
铁卷电子文档安全系统

TotalFileGuard™

管理员指南

V3.2

深圳市大成天下信息技术有限公司

SHENZHEN UNN00 Information Tech co., Ltd.

声明：本文档是深圳市大成天下信息技术有限公司(简称大成天下)解决方案的一部分，版权归大成天下所有，任何对文档的修改、发布、传播等行为都需获得大成天下书面授权，大成天下保留对违反以上声明的组织或个人追究责任，直至诉诸法律的权力。

二〇一〇年八月

目录

管理员指南 V3.2	1
目录	2
1. 管理中心	4
1.1. 简介	4
1.2. 登录、注销管理中心和修改密码	4
2. 策略管理	6
2.1. 基本策略	6
2.2. 安全策略	7
2.2.1. 受保护进程	7
2.2.2. 加密设置	8
2.2.3. 终端类型	10
2.2.4. 打印和截屏保护	13
2.2.5. 终端日志	15
2.2.6. 其他设置	16
2.2.7. 终端组件选择	20
2.2.8. 外发控制模块（TSP）	21
2.2.9. 文件备份模块	22
2.2.10. TFGProxy 模块	23
2.3. 策略模板	24
2.3.1. 模板的创建	25
2.3.2. 模板的应用	26
3. 客户端管理	27
3.1. 终端状态	27
3.2. 认证管理	27
3.2.1. 接入模式	27
3.2.2. Usb-key 模式	29
3.2.3. 软证书模式	30
3.3. 查看/修改策略	32
3.4. 组织管理	33
3.4.1. 组织结构图的建立	34
3.4.2. 终端重命名	35
3.4.3. 添加到组织	35
3.4.4. 从组织中移除	36
3.4.5. 审批模式	36
3.5. 命令管理	37
3.5.1. 发送消息	37
3.5.2. 远程执行	38
3.5.3. 远程升级/远程卸载终端程序	38
3.5.4. 查看/删除离线命令	38
3.6. 终端的搜索	39
4. 日志审计	40

4.1.	实时日志.....	40
4.2.	日志管理.....	41
4.2.1.	日志备份.....	41
4.2.2.	日志查询.....	43
4.3.	审计报告.....	48
5.	系统管理.....	49
5.1.	监控服务器状态.....	49
5.2.	许可管理.....	51
5.3.	申请管理.....	51
5.4.	密钥管理.....	52
5.4.1.	密钥的备份.....	52
5.4.2.	密钥的恢复.....	53
5.5.	管理组.....	54
5.6.	服务管理.....	55

1. 管理中心

1.1. 简介

大成天下的铁卷电子文档安全系统是一个综合的数据防泄密解决方案，用于帮助组织保护敏感信息不被意外外泄和主动泄密。该系统包含两个主要的子系统，防泄密客户端和管理服务器。铁卷管理服务器包含三个主要的子系统：管理中心、身份认证系统和带有 MySQL 的数据库。

铁卷采用了 C/S 通讯方式，每台受控的计算机上都必须安装防泄密客户端（以下简称用户终端），所有的用户终端由管理中心进行集中控制和管理。

管理中心的功​​能包括：查看和管理用户终端、审批终端提交的离线申请和解密申请、保存和维护企业密钥、记录重要的终端操作日志、远程升级和卸载用户终端程序等。

1.2. 登录、注销管理中心和修改密码

从系统“开始”-“程序”-“铁卷电子文档安全系统”中选取“管理中心”。



1-1 管理员登录

输入帐号和密码即可进入管理中心（如下图），默认帐号为 **system**，默认密码为 **11111111**。

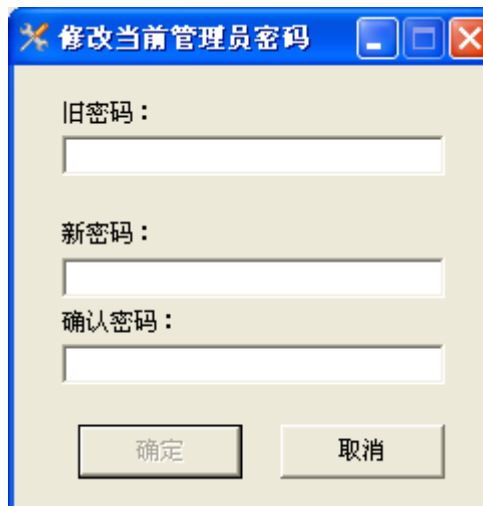


1-2 实时状态图

点击“管理中心”菜单中的“注销”退出管理中心的登录。

可以点击“工具”菜单中的“修改当前管理员密码”修改当前管理员密码，

也可以点击  实现。




1-3 修改当前管理员密码

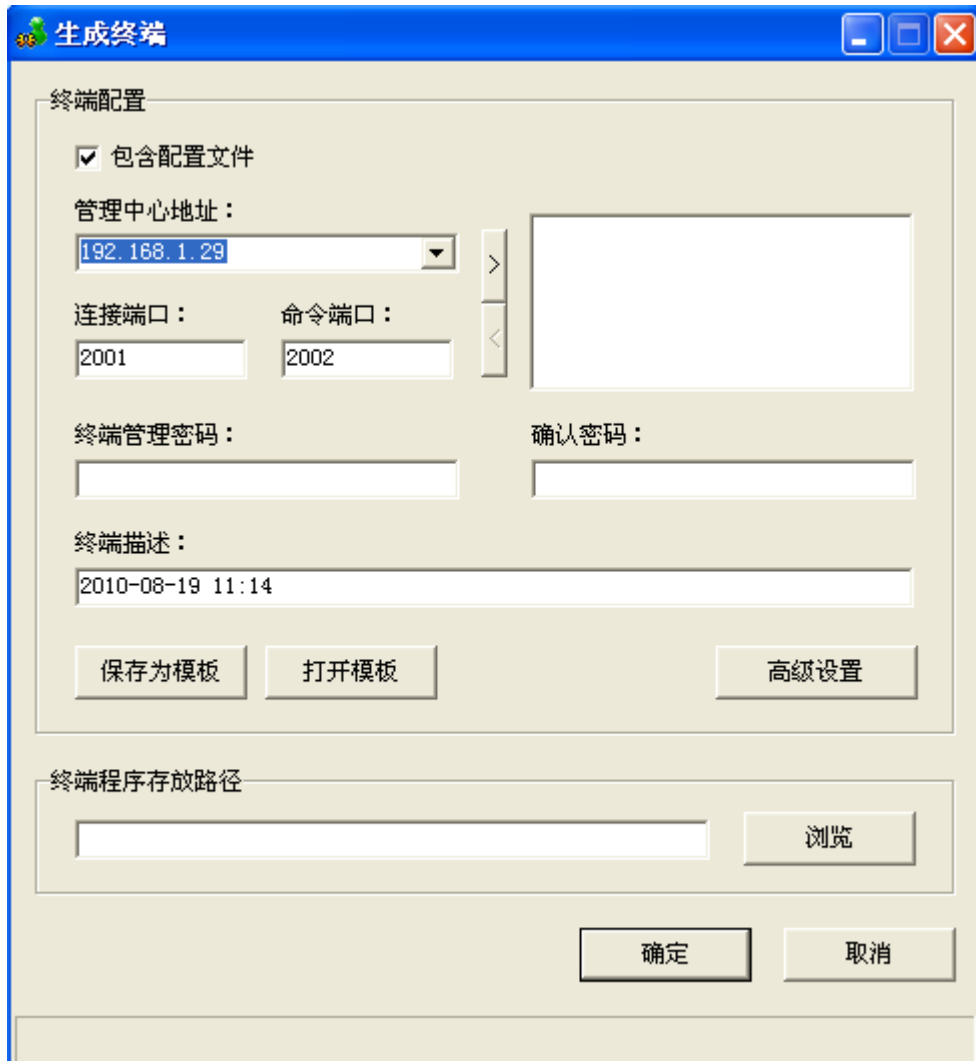
注意：密码最少 8 位。

2. 策略管理

铁卷策略管理的对象是用户终端，策略管理主要针对不同工作性质的用户群定制不同策略集的用户终端安装程序。

2.1. 基本策略

在管理中心选择“工具”->“生成终端”，或单击工具栏上的图标，可以调出如下界面：



生成终端

终端配置

包含配置文件

管理中心地址：
192.168.1.29

连接端口： 2001 命令端口： 2002

终端管理密码：

确认密码：

终端描述：
2010-08-19 11:14

保存为模板 打开模板 高级设置

终端程序存放路径
_____ 浏览

确定 取消

2-1 基本策略配置界面

管理中心地址：首先择正确的服务器对外 IP 地址，“连接端口”默认为 2001，“命令端口”默认为 2002。然后点击“>”将服务器 IP 地址和端口号加入右侧文本域中。

提示：可以设置多个 IP 地址和端口，用户终端默认选择第一位的 IP 地址为首选认证服务器。如果首选认证服务器不能提供认证服务，用户终端依先后顺序尝试连接认证服务器，直到认证通过；当下一次启动时，用户终端首先尝试连接首选认证服务器。

终端管理密码：在“输入密码”处填入的密码并填入确认密码（该密码用于终端管理，如：退出和卸载终端等。管理员必须牢记该密码）。

终端配置信息描述：默认为终端程序生成的时间，管理员可根据实际需要进行修改。

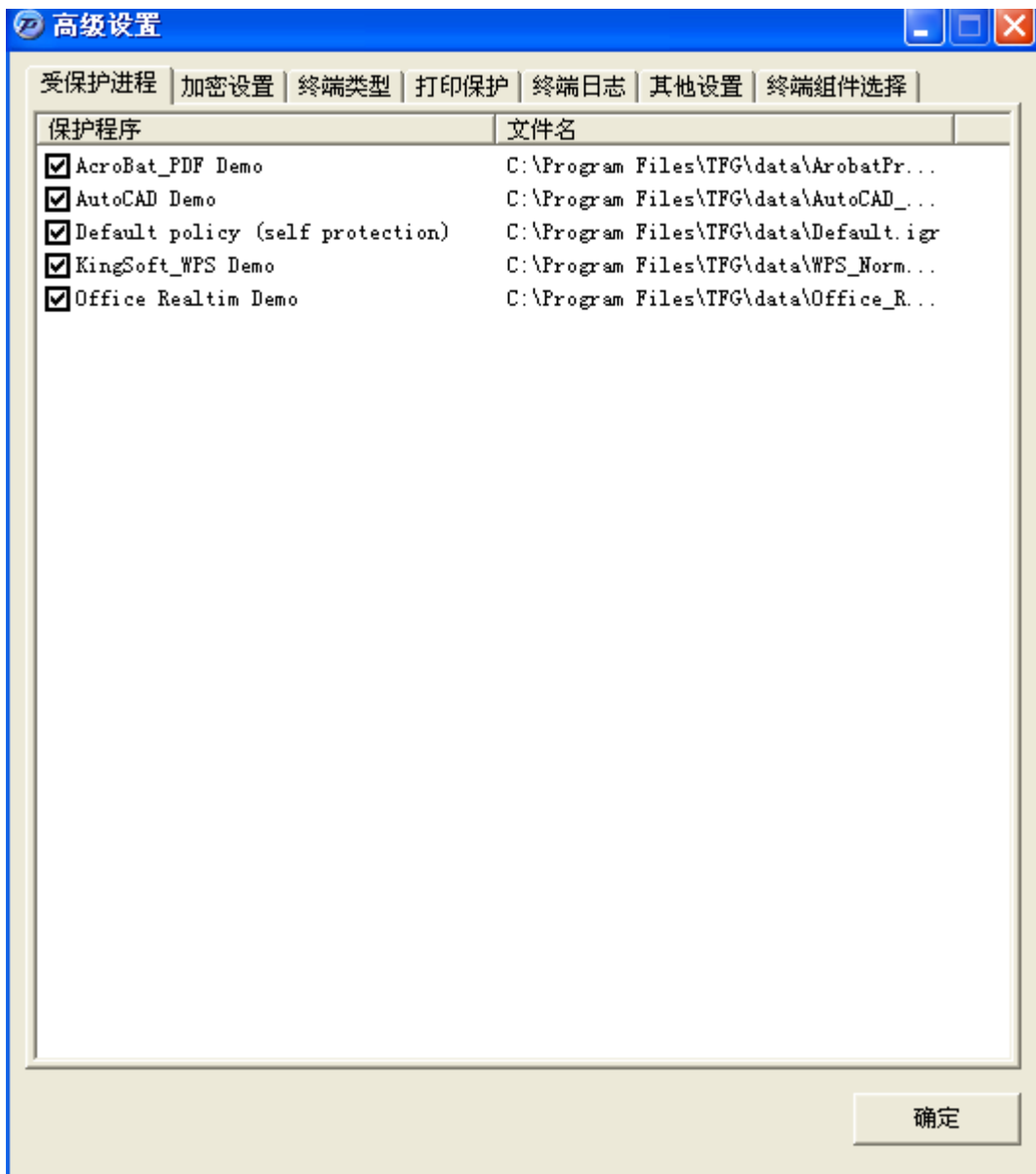
包含配置文件：当只更新用户终端程序而不更改安全策略时可取消此选项；例如当前的用户终端的版本为 3.2.12，而服务端版本为 3.2.14 时，可取消此选项进行用户终端版本的升级，不对用户终端的安全策略进行更改。

生成终端：在“终端程序存放路径”下面文本框中输入终端文件保存的位置和终端程序名；也可以点击文本框后的“浏览”，选择终端程序存放的位置。

2.2. 安全策略

2.2.1. 受保护进程

根据用户选购的软件支持版本（参考《铁卷软件支持列表》）不同，铁卷中提供的受保护进程规则也不同。用户可以在生成客户端的时候，按自己的需求来决定购买和使用软件支持版本。如果用户需要增加对某种类型的文档进行保护，可右键点击“导入”按钮导入相应的规则。



2-2 受保护进程

如果要取消对某个进程的保护，对相应规则不做勾选即可。

2.2.2. 加密设置

铁卷内置了 RC4、RC5 和 AES 三种加密算法供用户选择。默认为 128 位密钥的 RC4 加密算法。选择相同的加密算法和密钥长度，才不会影响各终端之间交换文档。

注意：密钥长度越大，则文件被破解的可能性越低，但加密解密的速度会更慢一些。一般情况下，由 128 位密钥加密的文件，已具备足够的抗攻击强度。用户可以根据实际情况灵活控制。



2-3 加密设置

全盘扫描时加密下列后缀名的文档: 该选项一般使用在终端初次部署时, 自动将计算机上的指定格式文件全部扫描后加密的功能。确保原有的文档不会以明文形式流传出去。

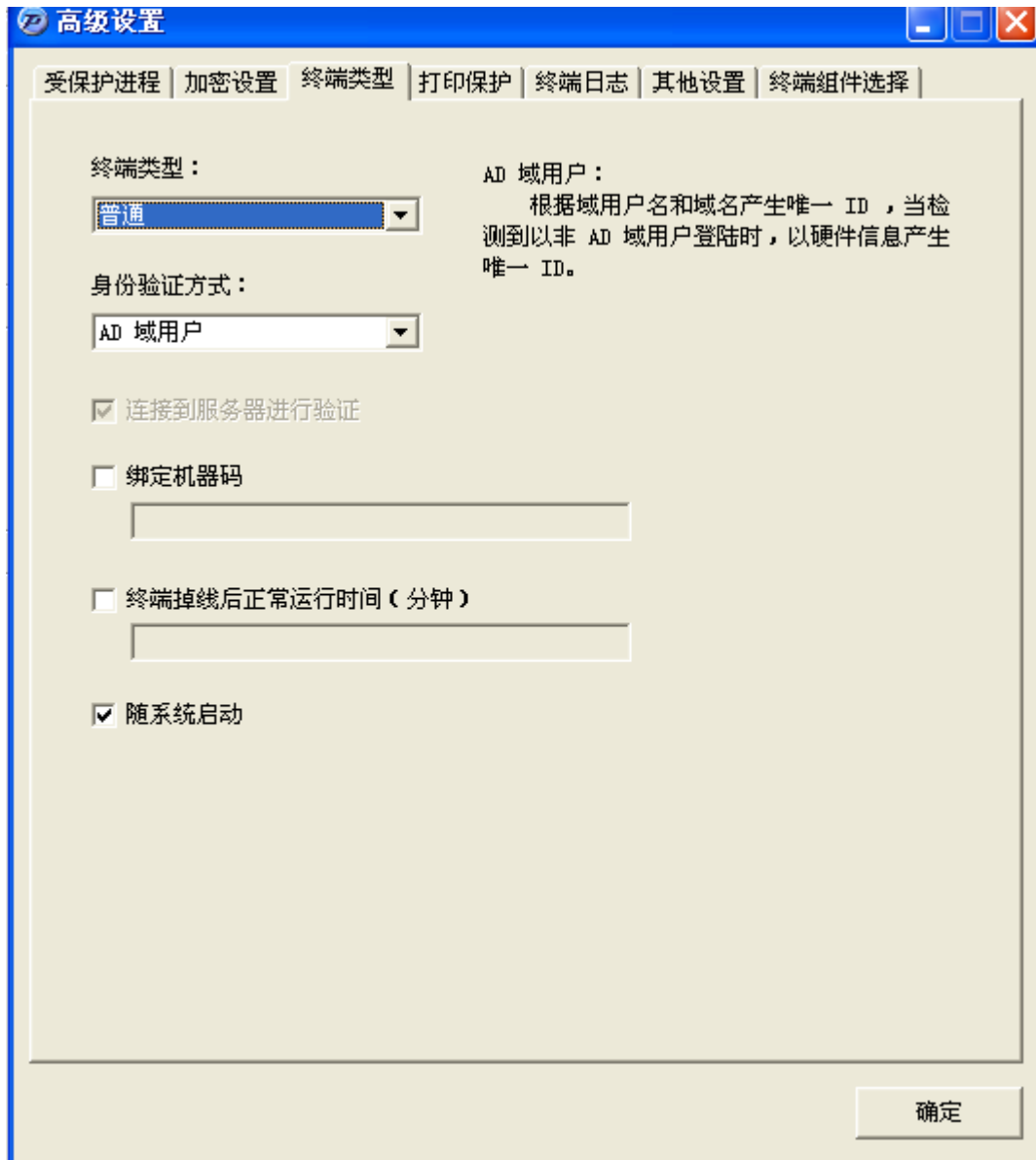
复制文件时加密下列后缀名文档: 勾选该选项, 则会在终端用户复制文件时强制将指定格式的目标文件加密。

强制加密的文件后缀名: 在下面的文本框中写文件后缀名, 如“doc”, 然后点击“>”加入列表框。

强制加密时忽略的目录: 指定目录内的文件不会在全盘扫描时被自动加密。设定方法同“强制加密的文件后缀名”。

注意：强制加密文件后缀名和强制加密时忽略的目录同时对应于全盘扫描加密和复制文件时加密

2.2.3. 终端类型



2-4 终端类型

终端类型：在该项设置中，终端类型有三个选项：“普通”、“只解密不加密”、“外部合作伙伴”。

各个选项的含义如下：

普通：适用于普通终端用户。文件打开时解密，保存、另存或新建时加密。

只解密不加密：适用于高层主管级用户。创建终端时选择该类型，则该终端不对新文档和明文文档强制加密，同时会保证已被加密的文档打开后为明文状态。

提示：需要受保护进程规则支持，例如 Word 文件必须要 Word 规则。

外部合作伙伴：

适用于企业以外的第三方合作伙伴。创建终端时选择该类型，则该终端可在用户需要透明解密文档时手动执行。在此期间可以查看和操作加密文件，新建文文件会被加密，对非加密文件保存后自动加密。无法解密加密文件，无法连接管理中心。处理完后可手动关闭终端。

身份验证方式有三个选项：

硬件信息：根据计算机硬件信息产生唯一 ID，当硬件改变后需要管理员重新允许接入。

USBKEY：由 USBKEY 内读取唯一 ID，与硬件信息无关。终端开始运行时必须插入 USBKEY 才能正常启动终端进程。当选择此项认证方式后，需要事先创建终端 KEY 供终端用户使用。

AD 域用户：根据域用户名和域名产生唯一 ID，并且依据域组自动建立组织结构图。当检测到以非 AD 域用户登录时，以硬件信息产生唯一 ID。

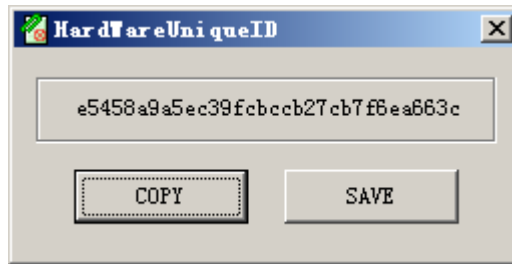
连接到服务器进行验证：当选中此项后，终端必须连接到服务器并通过验证才能认证生效。

绑定终端硬件 ID：选中此项，并在文本输入框中指定硬件 ID，则该终端程序只能在对应的主机上才能使用。如果不是在对应的主机上使用，则会出现如下的提示对话框。



2-5 硬件验证失败提示信息

提示：硬件 ID 可以使用本公司的软件自带的软件（位置为服务端安装目录\TFG\tools 下的 HardwareID.exe）获取。



2-6 获取终端硬件信息

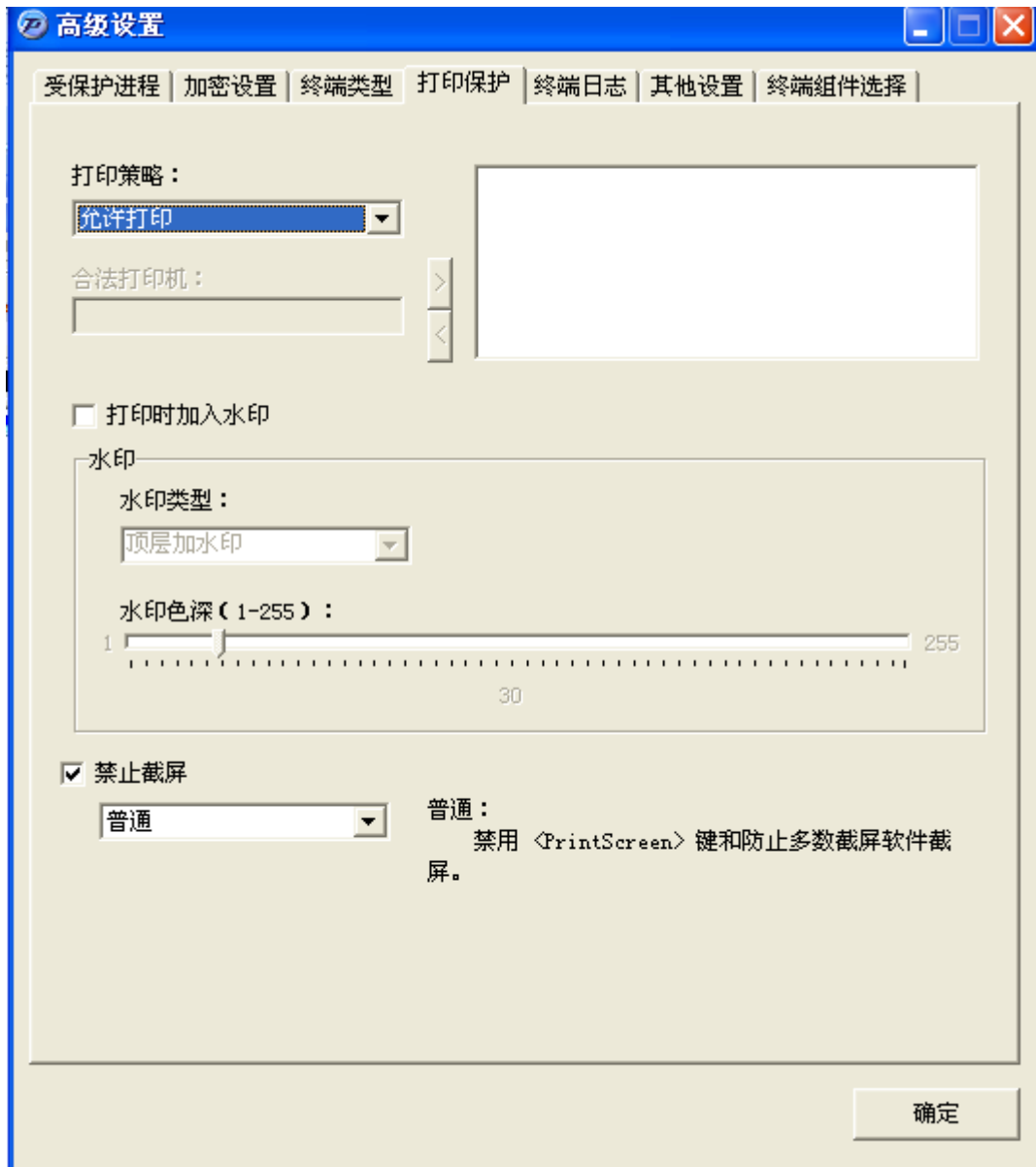
终端掉线后正常运行时间（分钟）：选择、设置终端掉线后正常运行的时间，保证在网络不稳定时客户端能够正常运行。

随系统启动：设置终端程序为开机自动运行。

终端类型默认配置表：

终端类型	身份验证方式	连接到服务器 进行验证	绑定机器码	终端掉线后正 常运行时间	随系统启动
普通	AD 域用户	是，不可修改	无，可设置	无，可设置	是，可修改
只解密不加密	AD 域用户	是，不可修改	无，可设置	无，可设置	是，可修改
外部合作伙伴	Usb-key	否，可修改	无，可设置	无，可设置	否，可修改

2.2.4.打印和截屏保护



2-7 打印和截屏保护设置

在打印策略中，可以对打印进行控制，包括“允许打印”、“禁止打印”和“限制打印”（需要填入合法打印机名称）三种选项，如上图所示：

如果希望终端用户只能将文档打印到指定打印机，则可以选择“限制打印”，并在填入打印机名称后通过“>”按钮添加至合法打印机列表。打印保护同时也可用于保护虚拟打印机。若终端用户将文档输出为 PDF 文件，则需要填入相应的 PDF 打印机名（如“\\Adobe PDF”）。当需要将网络打印机加入合法打印机列表时，必须按照“\\IP 地址\打印机名”的格式进行填写。如果使用列表以外的打印机，将会出现打印机错误提示信息。

水印：可以在文档中中入水印，勾选“打印时加入水印”，并可设置水印显示在底层还是顶层，水印是一组随机数字和字母组合。同时可以调节水印颜色深度，调至 255 时水印颜色最深。水印具体效果如下图所示。在终端日志里可以通过水印来确定什么时间、什么人打印了什么文件。



2-8 水印的效果

在截屏设置中，可以选择是否对截屏操作进行控制，以及控制的力度，其选项含义如下：

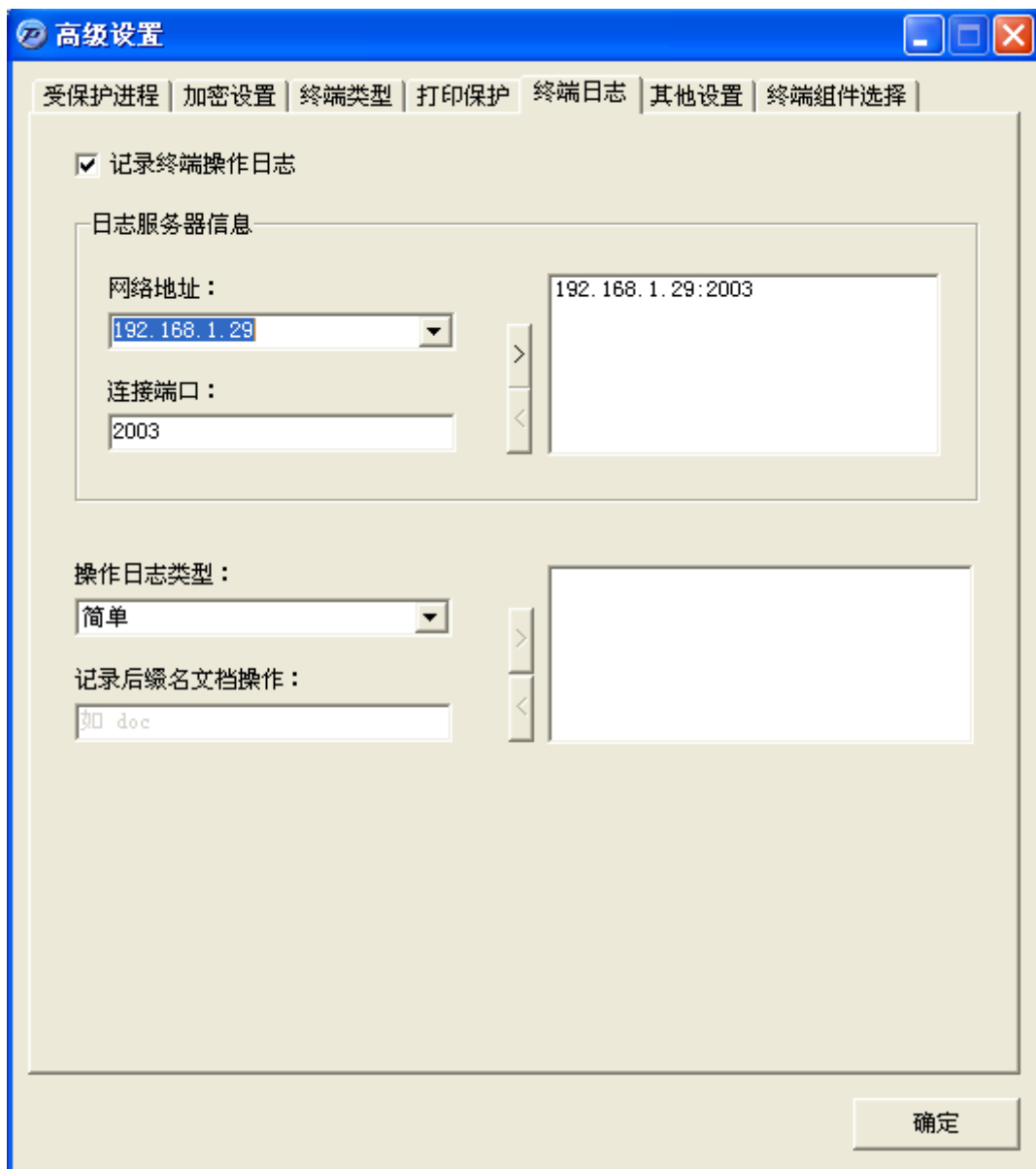
简单：只禁用<PrintScreen>键；

普通：禁用<PrintScreen>键和防止多数截屏软件截屏；

严格：禁用<PrintScreen>键，防止所有截屏软件截屏，但可能在阅读加密文档期间导致其他程序界面无法刷新。

提示：截屏保护仅对加密文件和受保护进程有效，未打开加密文件或受保护进程（或最小化状态）是可以进行截屏操作。

2.2.5. 终端日志



2-9 记录终端日志设置

首先选择正确的日志服务器对外 IP 地址，“连接端口”默认为 2003。然后点击“>”将服务器 IP 地址和端口号加入右侧文本域中。

记录终端操作日志：

简单：只记录文件的复制、移动、重命名、删除、水印操作。

详细：除“简单”设置下的操作记录外，还对文件的打开、修改操作进行记录。

注意：未指定特定后缀名的情况下，仅对加密文件的操作进行记录。

记录后缀名文档操作：添加特定的后缀名，不论文件是否为加密文件，均强制记录与该类文件相关的操作（记录内容依“简单”或“详细”设定而有所不同）。


2.2.6.其他设置



2-10 其他设置

显示终端图标：不选中该项，用户电脑任务栏不会出现铁卷的图标，终端无法调出终端管理界面。

指定终端语言：提供多国语言可供选择。

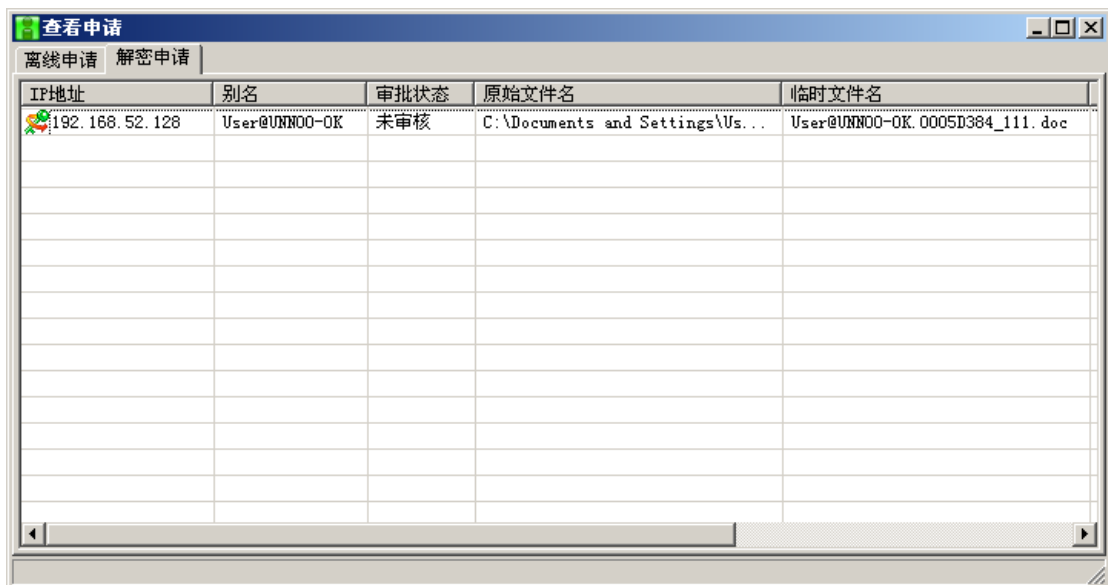
指定终端显示名称：设定终端托盘图标的提示信息。类似的提示信息为“音量”。

实时检测 USBKEY：如果选择此选项，则在所有需验证 USBKEY 有效性的操作中，终端必须始终插入 USBKEY 才能正常工作，如果中途拔除 USBKEY，则客户端认证失败。若不对此选项进行勾选，则仅需要在身份验证或行使特定功能时临时插入 USBKEY，验证通过后即可拔除 USBKEY。

验证代理管理员身份：在同一个部门中，可以设置一个或多个代理管理员，在有终端用户提出申请的时候，同部门的代理管理员将会弹出消息通知。当设置某一终端为代理管理员后，该终端有处理其部门内终端解密和离线申请功能。选中该项后有两项可供选择：密码验证、USBKEY 验证。

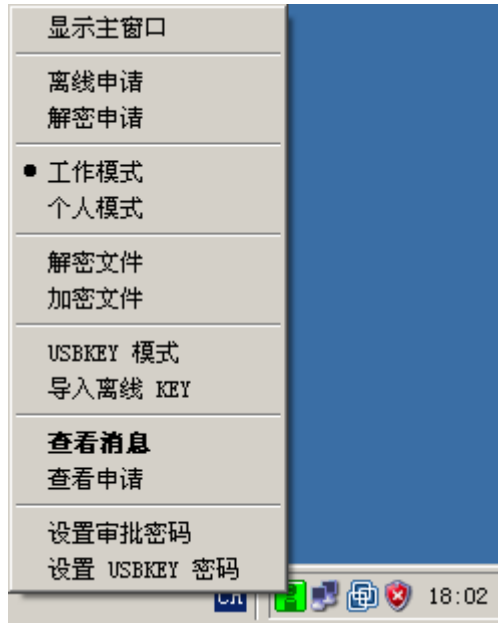
提示：代理管理员提出的申请不会发给自己的用户终端。

密码验证：当执行审批操作时，必须输入密码。默认密码为“1111111”。当有终端用户请求解密文件或离线申请时，代理管理员可以收到终端用户的请求。如下图所示：



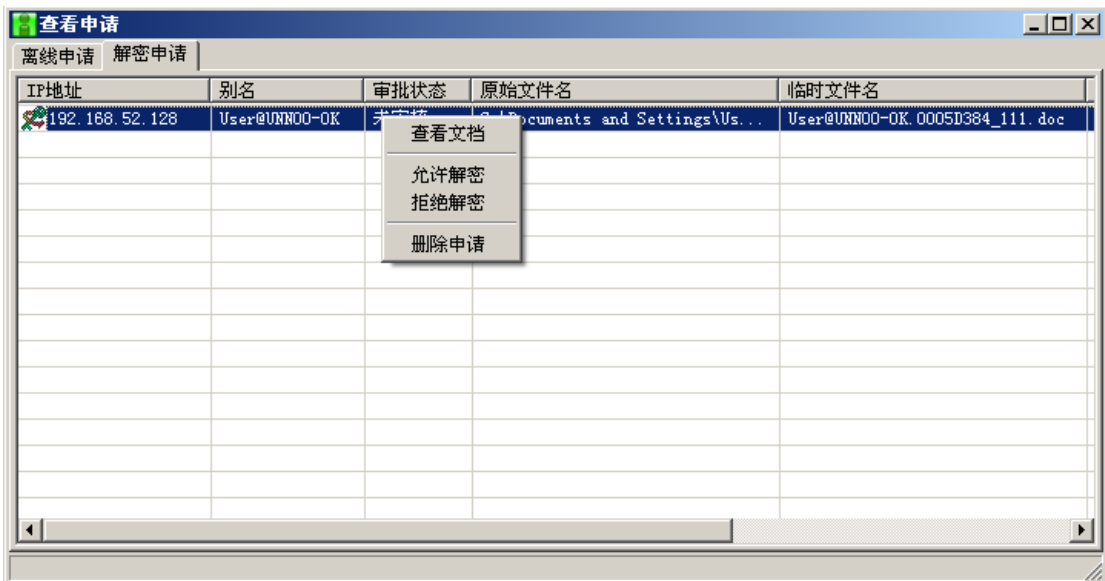
2-11 代理管理员收到终端解密申请

终端用户可以点击“设置审批密码”来设置代理管理员处理解密申请时输入的密码。



2-12 代理管理员设置审批密码

USBKEY 验证：必须插入 USBKEY 时才能进行操作。采用 USBKEY 方式后选择“允许解密”，将出现输入密码窗口，要求输入 USBKEY 的密码：



2-13 查看申请



2-14 输入 usb-key 密码

允许从受保护进程复制限量文字: 铁卷对剪贴板做了保护, 如果不选择该项, 终端程序会禁止从受保护进程复制任何信息到非受保护进程中。如只保护了 Word, 就无法从 Word 复制信息到记事本中。如果选中该项, 客户端将允许从受保护进程复制限量文字到非受保护进程中。

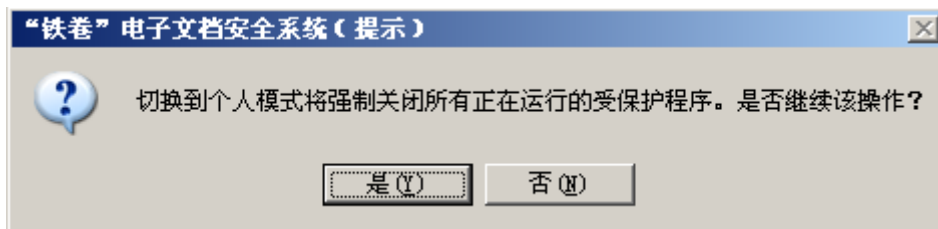
允许终端自行解密: 选中该项后, 用户终端功能菜单有“解密文件”选项, 进行终端可以进行自行解密操作, 不需要由代理管理员审批。

允许终端自行加密: 选中该项后, 终端功能菜单有“加密文件”选项, 用户终端可以进行手动加密操作。

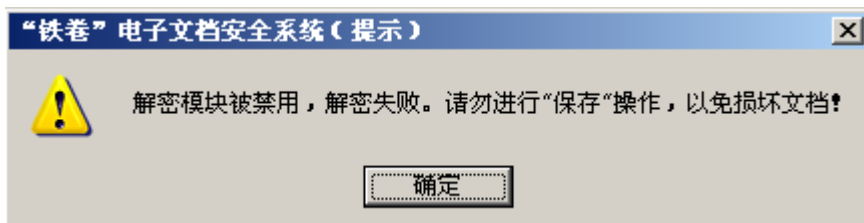
加密 Office 文档时更改后缀名另存: 此选项依赖“允许终端自行加密”, 选择后, 当终端自行加密时, 会将 Office 文档后缀名多加一个 V 字符, 如: test.doc 自动加密后产生一个新的 test.docv 文件。

提示: 此功能一般应用于涉密文件的传阅, 将另存加密后的文件传给只应用了 OfficeView 规则的用户终端进行阅读, 既规定涉密文件的传播范围, 又保证涉密文件的安全。

允许终端切换到个人模式: 选中该项后, 终端功能菜单有“工作模式”和“个人模式”选项, 默认选择“工作模式”。当选择“个人模式”后, 出现下图所示提示。



2-15 终端切换到个人模式时的选择信息



2-16 终端切换到个人模式后的提示信息

两种模式的具体区别见下表(表中的文件与受保护进程关联):

模式	新建文件	对明文的操作	对密文的操作
个人模式	不加密	可操作，不加密	不可操作
工作模式	加密	可操作，加密	可操作，加密

申请解密前上传服务器：申请解密时，终端自动将待解密的文件上传到铁卷安装目录下的 ApplyFiles 文件夹内。

审批解密后打包：选中该项后，终端在解密成功后会出现打包压缩窗口。

区别显示加密文档：选中该项后，加密后的文件图标上带一把小锁。显示效果如下图所示。



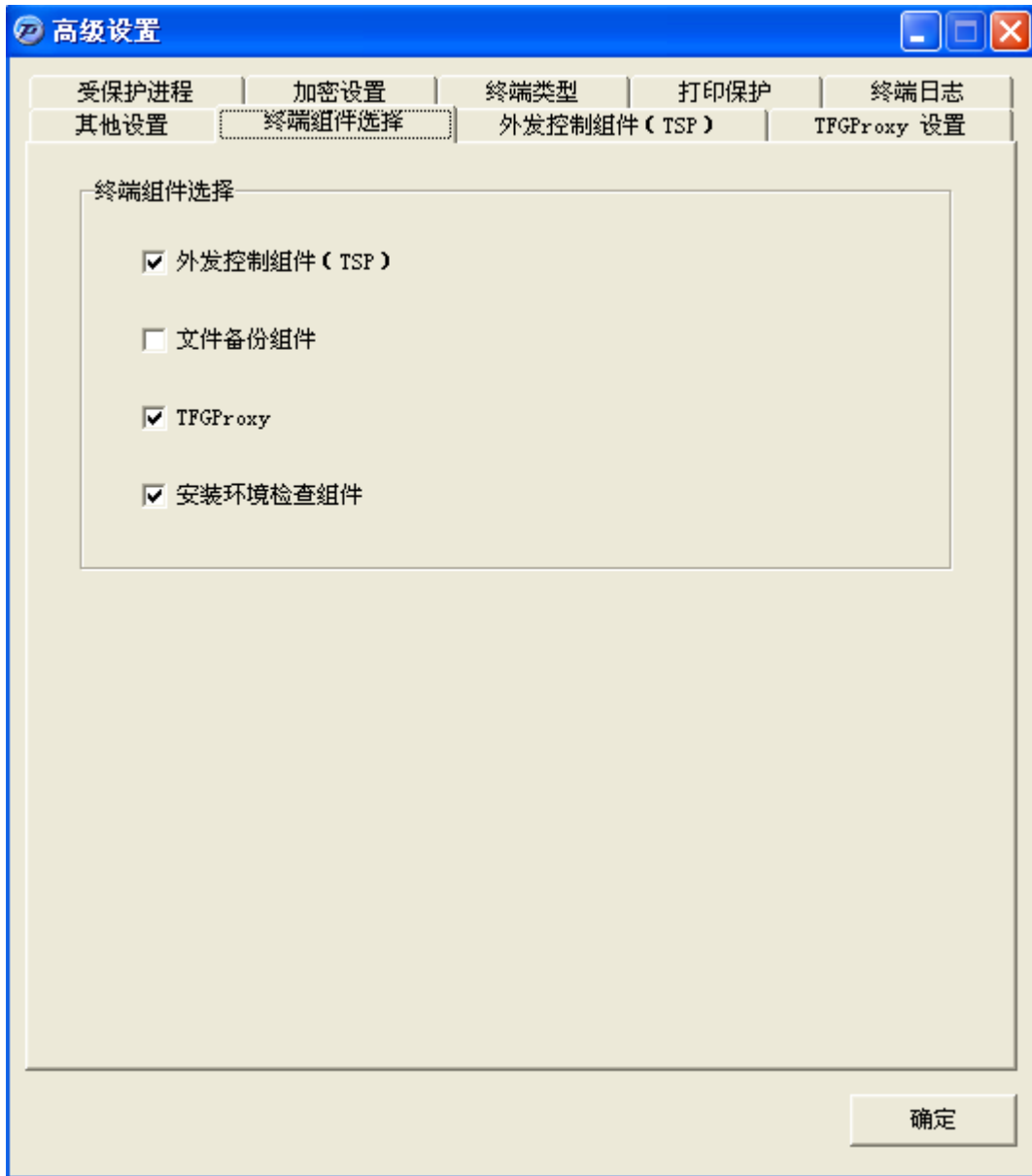
2-17 加密前的文件图标



2-18 加密后的文档图标

2.2.7. 终端组件选择

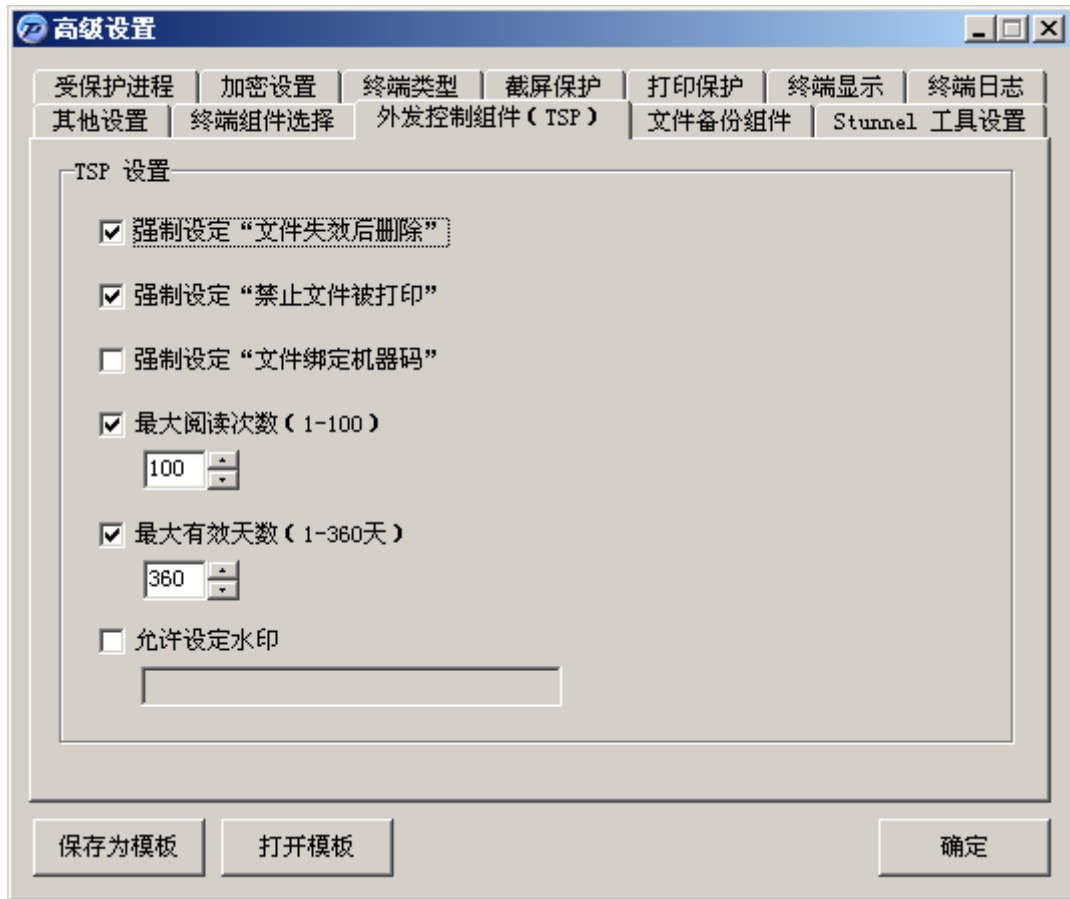
铁卷为用户提供的可选组件包括：外发控制组件（TSP）、文件备份组件、TFGProxy 和安装环境检查组件。



2-19 终端组件选择界面图

2.2.8. 外发控制模块 (TSP)

TSP 是 Total Safe Printer 的缩写。是本公司开发的一款基于虚拟打印技术的文档外发控制软件，此模块需要另行选购。如下图所示，各项选项的含义非常明了（详细说明请参考 TSP 使用说明书）：

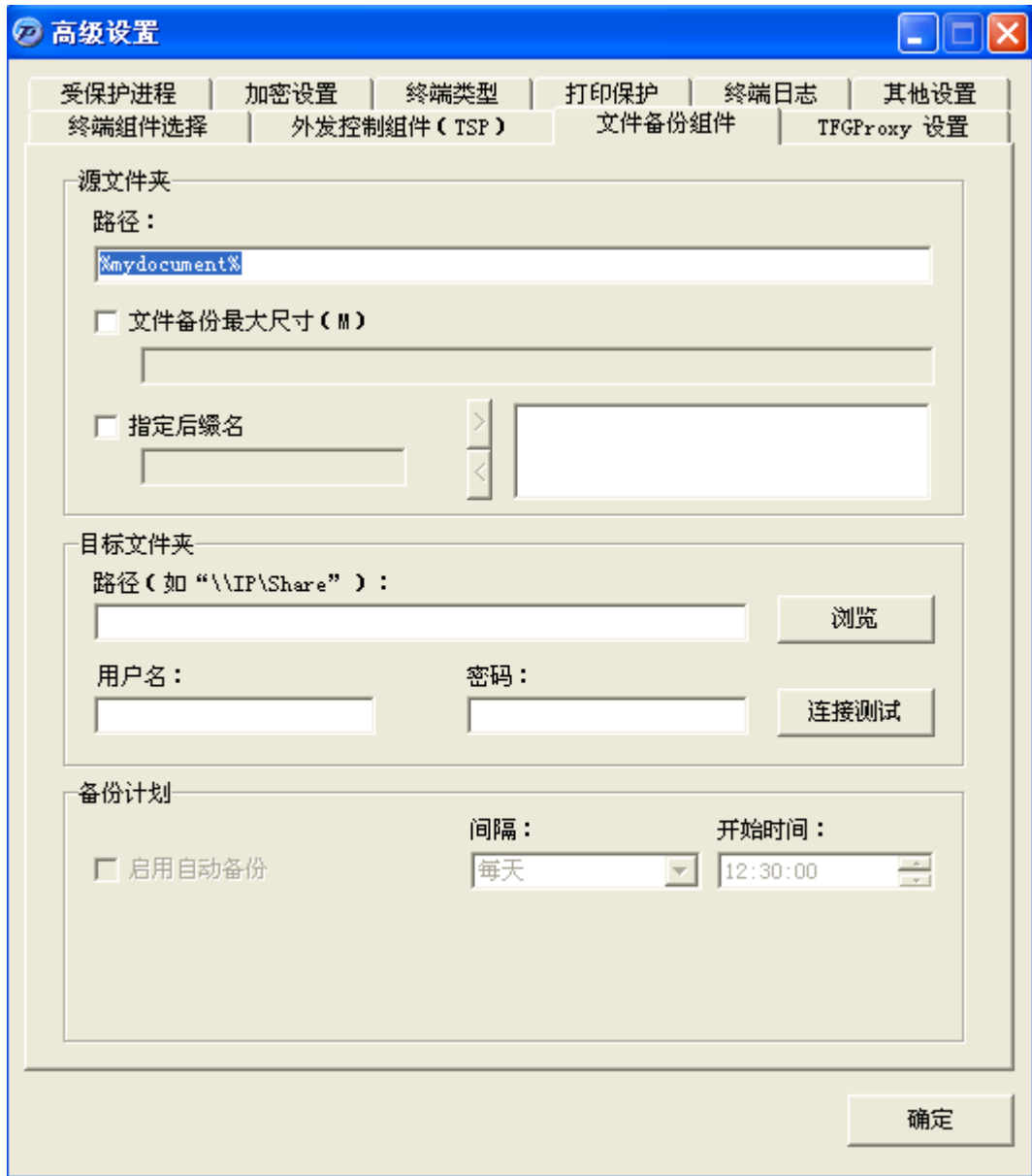


2-20 外发控制组件

2.2.9. 文件备份模块

铁卷内置了文件备份模块，可以将本地文件备份到指定的位置（通常为网络共享文件服务器）。文件备份工具可以设置自动备份时间，也可以手动备份。

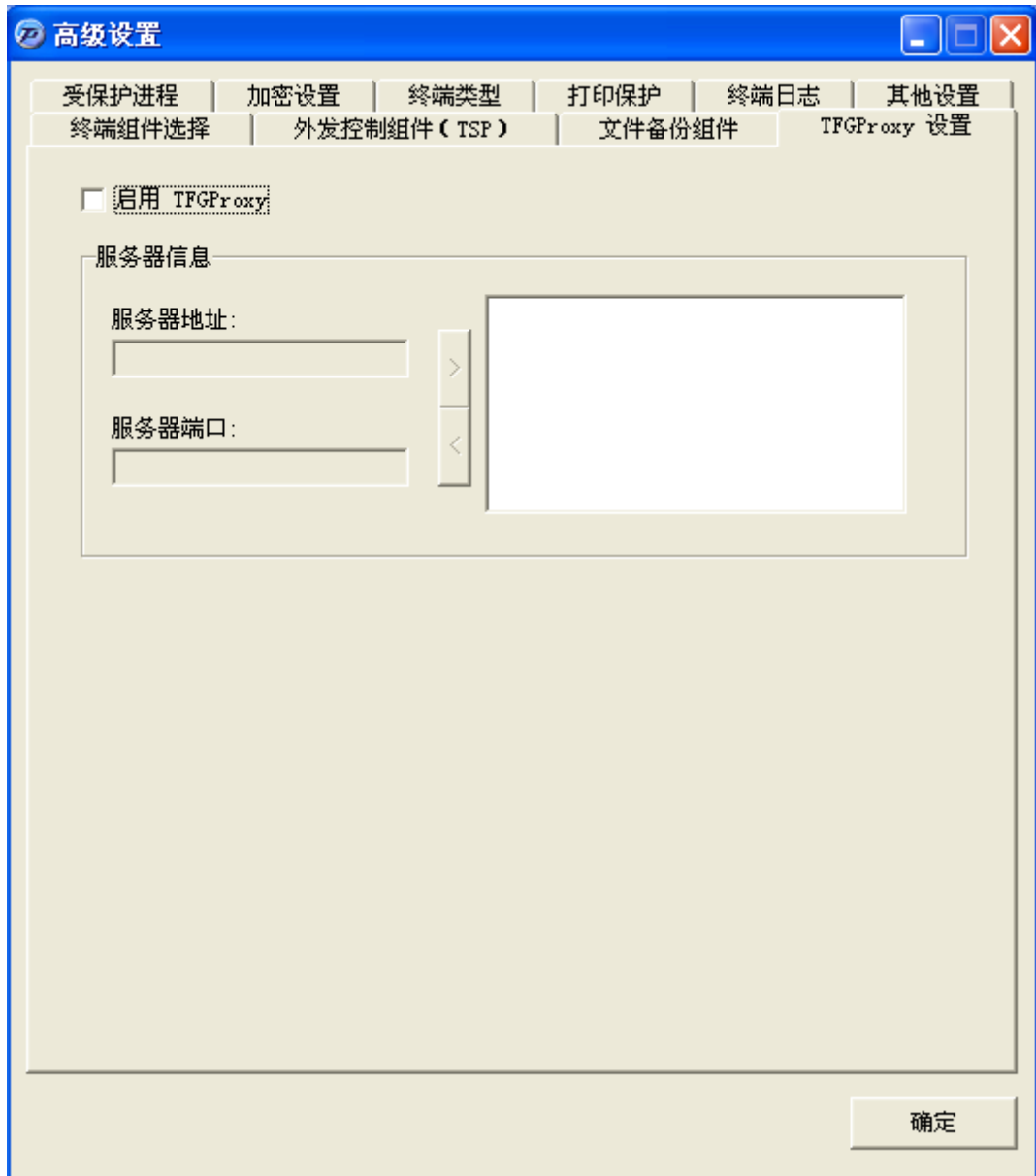
要启用文件备份先勾选“启用自动备份”，在源文件夹和目标文件夹内设置好路径（网络路径或本地路径）。用户名和密码为 Windows 共享方式登录目标机器的用户名和密码。为分散网络带宽负荷，文件备份工具里自动备份的实际执行，是自设定时间开始的半小时区间内随机触发的。



2-21 文件备份组件

2.2.10. TFGProxy 模块

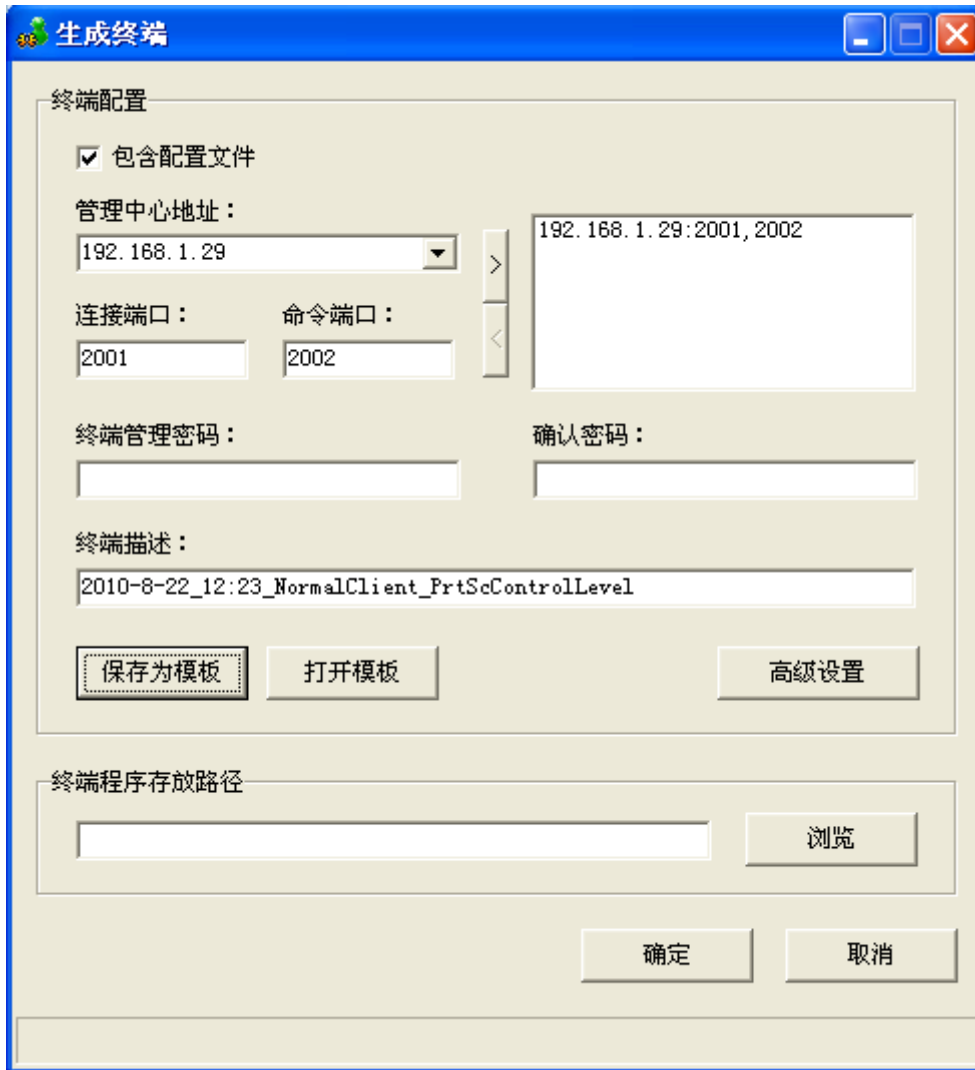
铁卷可选购 TFGProxy（安全代理）模块，此设置页只提供 TFGProxy 的客户端配置，服务端需要另外搭建，具体请参考 TFGProxy 配置手册。主要保护企业事业中的各种应用系统，控制对应用系统的准入和应用系统中数据进行保护。



2-22TFGProxy 模块设置界面

2.3. 策略模板

通过窗口左下角按钮可以保存和打开客户端配置模板（规则文件除外），不必每次重新设置各个选项。



2-23 高级设置界面图

2.3.1.模板的创建

点击上图中的“保存为模板”，弹出“保存终端模板”的界面，如下图。在“保存终端模板”的界面中填写好模板名称和描述，描述最好能表示出这个模板的一些特定设置。然后点“确定”，用户终端模板即创建成功。

3. 客户端管理

3.1. 终端状态

点击终端信息标签页可查看当前终端状态，包括连接状态、别名、计算机名、当前用户、所属部门、版本、配置说明等状态信息。

IP地址	别名	计算机名	当前用户	所属部门	终端状态	高优命令数目	程序版本	允许接入	终端配置信息描述
192.168.52.156	陈炳生	D7181F52X	admin	质检部\海克斯...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.164	薛斐勃	IUEAIQIN	hkl s6	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.60.115	熊莹珍	LGCT521	user001	液压机械有限公...	离线	0	3.1.59h	是	2009-01-13 14:27
192.168.52.157	前丹红	T-96856ZF91E2C4	user001	液压机械有限公...	离线	0	3.1.59h	是	2009-01-13 14:27
192.168.52.158	张有砂	LGCT509	admin	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.25.98	李鹏鹏	HJLS26888	user001	液压机械有限公...	离线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.119	罗云秀	JLS888	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.118	徐敏	CM888	CM	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.143	黄克玉	LG-HJLS888	lqh	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.157	江彦	CHEMTAKSHUT	hkl s4	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.122	林飞坤	LG	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.126	代冬梅	VJ0020	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.142	钟德红	LG0337	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.165	邓家兴	A	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.113	前如善	前如善	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.124	刘小英	HJLS-CK	user001	液压机械有限公...	离线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.123	陈阳辉	CH	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.106	陈阳辉	CHANGYU	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.58.157	梁方贵	CHEMTAKSHUT	hkl s5	液压机械有限公...	离线	0	3.1.59h	是	2009-01-13 14:27
192.168.52.139	熊巧香	LG-BC031D05T1A7	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.52.125	王发连	COCO	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.52.134	周露芳	LG0495	user001	液压机械有限公...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.59.129	曾启祥	ZENGZONG	admin	液压机械有限公...	离线	0	3.1.59h	是	2009-01-13 14:27
192.168.45.182	梁丹	HJLS0510	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2008-12-18 17:10
192.168.45.184	李一峰	LGCT042	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2008-12-18 17:10
192.168.45.144	石涛	LGCT094	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.51.13	张应文	LG7055	user001	研发部门\挖掘...	离线	0	3.1.59h	是	2008-12-18 17:10
192.168.45.137	王玉慧	HJLS20	admin	研发部门\挖掘...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.45.165	蔡文祥	LGCT034	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2008-12-18 17:10
192.168.45.160	王娟	LGCT057	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2009-01-13 14:27
192.168.45.151	文兵	LGCT054	user	研发部门\挖掘...	在线	0	3.1.59h	是	2008-12-18 17:10
192.168.45.169	张冬菊	LG03141	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2008-12-18 17:10
192.168.45.185	张斌	LGCT037	user001	研发部门\挖掘...	在线	0	3.1.59h	是	2008-12-18 17:10

3-1 终端状态表

3.2. 认证管理

3.2.1. 接入模式

3.2.1.1. 允许/拒绝接入

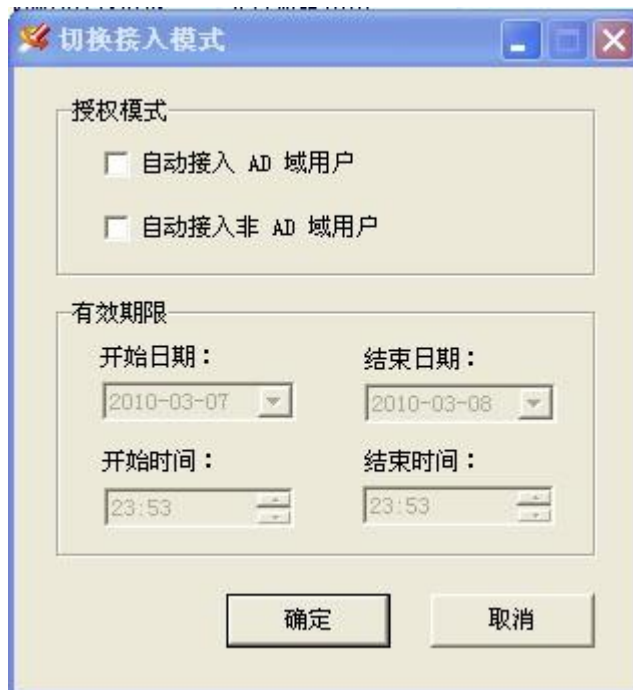
当用户安装好用户终端后，服务器上会收到如下图所示的终端信息，管理员通过执行未接入用户终端右键菜单中“允许接入”进行认证激活；也可通过执行已接入用户终端右键菜单中的“拒绝接入”操作，使用户终端失效，并且可执行“从数据库中删除”操作，使失效用户终端不显示。



3-2 接入模式

3.2.1.2. 自动允许接入

如果用户非常多，可以通过选择“工具”->“切换接入模式”，在弹出的窗口中选择“自动”，这样终端程序首次运行时自动允许接入，减少的管理员的工作量。



3-3 切换接入模式

可选择自动接入 AD 域用户和自动接入非 AD 域用户，可同时选取。并且可设置自动允许接入的有效期限，到结束时间后，新安装的用户终端需要手动认证接入。

3.2.2.Usb-key 模式

用户终端通过使用 usb-key 模式进行认证，类似银行的 U 盾认证。具体操作为选取客户端的“usb-key 模式”，提示插入 usb-key，输入正确的密码通过认证。



3-4USBKEY 模式

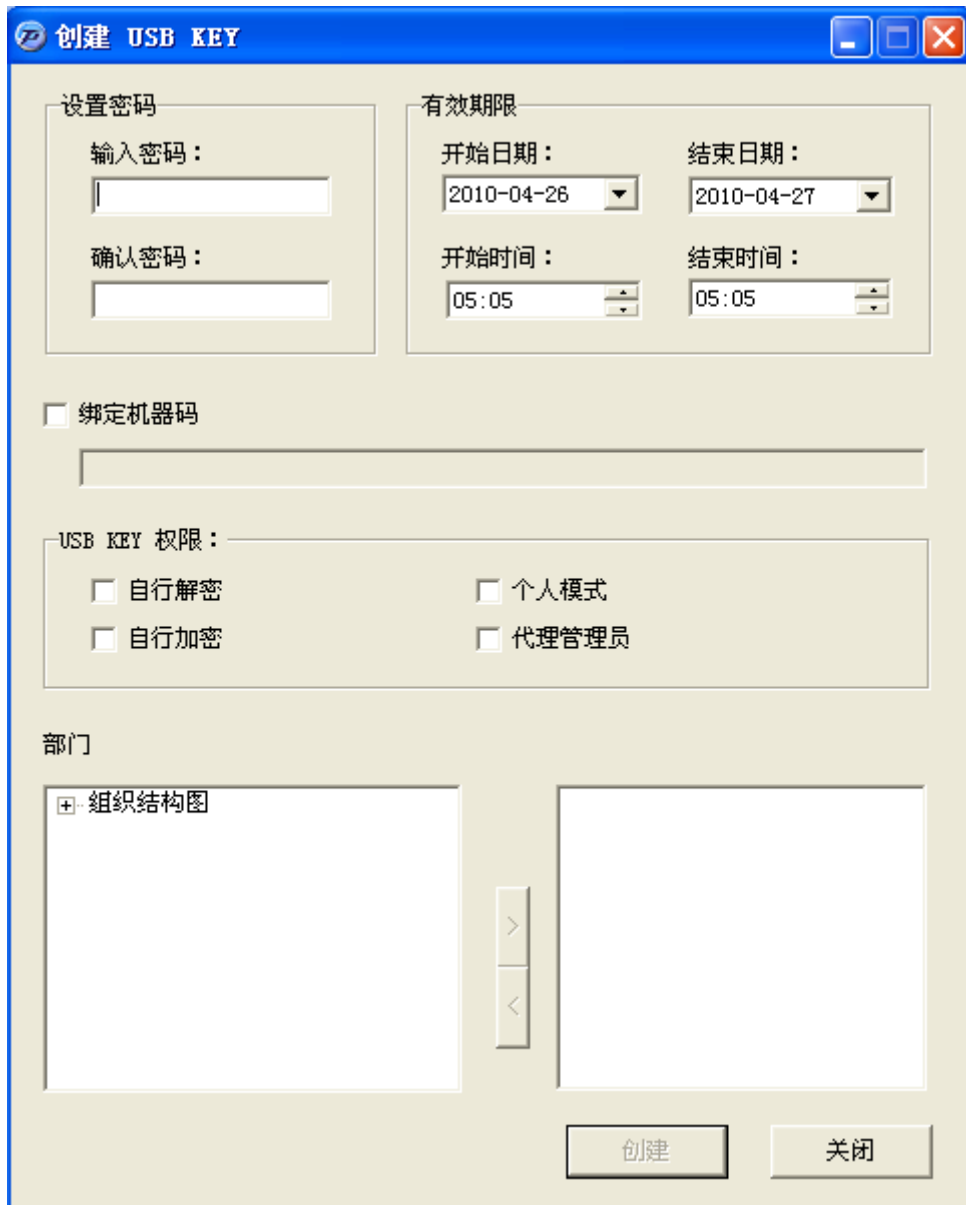
Usb-key 的创建:

在管理中心主界面菜单点击“管理中心”->“创建 usb key”，将 usb-key 插入服务器的 usb 口。

警告：创建时必须将服务端 KEY 拔出。



3-5 创建 usb-key



3-6 创建 usb-key

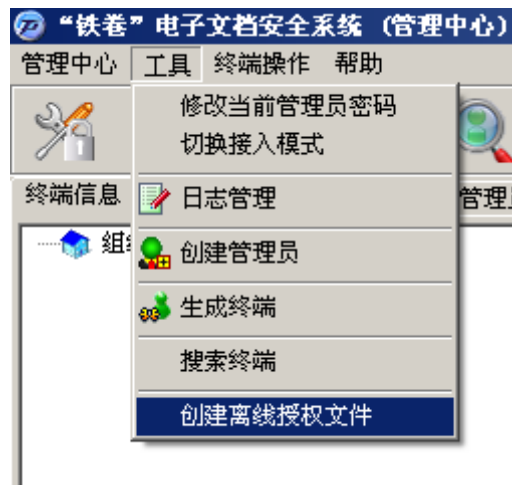
输入要使用该 USB KEY 时所需要的密码和该 USB KEY 的有效时间，选择 USB KEY 的权限和所属部门，点击“创建”按钮。此时 USB KEY 上的红色指示灯会闪烁不停，表示数据正在写入。数据写入完毕后，系统将提示创建 USB KEY 成功并询问是否需要继续创建。

3.2.3. 软证书模式

用户终端通过使用软证书模式进行认证，类似正版软件的许可文件。具体操作为执行客户端的“导入离线授权文件”，选取正确的授权文件，输入正确的密码通过认证。用户终端也可以执行“取消离线”操作结束软证书认证模式。

离线授权文件的创建:

在管理中心点击“工具”->“创建离线授权文件”。在出现的窗口中设置好开始结束时间和保存的位置。



3-7 创建离线授权文件

创建离线授权文件

累计时间

12 小时

有效期限

开始日期： 2010-04-26 结束日期： 2010-05-06

开始时间： 06:28 结束时间： 06:28

密码：

输入密码：

确认密码：

绑定机器码

文件存放路径

浏览

确定 取消

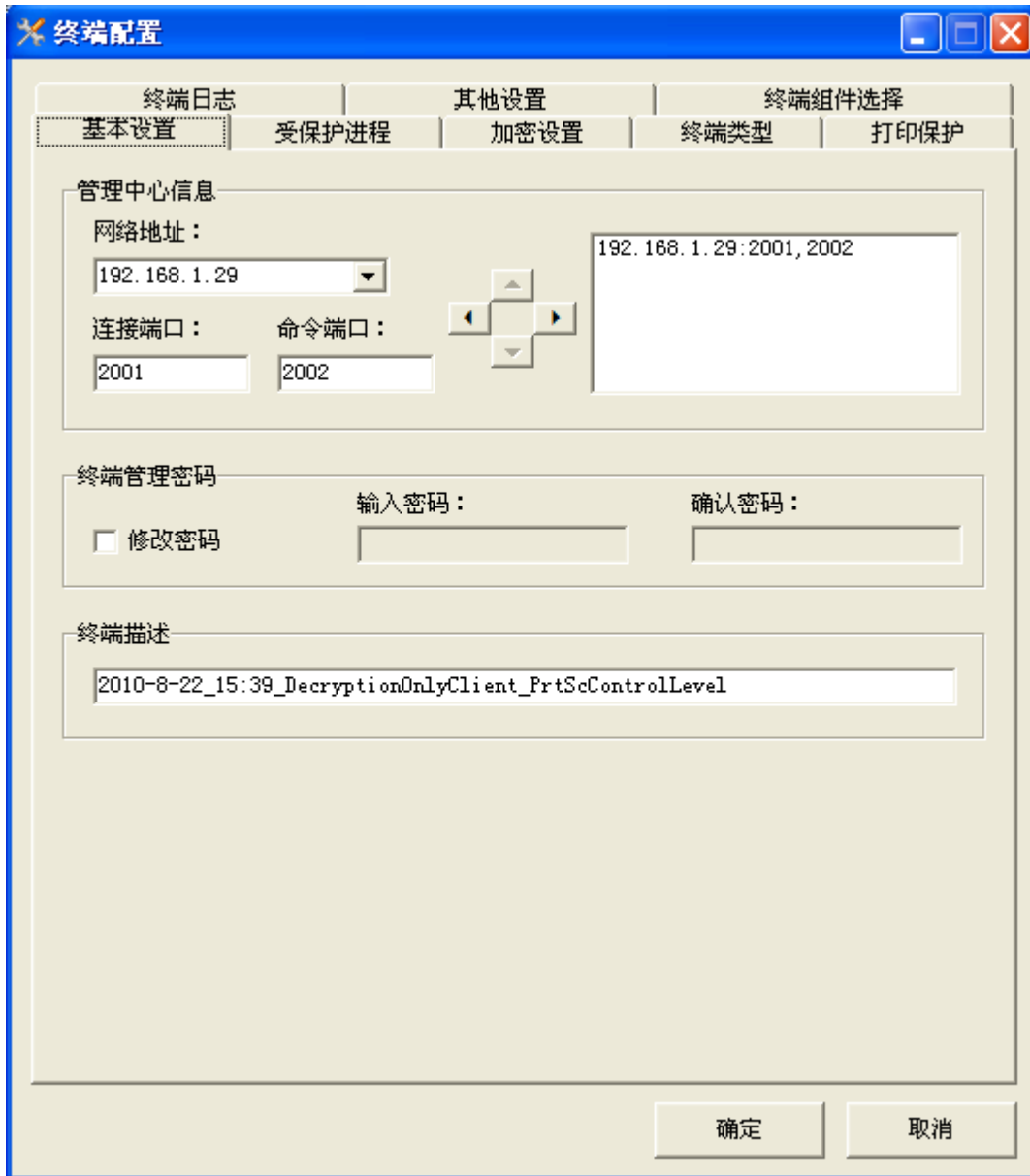
3-8 配置离线授权文件

把生成的离线授权分发给终端用户。当用户离线时可以导入该离线授权文件。在规定的有限日期和累计时间内用户终端通过认证使用。

注意：离线授权文件导入一次后即作废，不能进行重复导入操作。

3.3. 查看/修改变略

在终端信息标签页，管理员通过执行用户终端的“终端信息”操作来查看和修改当前用户终端的策略。



3-9 查看、修改策略

提示：“终端组件选择”不能通过修改配置来增删，只能通过重新生成新用户终端安全程序并升级客户端来增删。

3.4. 组织管理

铁卷组织管理主要体现在管理中心的“终端信息”标签页的组织结构图中，如下图所示。



3-10 组织结构图

3.4.1. 组织结构图的建立

手动建立： 在下图所示组织结构图上右击在出现的菜单中选择“增加子部门”，输入部门名称。也可以向子部门内添加子部门，方法相同。

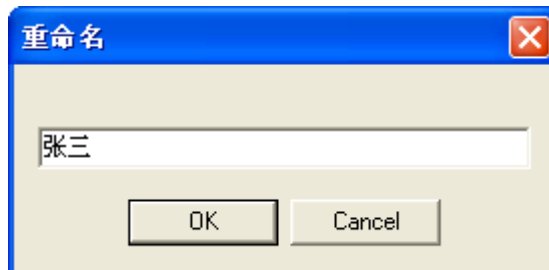


3-11 建立组织结构图

自动建立：如果公司内已经建好 AD 域环境，并且用户终端都采用“AD 域认证”的方式进行认证，按 AD 域结构自动建立组织结构图。

3.4.2. 终端重命名

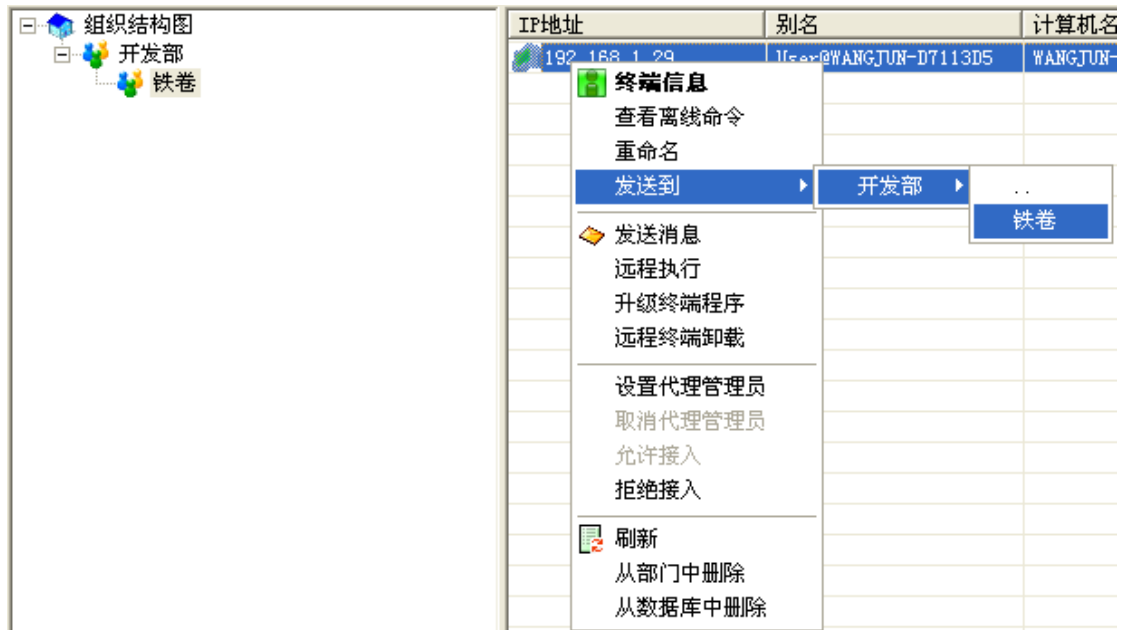
用户终端名称默认为“当前用户@计算机名或域名”，为了方便在组织管理中更直观的显示，并且在日志审计中准确定位到人，一般都会将用户终端别名重命名为计算机的责任人姓名。具体操作为执行用户终端右键菜单中的“重命名”，修改别名。如下图所示：



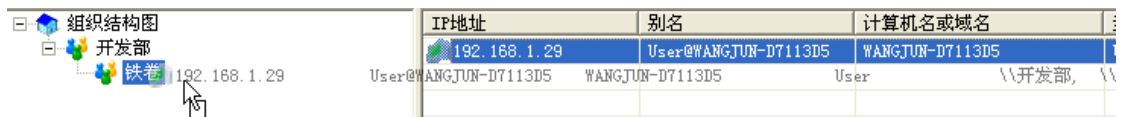
3-12 终端重命名

3.4.3. 添加到组织

组织结构图建立好后，需要将用户终端添加到相应的组织或部门中（AD 域认证自动添加），可以先选取同一部门的用户终端一次性添加（可使用 Ctrl 和 Shift 组合键）到部门中，也可以使用拖拽的方法将用户终端拖入部门中。如下图所示：



3-13 发送到组织



3-14 拖拽到组织

3.4.4. 从组织中移除

如果要从组织或部门中将某一用户终端移除，请执行用户终端的右键菜单中“从部门中删除”操作。

3.4.5. 审批模式

对各个部门内的用户终端提出的离线和解密申请，可按照企业需要设置自动审批模式或者代理审批模式。

自动审批模式：部门内用户终端提出的离线和解密申请系统自动批准。

代理审批模式：部门内用户终端提出的离线和解密申请系统默认发给代理管理员，由代理管理员进行审批。

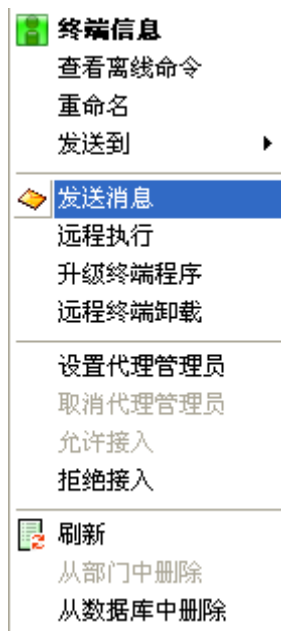
注意：代理管理员不能审批自己的申请，由上一级代理管理员审批。



3-15 审批模式

3.5. 命令管理

命令管理主要集中在管理中心用户终端的右键菜单上，见下图：



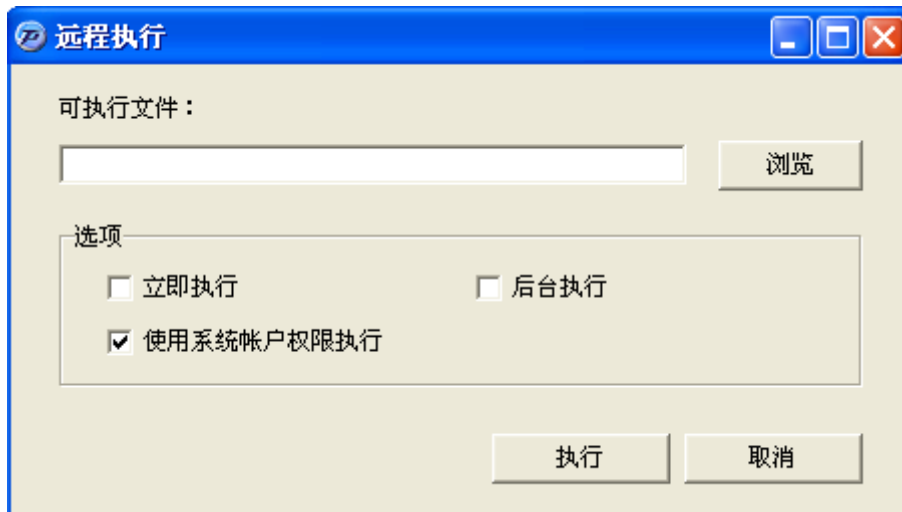
3-16 用户终端菜单

3.5.1. 发送消息

当管理员需要给用户发通知时，可以利用上图中的“发送消息”命令来实现，可以使用 Ctrl 和 Shift 组合键。

3.5.2. 远程执行

铁卷为方便管理员远程执行管理或维护工具时,可通过上图中的“远程执行”命令来实现,并且可以选择执行的方式。



3-17 远程执行

3.5.3. 远程升级/远程卸载终端程序

管理员可以通过上图中的“升级终端程序”和“卸载远程终端”进行升级用户终端和卸载终端。为保证企业网络在升级时不拥堵,升级终端程序在 24 小时内随机完成,卸载终端实时生效。

3.5.4. 查看/删除离线命令

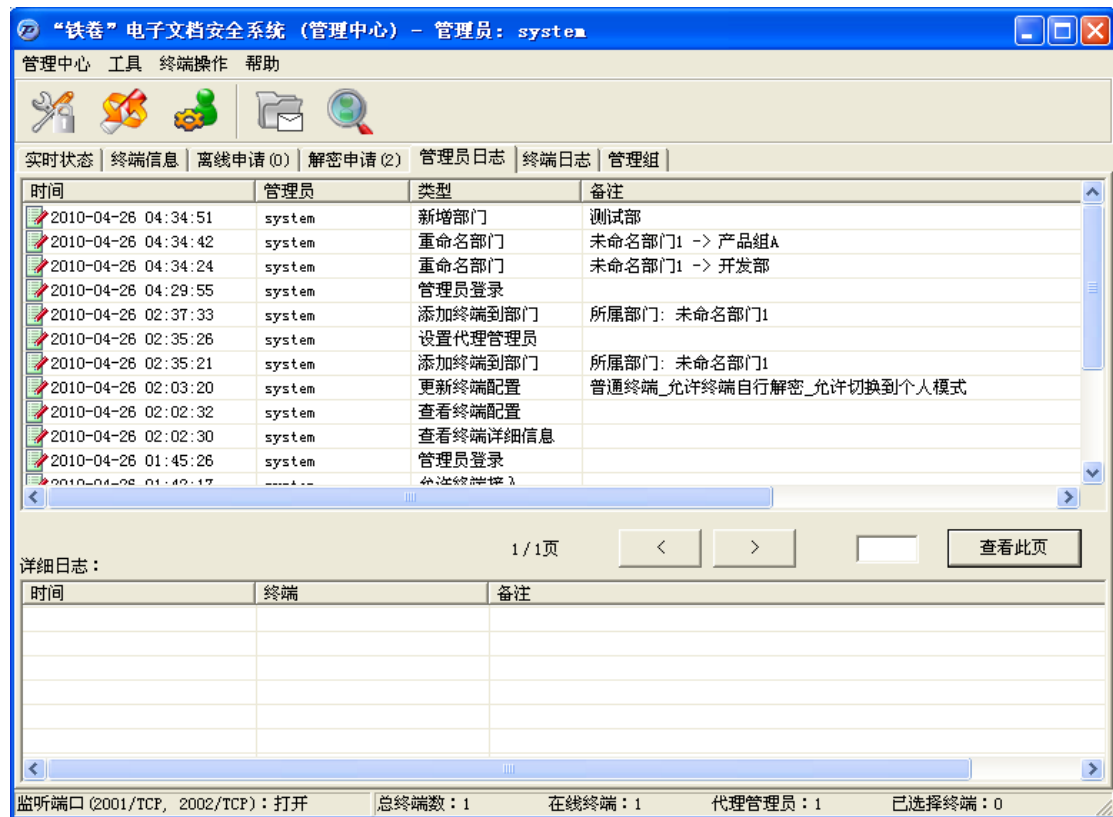
当管理员在执行命令管理时,在线用户终端实时执行;离线用户终端会保留一个离线命令,上线后离线命令马上执行。通过执行“查看离线命令”查看具体命令,也可以删除掉已作废的离线命令。

4. 日志审计

4.1. 实时日志

实时日志分“管理员日志”和“终端日志”，分别位于管理中心的两个标签页，实时记录了管理员和用户终端所有敏感操作。

铁卷提供了详细的操作日志，这些日志是被铁卷系统自动、强制记录的，可供具有“日志管理员”权限的管理人员查看。



4-1 查看管理员日志

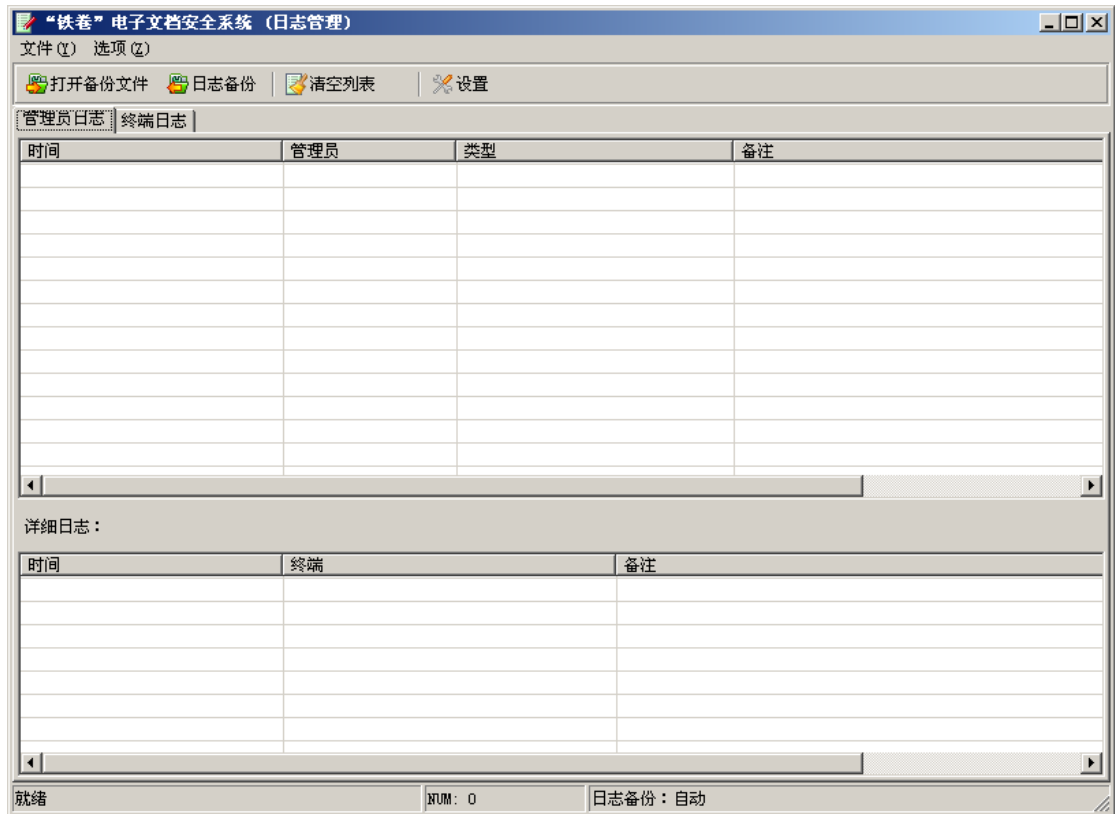
如下图所示，我们在文本框内输入页码后点击“查看此页”，就可以看到该页中所有信息。也可以点击“>”或“<”来查看下一页或上一页。



4-2 查询某一页日志

4.2. 日志管理

铁卷提供了方便的日志管理功能，通过单击“工具”->“日志管理”就会进入日志管理的主界面。日志管理程序，包括导入日志、导出报表和备份日志功能。导入日志后，避免日志太多时加载时间过长，必须输入搜索条件才能显示结果。

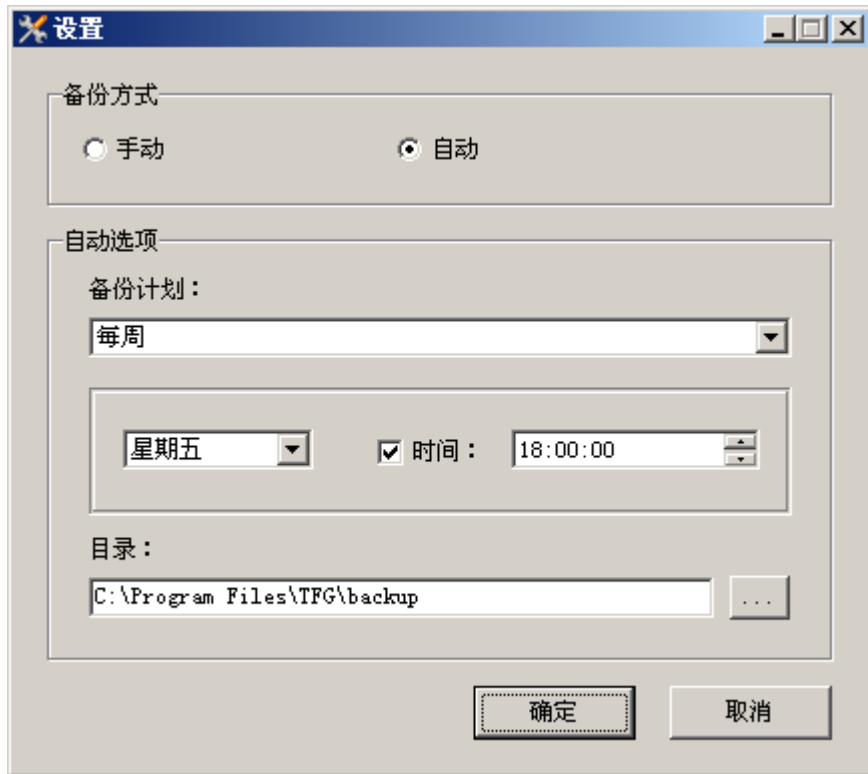


4-3 日志管理主界面

4.2.1. 日志备份

自动备份

铁卷的日志备份功能提供两种方式，即自动备份和手动备份。默认情况下为自动备份，需要特别注意的是自动备份功能会清除掉日志。选择“选项”菜单里的“设置”功能，会弹出“设置”窗口，如图：



4-4 备份方式设置界面

在“设置”窗口里可以对自动备份进行更详细的设置，比如备份计划可以设置按天、按周、按月进行备份以及备份的时间等。如果选择了手动备份，自动备份功能将取消。

手动备份

选择“文件”菜单的“日志备份”，会弹出手动备份的窗口，选择日志备份的起始时间，设置是否备份后清除日志即可。日志备份功能界面如下图：



4-5 日志备份功能界面

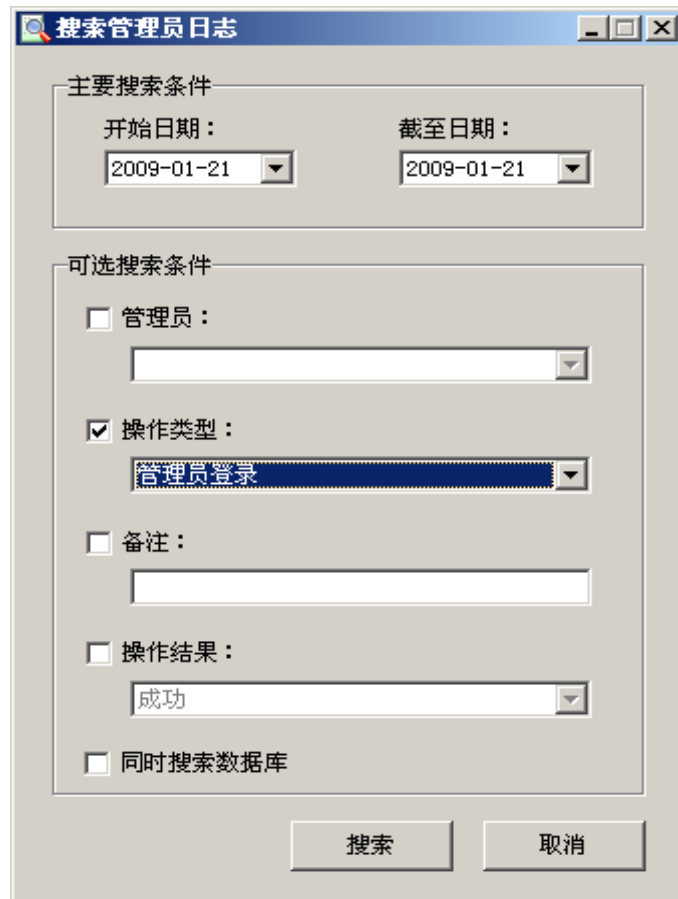
注意：此处备份产生的文件是 xml 格式。自动备份后为防止实时日志过大默认清除实时日志，手动备份时可选择是否清除实时日志。

4.2.2. 日志查询

“文件”菜单里的“打开备份文件”功能，主要是导入先前备份过的 xml 文件（可一次导入多个）然后进行解析，以方便进一步的查询或导出报表等操作。

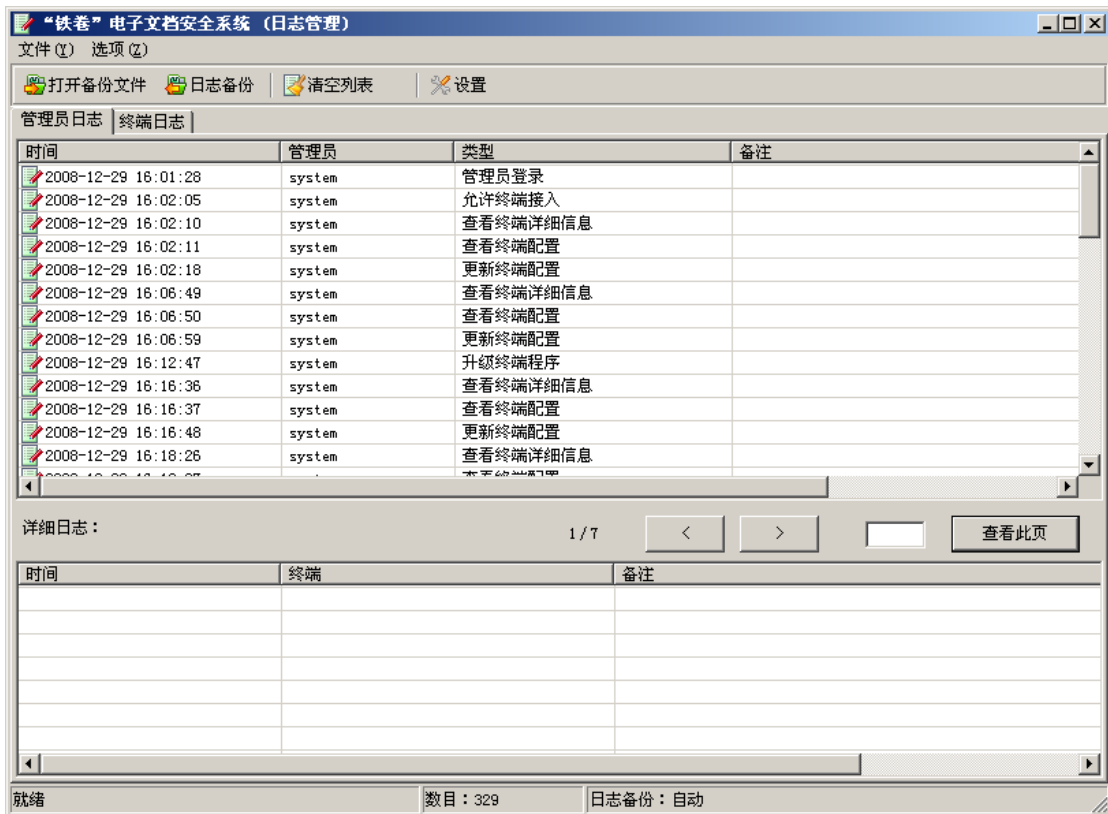
导入备份过的 xml 文件进来后，会提示：导入日志成功，请查询需要的日志信息。

在“管理员日志”或“终端日志”里空白处右击，选择“查询日志”功能，即可利用查询功能找到想要的数 据，如下图：



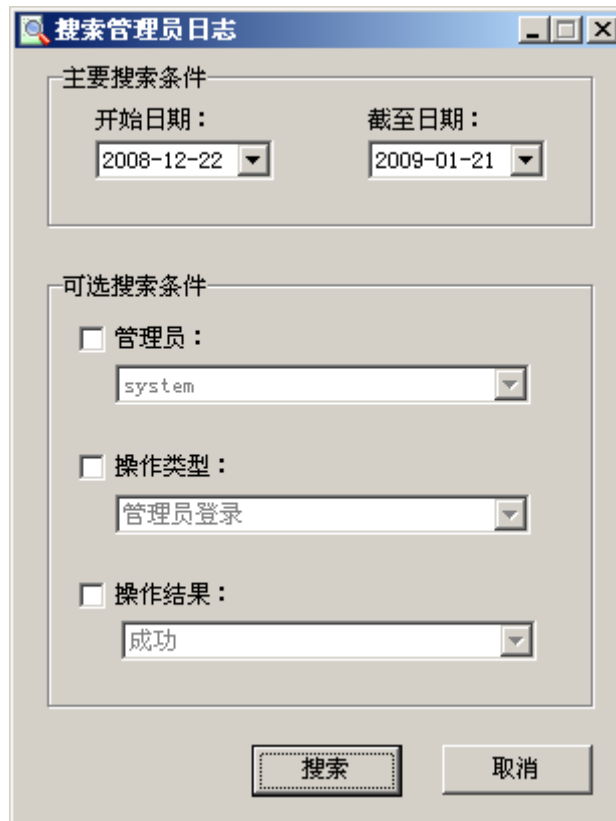
4-6 设置搜索日志

设置好搜索条件后，点击“搜索”按钮，会显示出搜索到的结果，如下图：



4-7 搜索后的显示界面

另外，导入日志功能支持多个 xml 文件导入，然后进行查询显示。



4-8 搜索管理员日志

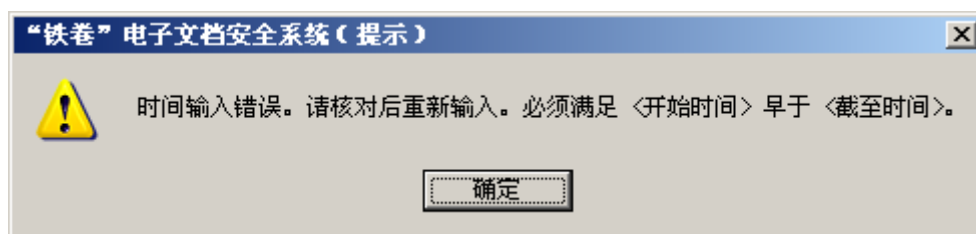
铁卷提供了日志搜索的功能，以方便管理员从海量的日志信息中找到自己需要的日志。在日志标签栏里点击右键，在弹出菜单中选择“搜索管理员日志”。

主要搜索条件：确定一个搜索范围。只搜索“开始日期”、“截止日期”这间的日志。当我们点击开始日期或截止日期后将出现日期选择窗口，如下图所示。



4-9 选择开始或结束日期

当我们选择错误，例如选择的“开始日期”大于“截止日期”时间将会出现出错提示。

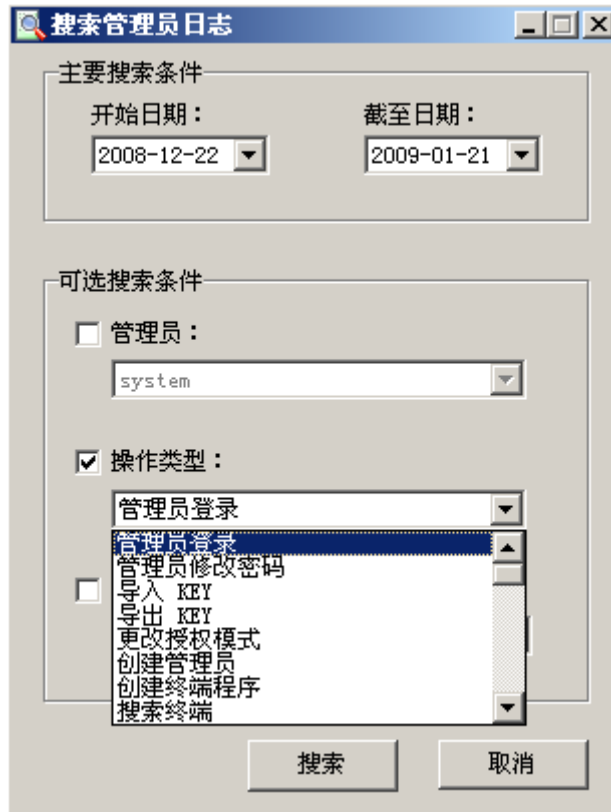


4-10 出错提示

可选搜索条件：含有三个可选项。

管理员：该选项下拉菜单中包含所有已存在的管理员账号。选择某一管理员，则搜索范围仅限制在这个管理员范围内。

操作类型：包含多种管理员操作事件。如下图所示。



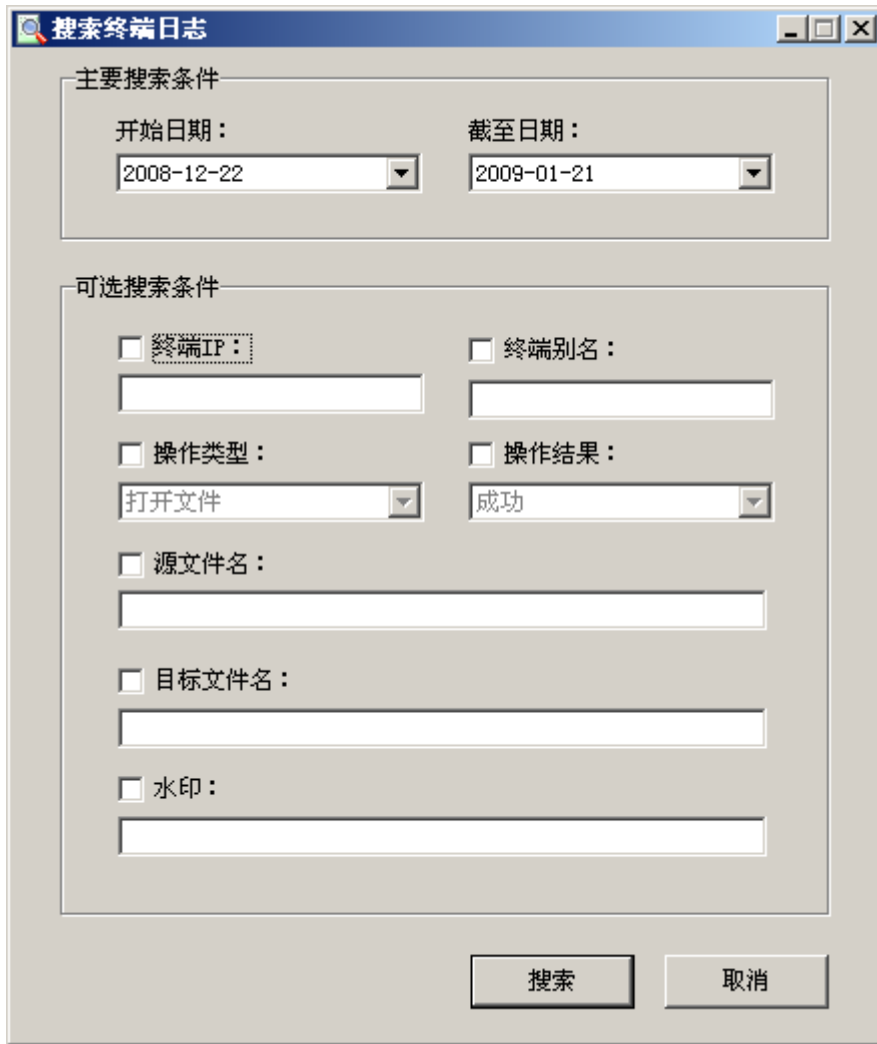
4-11 设置搜索管理员日志搜索条件

操作结果：有成功和失败两种选项。

管理员根据需要填写相应的条件，铁卷会自动列出符合条件的日志。也可以选择清空管理员日志。清空后，会产生一条清空日志。

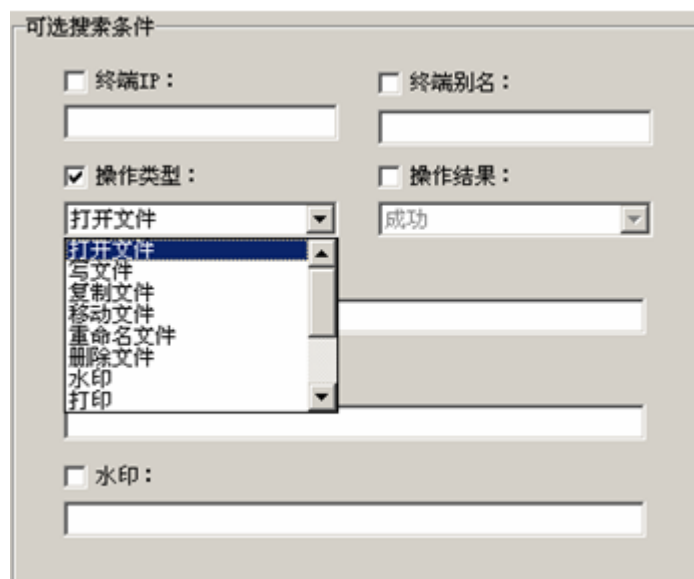
终端日志的大部分操作同管理员日志，已介绍过的不再介绍。搜索日志窗口如下图所示。

主要搜索条件：确定一个搜索范围。只搜索开始日期、截至日期之间的日志。和搜索管理员日志相同。



4-12 设置搜索终端日志搜索条件

可选搜索条件：特别说明以下几项。



4-13 可选搜索条件

4.3. 审计报告

这个功能主要是对搜索出来的结果导出，生成一个 **xls** 格式的文件，供审查。在搜索出来的结果中，右击选择“全部选中”，然后右击选择“导出报表”功能，即可对搜索出来的结果进行导出，导出成功后会有提示信息。

5. 系统管理

5.1. 监控服务器状态

在任务栏里单击小齿轮“服务器管理器”会弹出如下图的界面。

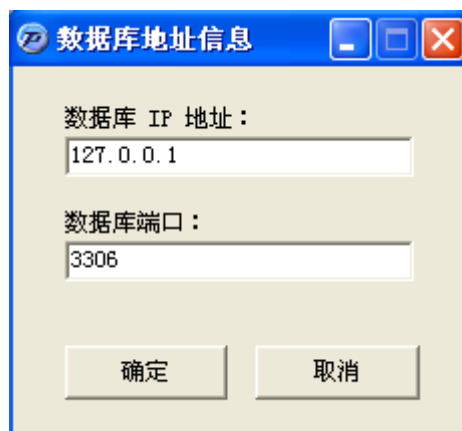


5-1 服务器管理器界面



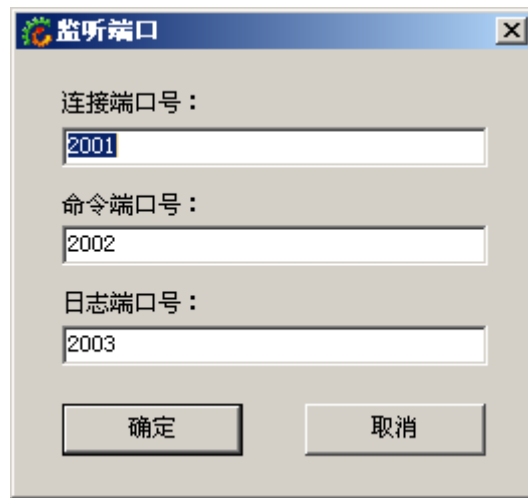
5-2 服务器状态

执行数据库配置，可以查看数据库的 IP 地址和端口。数据库连接端口默认是 3306，建议不要更换。



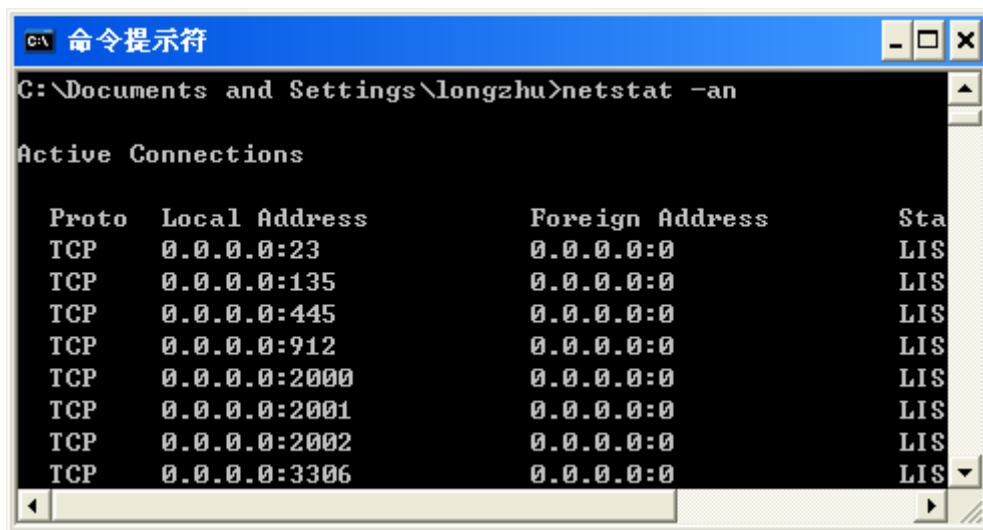
5-3 数据库配置界面

可以通过单击“服务器管理器”->“监听端口”来监控服务器的连接端口情况，服务器使用 2001 号端口接收终端连接命令，2002 号端口接收终端数据，2003 号端口接收日志。这三个端口通常不需要更改。



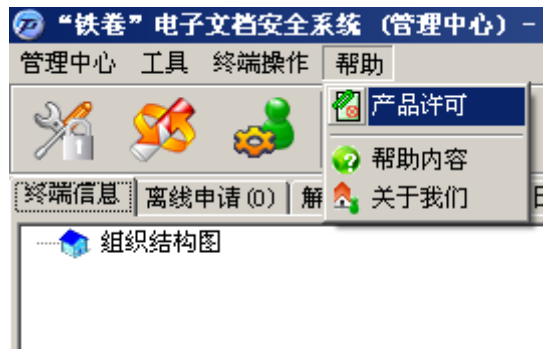
5-4 监听端口界面

也可以在命令提示符下输入 `netstat -an` 查看这三个端口的运行状态。



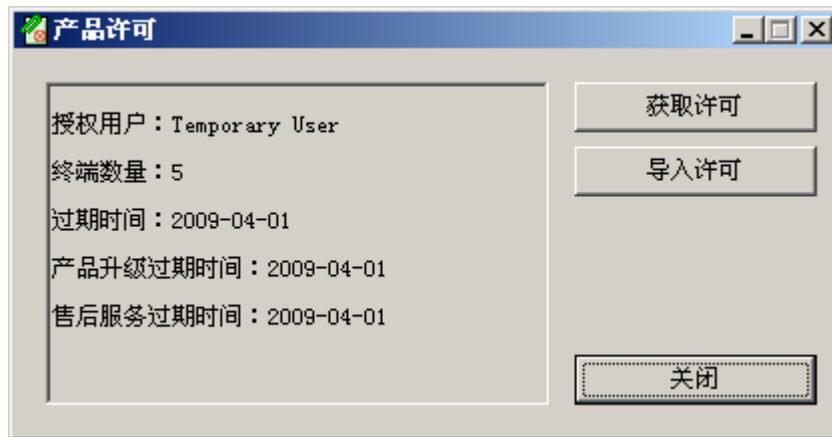
5-5 查看端口状态

5.2. 许可管理



5-6 产品许可菜单

查看产品使用期限，点击“帮助”->“产品许可”，将出现如下窗口。窗口中显示有过期时间。



5-7 产品许可信息

点击“获取许可”。程序将生成一个 inf 文件，将此文件命名为“公司名称.inf”，通过 E-mail 等方式将此文件发给深圳市大成天下信息技术有限公司。

深圳市大成天下信息技术有限公司在收到上述文件后，将生成一个授权文件，使用“帮助”->“产品许可”->“导入许可”将此授权文件导入。

导入正版授权后，需要重新启动铁卷服务器。

提示：也可以通过执行实时状态页面的“导入许可”完成许可的导入。

5.3. 申请管理

管理员可以在管理中心实时查询或处理未审核的离线和解密申请，如下图所示。

IP地址	别名	审批状态	文件名	原始文件名
192.168.1.29	User@WANGJUN-D7113D5	未审核	新建 Micros...	C:\Documents and Settings\User\桌面\新建...
192.168.1.29	User@WANGJUN-D7113D5	未审核	呀看不.doc	C:\Documents and Settings\User\桌面\呀看...
192.168.1.29	User@WANGJUN-D7113D5	未审核	~\$呀看不.doc	C:\Documents and Settings\User\桌面\~\$呀...
192.168.1.29	User@WANGJUN-D7113D5	未审核	20100805_关...	C:\Documents and Settings\User\桌面\2010...
192.168.1.29	User@WANGJUN-D7113D5	未审核	呀看不.doc	C:\Documents and Settings\User\桌面\呀看...

5-8 申请管理界面

5.4. 密钥管理

5.4.1. 密钥的备份

为了避免因为服务器硬件损坏、操作系统崩溃造成不可挽回的损失（例如所有加密文档因为密钥丢失导致无法解密），铁卷提供密钥导出备份功能，选择菜单上的“管理中心”->“导出密钥”，系统会首先要求输入一个密码，该密码将用于将来的密钥导入（请牢记该密码，否则即使备份密钥也无法恢复）：



5-9 设置密钥导入密码

输入密码后点击“确定”按钮，弹出密钥保存窗口，这时可以选择适当的位置保存密钥。如果系统弹出以下提示，则密钥导出成功。



5-10 导出密钥成功提示

5.4.2. 密钥的恢复

如果由于系统崩溃需要重新安装服务器，管理员可以利用导入密钥功能方便地将铁卷密钥导入目前系统，而无需重新部署所有客户端，点击菜单上的“管理中心”->“导入密钥”。这时我们选中之前导出的密钥文件，单击“打开”按钮。



5-11 选择要导入的 KEY 文件

在弹出的“输入密码”对话框中输入备份时的密码，如果密码正确，则会弹出以下提示窗口，密钥导入成功：



5-12 警告信息

5.5. 管理组

铁卷为保障服务器安全，允许多个管理员对服务器进行管理，并授予管理员不同的权限，以保证管理员不会越权操作。启动管理中心或将管理中心从最小化恢复时，均需要通过登录验证。

管理员的权限分为：

- 普通管理员

普通管理员拥有审核终端和部门行为（如解密申请，允许接入，添加、删除部门等）、属性（如重命名，修改终端所属部门）的权限。但不具有审核日志，创建管理员，安装、卸载铁卷的权限。

- 日志管理员

日志管理员拥有审核、清空日志的权限。（清空日志后，会产生一条关于此次操作的新日志）

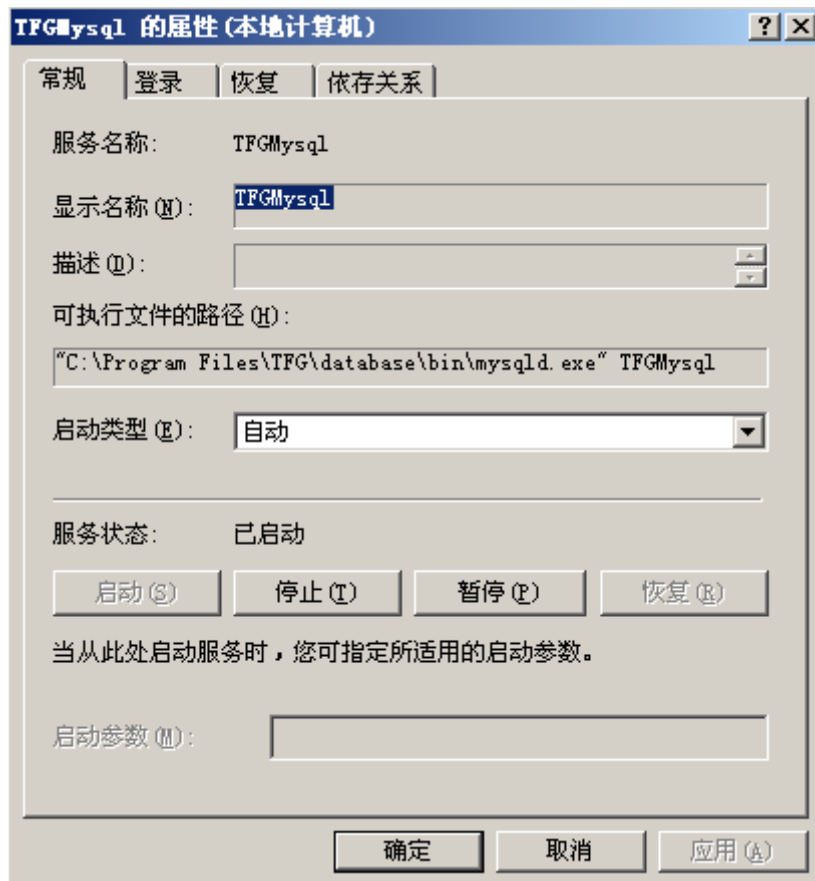
- 系统管理员

系统管理员拥有创建、修改、删除管理员，安装、卸载铁卷的权限。

同一个账号可以同时拥有一种或多种管理员权限。

具有“系统管理员”权限的管理员可在“工具”->“创建管理员”菜单中创建新的管理员。

5-13 创建管理员



5-15TFGMysql 服务