，系统自动显示 USB 设备信息，如盘符，容量，厂商代号，产品代号和序列号，如图 3-25 所示：



图 3-25 设备登记

(1) 内部使用权限

读写权限分为三种：禁用、只读、或读写。

选择“禁用”时，该 USB 设备在所选有效期、使用范围内无法使用。

选择“只读”时，该 USB 设备在所选有效期、使用范围内处于只读状态，无法对 USB 设备内容进行写入操作。

选择“读写”即允许该 USB 设备在所选有效期、使用范围内使用。

(2) 外部使用权限

允许 U 盘在外部使用时，需要设置普通区和安全区大小，并可选择有无监控操作记录，如图 3-26 所示：



图 3-26 外部使用权限

2、设备授权

管理员通过平台可以将 USB 设备制作为安全 U 盘，插入 U 盘，在设备登记中进行设置。

(1) 设备基本信息

插入 U 盘，点击“刷新”按钮，如图 3-27 所示：



图 3-27 设备基本信息读取

(2) 内部使用权限

可以设置内部使用权限为禁用、只读、读写，选择设备持有者的部门及姓名，设置有效期限和内部使用范围，如图 3-28 所示：



图 3-28 内部使用范围

(3) 外部使用权限

A、设备在外部可以使用，划分安全区，有外部使用操作记录监控，如图 3-29 所示：

☒ 外部使用权限

☒ 划分安全区

☒ 监控操作记录

普通区12.91%

493 MB

安全区87.07% (3326MB)

3820MB

- 可以在外部使用
- 外存设备划分为普通区和安全区
- 监控外存设备在外部使用的操作记录

图 3-29 外部划分安全区及操作记录

B、设备在外部可以使用，划分安全区，无外部使用操作记录监控，如

图 3-30 所示：

☒ 外部使用权限

☒ 划分安全区

☐ 监控操作记录

普通区12.91%

493 MB

安全区87.07% (3326MB)

3820MB

- 可以在外部使用
- 外存设备划分为普通区和安全区
- 不监控外存设备在外部使用的操作记录

图 3-30 外部使用无操作记录

C、设备在外部可以使用，全部划分为普通区，无外部使用操作记录监

控，如图 3-31 所示：

☒ 外部使用权限

☐ 划分安全区

☐ 监控操作记录

- 可以在外部使用
- 外存设备全部划分为普通区
- 不监控外存设备在外部使用的操作记录

图 3-31 外部设置普通区

D、设备外部不可以使用，如图 3-32 所示：

☐ 外部使用权限

☐ 划分安全区

☐ 监控操作记录

- 不可以使用

图 3-32 外部禁用权限

设置完成，点击“授权”按钮，如图 3-33 所示：



图 3-33 授权成功

U 盘授权成功后，用户打开 U 盘会显示，可执行程序 SafeDisk.exe 单击可执行程序 SafeDisk.exe，输入密码方可使用保护区域（安全 U 盘的具体使用见第四章），如图 3-34 所示：

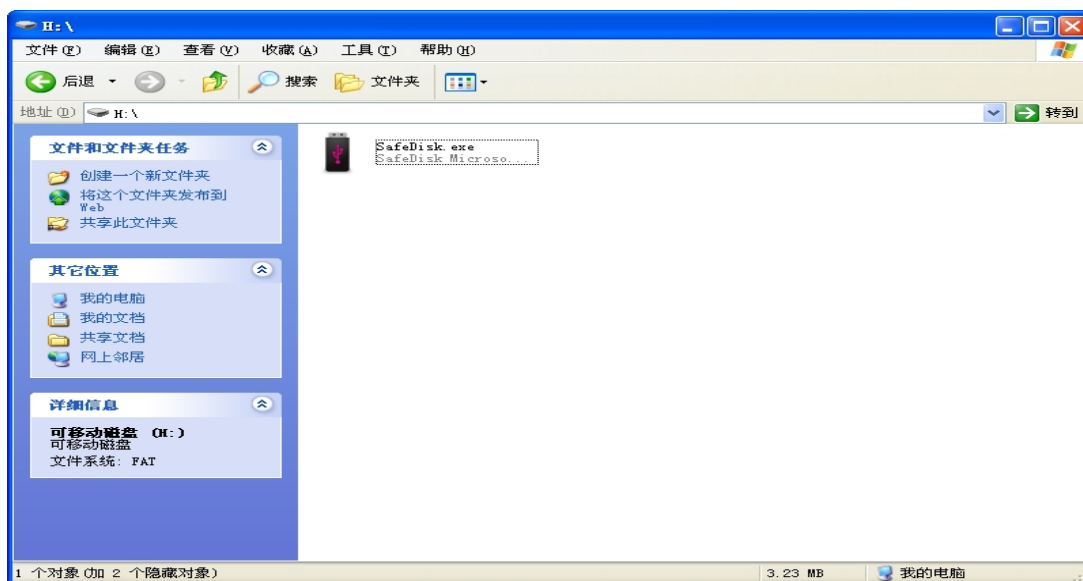


图 3-34 安全 U 盘

【注意】

授权安全 U 盘前需要先将 U 盘数据备份，一旦备份，U 盘会被格式化并分出普通区和保护分区两部分。

“重置”按钮，则恢复设置的所有内容。

3、已登记设备信息

单击打开已登记设备信息界面，如图 3-35 所示：



图 3-35 已登记设备信息主界面

(1)勾选显示当前插入的 U 盘，即可查看当前插入的 U 盘信息，如图 3-36 所示：



图 3-36 当前插入的 U 盘信息

(2) 根据人员分组、持有者进行查看设备信息，如图 3-37 所示：



图 3-37 根据分组查看

(3) 点击右下角的导出报表, 可以导出设备信息的所有记录内容, 如图 3-38

所示:

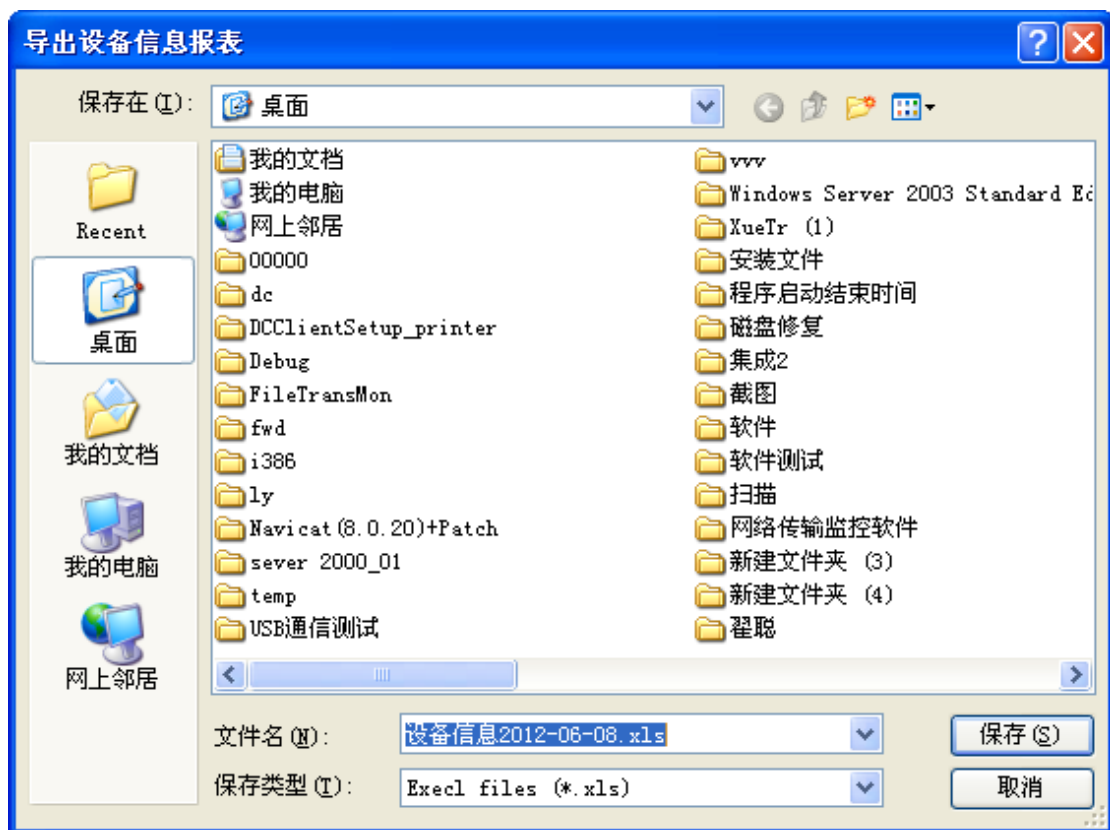


图 3-38 导出报表

点击“保存”按钮, 提示报表导出成功, 如图 3-39 所示:

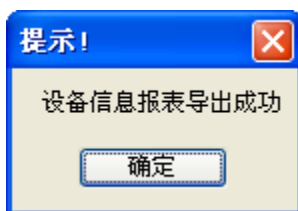


图 3-39 报表导出成功

桌面上出现设备信息 EXCEL 表, 如图 3-40 所示:



图 3-40 导出 EXCEL 表

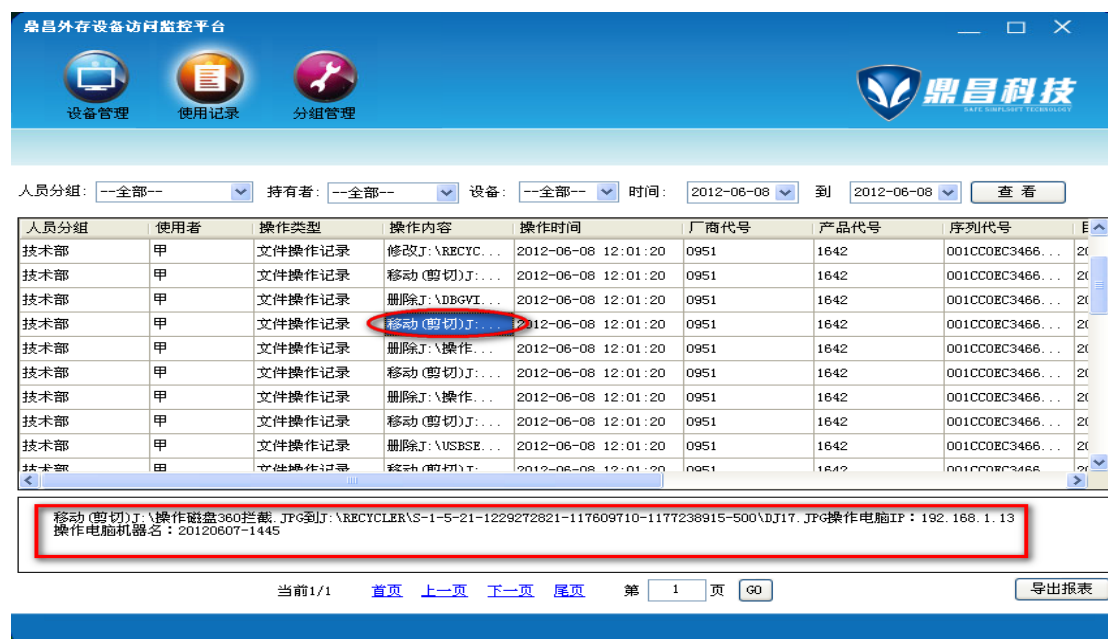
3.3.3 使用记录

管理员通过平台可以查看操作记录，选择人员分组、持有者及设备、选择查看时间进行查看，操作记录即显示，如图 3-41 所示：



人员分组	持有者	操作类型	操作内容	操作时间	厂商代号	产品代号	序列代号
市场部	乙	拔出	拔出U盘	2012-06-08 14:20:55	0951	1642	001CC0EC3466...
市场部	乙	插入	插入U盘	2012-06-08 14:17:55	0951	1642	001CC0EC3466...
市场部	乙	拔出	拔出U盘	2012-06-08 14:16:24	0951	1642	001CC0EC3466...
技术部	甲	插入	插入U盘	2012-06-08 12:59:13	0951	1642	001CC0EC3466...
技术部	甲	拔出	拔出U盘	2012-06-08 12:02:07	0951	1642	001CC0EC3466...
技术部	甲	插入	插入U盘	2012-06-08 12:01:59	0951	1642	001CC0EC3466...
技术部	甲	拔出	拔出U盘	2012-06-08 12:01:43	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	修改J:\RECYC...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...

图 3-41 插拔记录



人员分组	使用者	操作类型	操作内容	操作时间	厂商代号	产品代号	序列代号
技术部	甲	文件操作记录	修改J:\RECYC...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	删除J:\DBGVI...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	删除J:\操作...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	删除J:\操作...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	删除J:\USBSE...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...

移动(剪切)J:\操作磁盘360拦截.JPG到J:\RECYCLER\S-1-5-21-1229272621-117609710-1177238915-500\DJ17.JPG操作电脑IP: 192.168.1.13
操作电脑机器名: 20120607-1445

图 3-42 文件操作记录

使用记录查看：

(1) 选择人员分组的部门，选择时间段，点击查看，就可以看到所选部门

在这个期限内所有外存持有者的操作记录，如图 3-43 所示：



人员分组	持有者	操作类型	操作内容	操作时间	厂商代号	产品代号	序列代号
市场部	乙	拔出	拔出U盘	2012-06-08 14:47:16	0951	1642	001CC0EC3466...
市场部	乙	插入	插入U盘	2012-06-08 14:31:50	0951	1642	001CC0EC3466...
市场部	乙	拔出	拔出U盘	2012-06-08 14:20:55	0951	1642	001CC0EC3466...
市场部	乙	插入	插入U盘	2012-06-08 14:17:55	0951	1642	001CC0EC3466...
市场部	乙	拔出	拔出U盘	2012-06-08 14:16:24	0951	1642	001CC0EC3466...

图 3-43 人员分组记录

(2) 选择持有者的姓名就可以查看持有者所在部门以及所在机器上操作哪

些内容，如图 3-44 所示：



人员分组	持有者	操作类型	操作内容	操作时间	厂商代号	产品代号	序列代号
技术部	甲	插入	插入U盘	2012-06-08 12:59:13	0951	1642	001CC0EC3466...
技术部	甲	拔出	拔出U盘	2012-06-08 12:02:07	0951	1642	001CC0EC3466...
技术部	甲	插入	插入U盘	2012-06-08 12:01:59	0951	1642	001CC0EC3466...
技术部	甲	拔出	拔出U盘	2012-06-08 12:01:43	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	修改J:\RECYC...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	删除J:\DBGVI...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	移动(剪切)J:...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...
技术部	甲	文件操作记录	删除J:\操作...	2012-06-08 12:01:20	0951	1642	001CC0EC3466...

图 3-44 持有者记录操作

(3) 选择持有者的设备，可以查看该设备在所有机器上进行的操作记录，如图 3-45 所示：

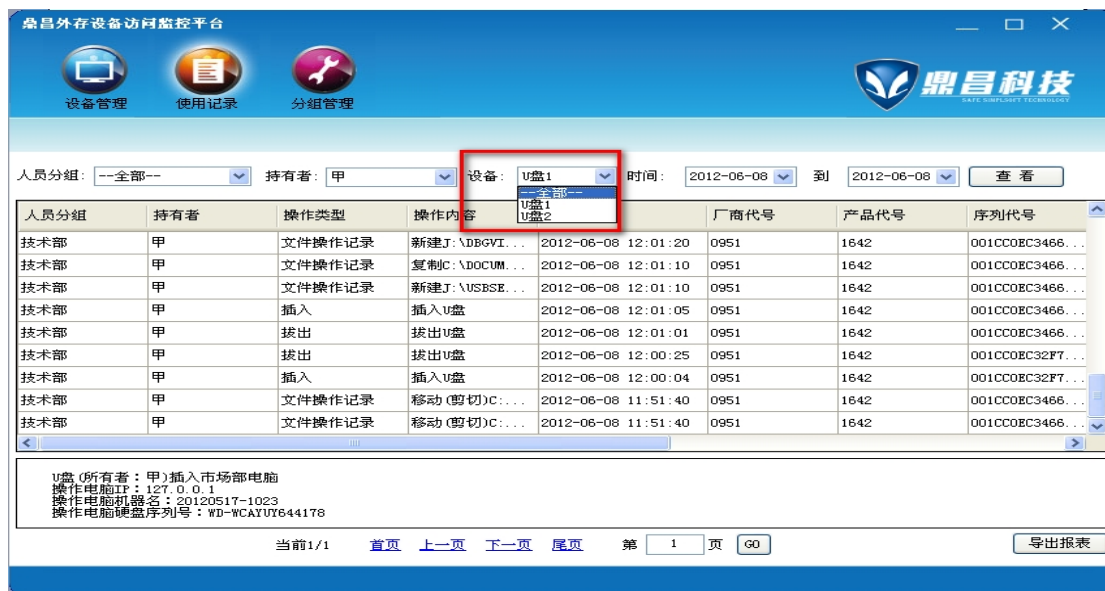


图 3-45 设备操作记录

4. 如果想查看清楚插拔设备的性质、所在部门的哪台机器、操作的类型、操作的内容及具体时间的操作情况，可以点击生成报表，如图 3-46 所示：

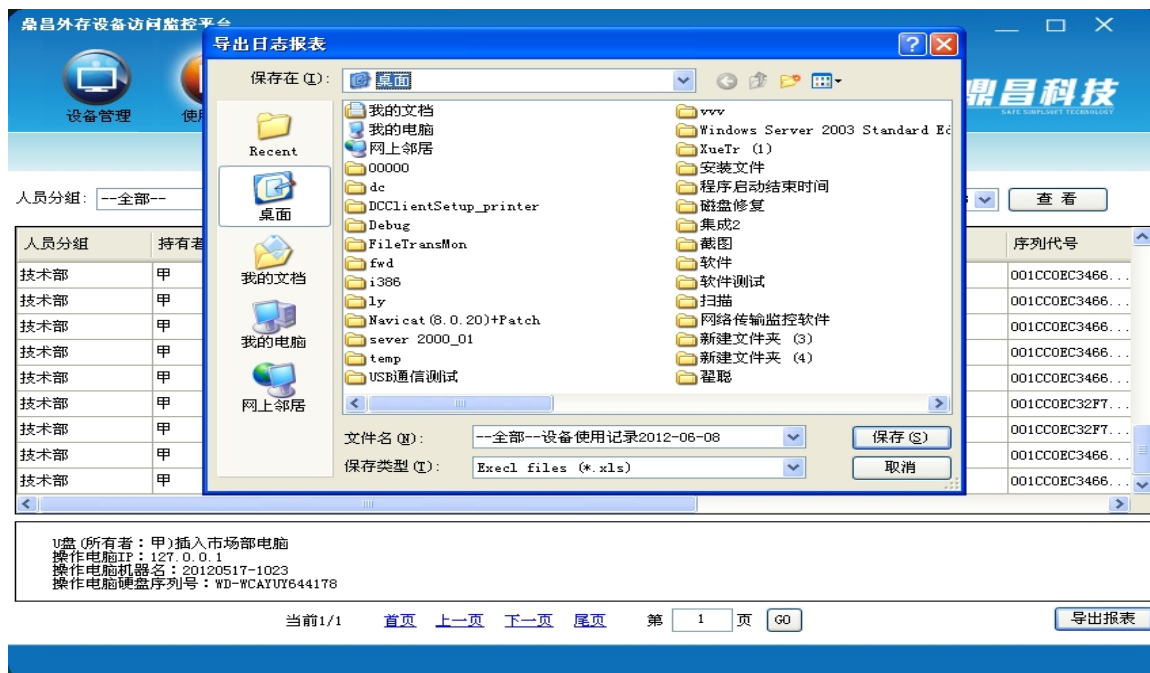


图 3-46 导出报表

点击“保存”按钮，提示设备使用记录保存成功，如图 3-47 所示：

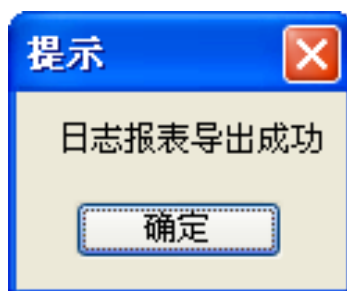
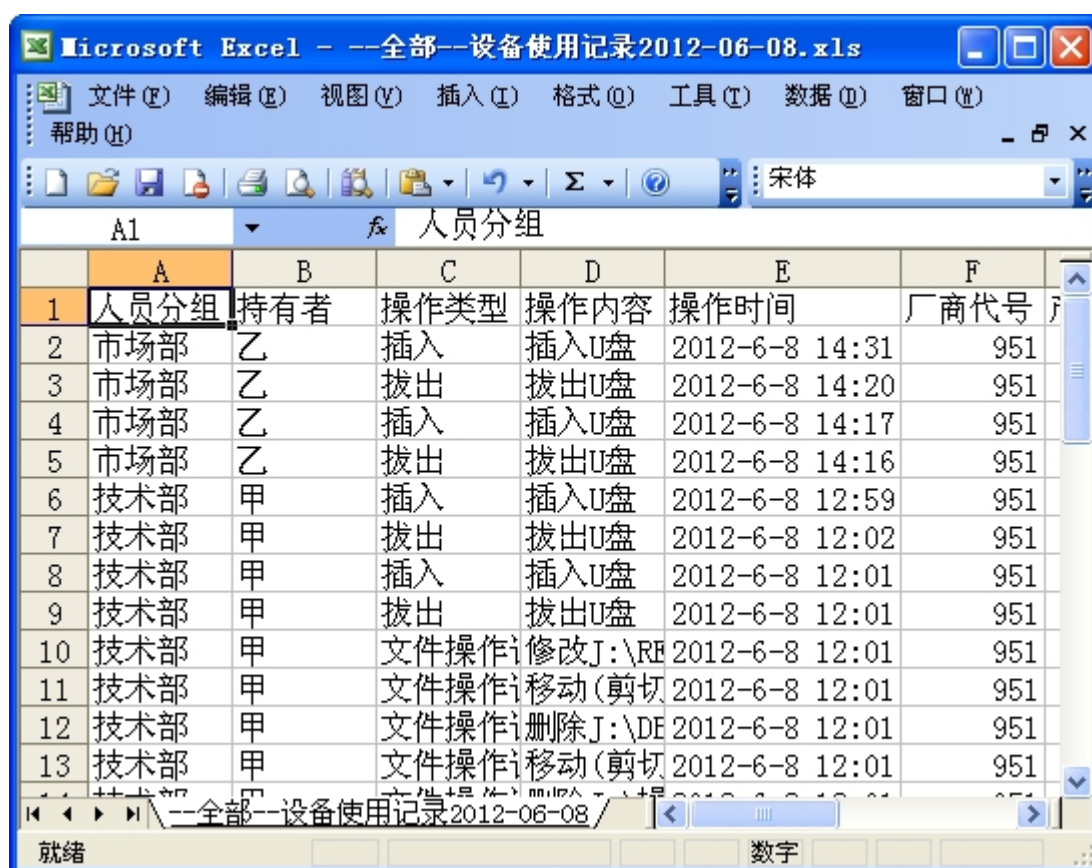


图 3-47 报表导出提示

生成 EXCEL 表，打开报表，如图 3-48 所示：



Microsoft Excel - --全部--设备使用记录2012-06-08.xls

文件(F) 编辑(E) 视图(V) 插入(I) 格式(O) 工具(T) 数据(D) 窗口(W) 帮助(H)

宋体

	A	B	C	D	E	F
1	人员分组	所有者	操作类型	操作内容	操作时间	厂商代号
2	市场部	乙	插入	插入U盘	2012-6-8 14:31	951
3	市场部	乙	拔出	拔出U盘	2012-6-8 14:20	951
4	市场部	乙	插入	插入U盘	2012-6-8 14:17	951
5	市场部	乙	拔出	拔出U盘	2012-6-8 14:16	951
6	技术部	甲	插入	插入U盘	2012-6-8 12:59	951
7	技术部	甲	拔出	拔出U盘	2012-6-8 12:02	951
8	技术部	甲	插入	插入U盘	2012-6-8 12:01	951
9	技术部	甲	拔出	拔出U盘	2012-6-8 12:01	951
10	技术部	甲	文件操作	修改J:\RE	2012-6-8 12:01	951
11	技术部	甲	文件操作	移动(剪切	2012-6-8 12:01	951
12	技术部	甲	文件操作	删除J:\DE	2012-6-8 12:01	951
13	技术部	甲	文件操作	移动(剪切	2012-6-8 12:01	951

就绪 数字

图 3-48 导出报表内容

第四章 用户使用指南

制作好安全 U 盘以后，该 U 盘就会被划分成一个普通区和一个安全分区。其中普通区，可以直接访问。安全分区需要验证登陆保护区口令成功后方可访问。

具体使用步骤如下：

1、打开安全盘的普通分区后会发现该分区中有一个可执行文件 SafeDisk.exe，也可以双击桌面上的“SafeDisk.exe”快捷图标，如图 4-1 所示：

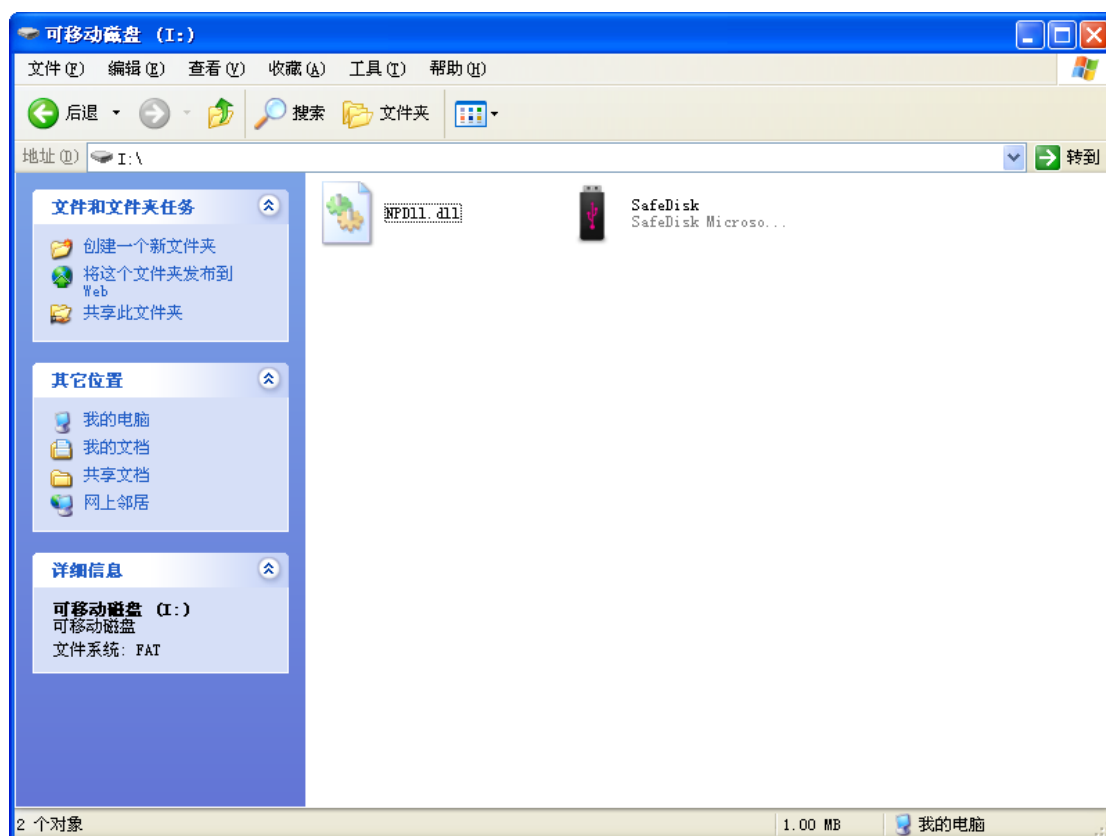


图 4-1 安全 U 盘使用

2、运行该文件，会弹出保护区登陆窗口，如图 4-2 所示：

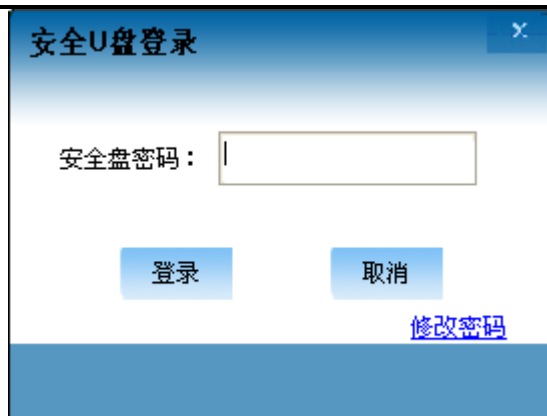


图 4-2 安全 U 盘保护部分登录界面

3、安全 U 盘首次使用时，我们要进行保护分区登陆口令修改。单击“修改密码”后弹出修改密码对话框，输入默认密码“123456”，新密码，输入确认密码后，单击确定完成修改，如图 4-3 所示：

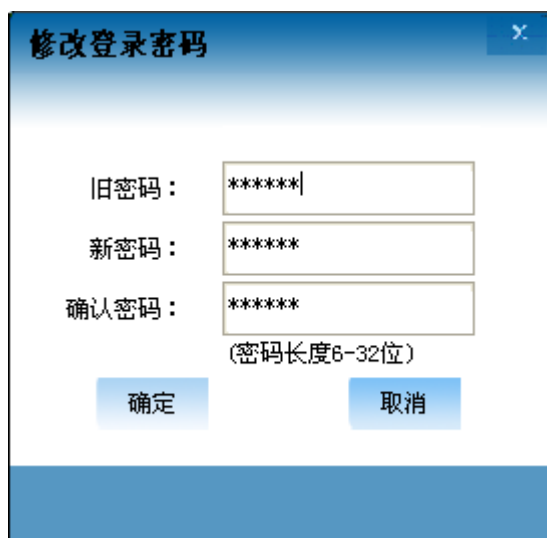


图 4-3 登录密码修改

建议口令长度不小于 6 位,而且最好由数字和字母组成。

4、当成功修改口令后，就可以用修改后的口令登陆保护分区了，如图 4-4 所示：

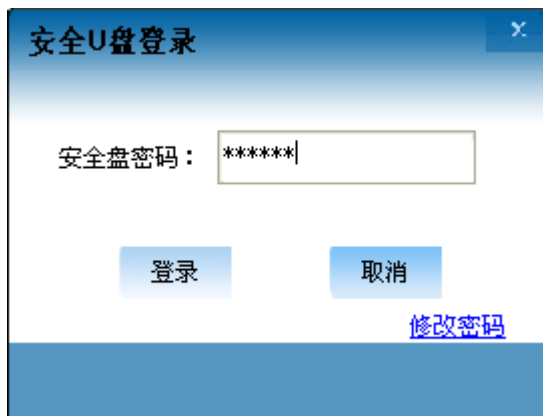


图 4-4 安全 U 盘保护区域登录

登陆成功后，程序自动打开安全盘界面，如图 4-4 所示：

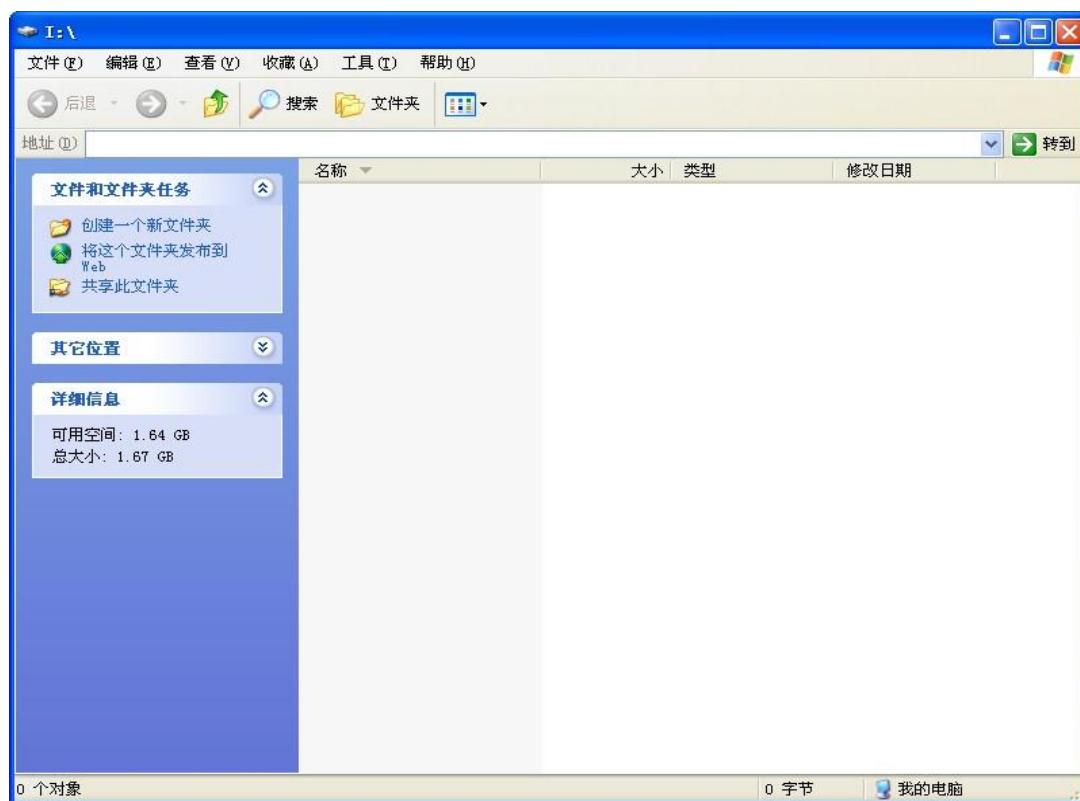


图 4-5 安全 U 盘保护区域

同时，“我的电脑”里出现一个新盘符“安全 U 盘”，如图 4-6 所示：



图 4-6 安全 U 盘

此时，安全 U 盘就可以使用了。

4.1 内部安全 U 盘的使用

(1) 禁用

如果 USB 设备登记时设定在选定部门分组中禁用，用户想要打开登记的 USB 设备时，如图 4-7 所示：



图 4-7 拒绝访问

(2) 只读

如果 USB 设备登记时设定置在选定部门只读,用户打开登记的 USB 设备进行编辑或删除操作,会出现提示信息,无法进行复制,移动 删除等操作,进入安全盘进行操作,则操作的内容拔出 U 盘后,再次插入,没有任何内容,如图 4-8 所示:



图 4-8 只读权限操作

(3) 读写

如果 USB 设备登记时设定在选定部门读写访问,用户可以对登记设备正常操作,不受任何限制,如图 4-9 所示:

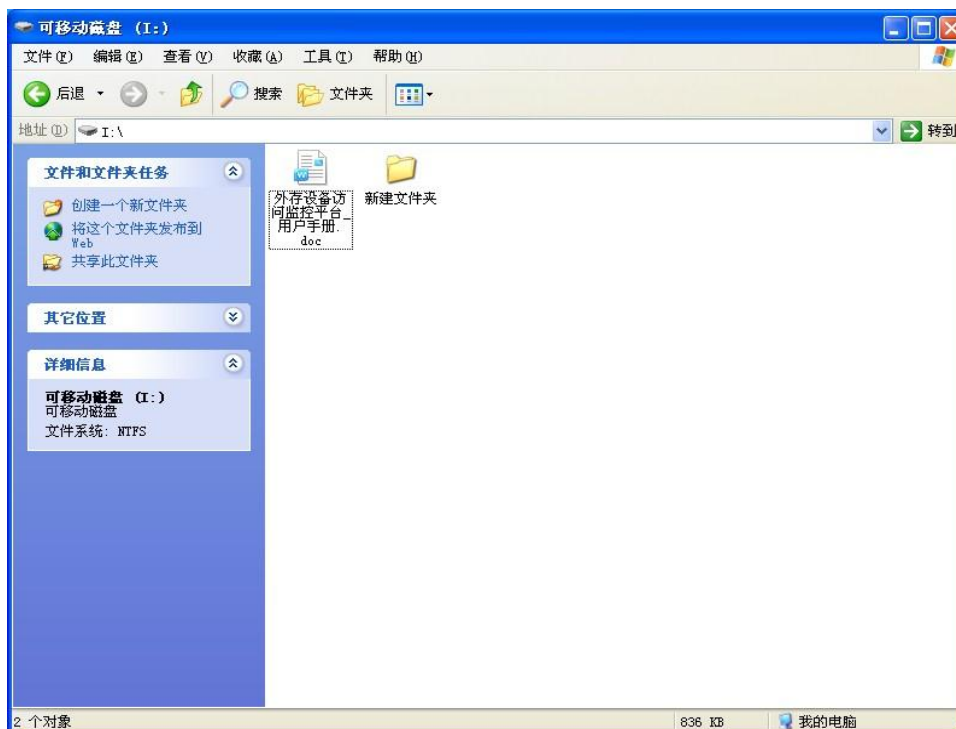


图 4-9 读写权限操作

4.2 外部安全 U 盘的使用

1、设备在外部可以使用，划分安全区，有外部使用操作记录监控。

可以进行复制、编辑、删除等操作，如图 4-10 所示：

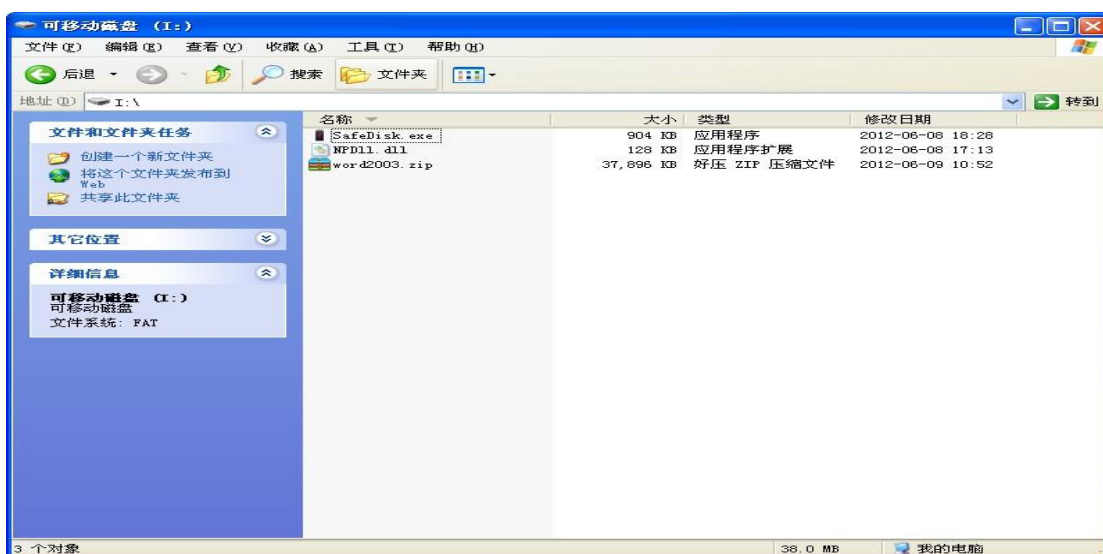


图 4-10 外部 U 盘使用

双击 safedisk.exe，打开安全 U 盘 J 盘，如图 4-11 所示：

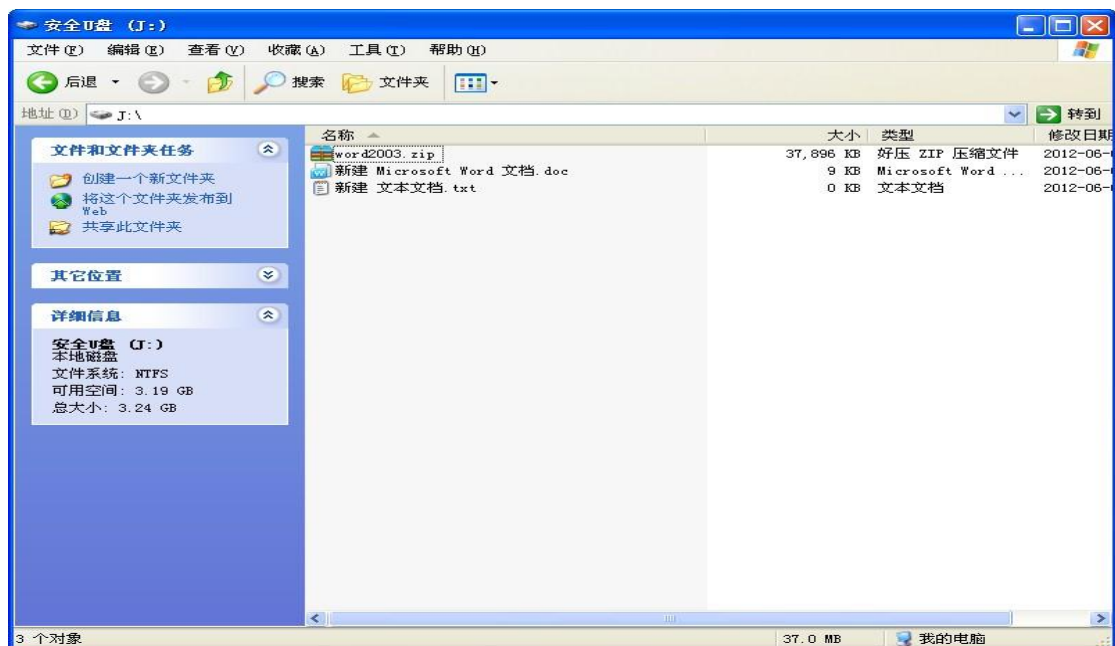


图 4-11 安全 U 盘使用

操作完成之后，拔出 U 盘,在服务端的使用记录中进行查看，如图 4-12 所示：

人员分组：	--全部--	持有者：	--全部--	设备：	--全部--	时间：	2012-06-09	到	2012-06-09	查看
人员分组	持有者	操作类型	操作内容	操作时间	厂商代号	产品代号	序列代号			
综合部	丙	插入	插入U盘	2012-06-09 15:13:12	0951	1624	001CC0EC34BE...	20		
市场部	甲	文件操作记录	修改J:554.TXT	2012-06-09 15:12:40	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	打开J:554.TXT	2012-06-09 15:12:30	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	修改J:RECYCL...	2012-06-09 15:12:30	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	移动(剪切)J:...	2012-06-09 15:12:30	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	删除J:EQUIPM...	2012-06-09 15:12:30	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	修改J:RECYCL...	2012-06-09 15:12:20	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	修改J:RECYCL...	2012-06-09 15:12:20	0951	1642	001CC0EC34BE...	DC		
市场部	甲	文件操作记录	移动(剪切)E:...	2012-06-09 15:12:10	0951	1642	001CC0EC34BE...	DC		
市场部	田	文件操作记录	新建T:网络...	2012-06-09 15:12:10	0951	1642	001CC0EC34BE...	DC		

打开J:554.TXT操作电脑IP: 192.168.1.15
 操作电脑机器名: DC-GQ

当前第1页/共2页 共96条记录 [首页](#) [上一页](#) [下一页](#) [尾页](#) 第 1 页 [GO](#) [导出报表](#)

图 4-12 文件操作记录

如果想查看所有详细记录，可以点击“导出报表”进行查看。

2、设备在外部可以使用，划分安全区，无外部使用操作记录监控

此操作步骤同上。

3、设备在外部可以使用，全部划分为普通区，无外部使用操作记录监控

可以在外部使用，外存设备全部划分为普通区，不监控操作记录，如图 4-13 所示：

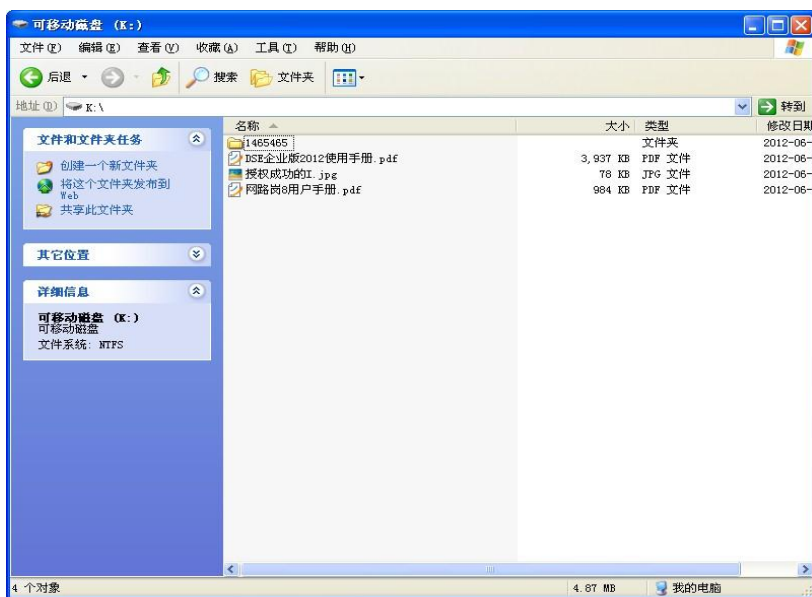


图 4-13 外部为普通区使用

4、设备外部不可以使用

打开 U 盘复制文件到 U 盘时，如图 4-14 所示：

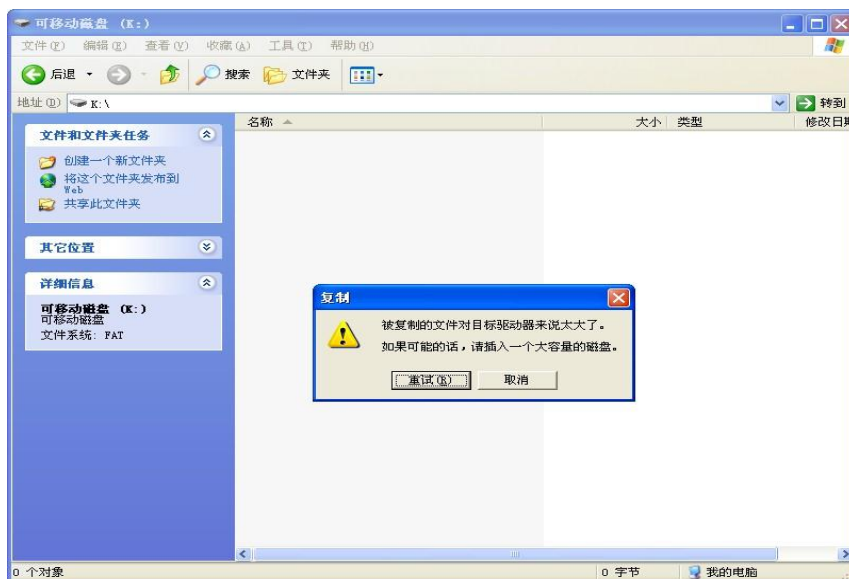


图 4-14 外部禁止使用

查看 U 盘属性，如图 4-15 所示：

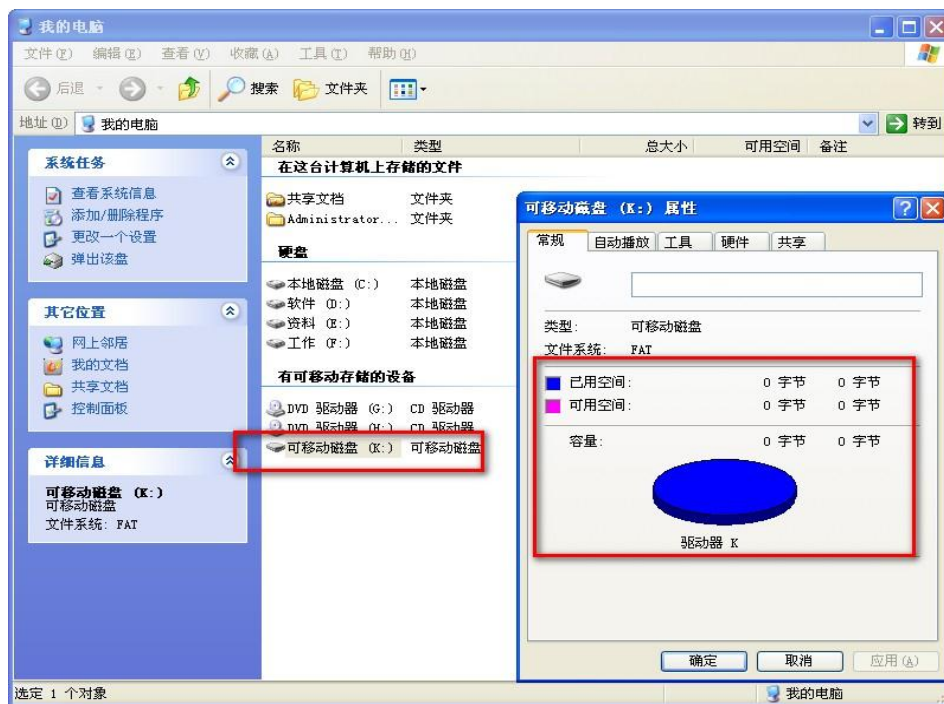


图 4-15 查看 U 盘属性

第五章 联系我们

郑州鼎昌计算机科技有限公司是专门从事计算机、软、硬件研发的高新技术企业，致力于数据信息安全的探索和实践，在计算机数据使用、监控、追踪以及网络通讯安全等方面积累了丰富的技术经验，业务涵盖政府、事业、企业、军工、科研、个人等不同层次的应用领域。

鼎昌科技以创新、稳健为基石，以专业、实用为目的，以简单、易用为原则，以务实、积极为理念，愿携手全国同行同业为发展我国信息安全事业而做出不懈努力！

客服电话：0371-69105833 400-00-13851

传 真：0371-63790716

电子邮箱：dingchangkj@126.com