

恒隆文档加密软件

用户管理手册

公司名称：无锡恒隆科技有限公司
地 址：江阴市金山路201号数码港F座5楼
联系电话：0510-86023225、86023235
公司网址：www.hl158.net
邮箱地址：zmb040912@126.com

目 录

| | |
|-----------------------|----|
| 第一章 系统概述..... | 4 |
| 1.1 系统简介..... | 4 |
| 1.2 主要模块及其功能..... | 4 |
| 第二章 安装与卸载..... | 8 |
| 2.1 机器码..... | 8 |
| 2.2 服务端安装..... | 10 |
| 2.3 客户端安装..... | 13 |
| 2.4 客户端卸载..... | 16 |
| 2.5 服务端卸载..... | 18 |
| 2.6 服务端及客户端升级..... | 19 |
| 2.7 win8 64位系统配置..... | 23 |
| 第三章 定义加密策略配置..... | 26 |
| 3.1 服务器加密策略..... | 26 |
| 3.2 本机加密策略..... | 31 |
| 3.3 如何自定义加密策略..... | 32 |
| 3.4 设置本机离线使用天数..... | 32 |
| 3.5 出差在外离线延时..... | 33 |
| 3.6 加密密级管理..... | 35 |
| 3.7 禁用或只读 U 盘..... | 36 |
| 3.8 显示加密锁标记..... | 35 |
| 3.9 设置少量文本拷贝..... | 37 |
| 3.10 设置程序定向拷贝..... | 37 |
| 3.11 设置备份目标目录..... | 39 |
| 3.12 客户端扫描加密策略..... | 39 |
| 3.13 手动更新本机加密策略..... | 40 |
| 第四章 解密流程使用配置..... | 41 |
| 4.1 启用解密流程..... | 41 |
| 4.2 创建恒隆加密系统的用户..... | 42 |
| 4.3 解密流程..... | 45 |
| 4.4 常见问题..... | 51 |
| 第五章 文件外发配置..... | 54 |
| 5.1 文件外发的 4 大特点..... | 54 |
| 5.2 如何将外发文件做成外发包..... | 54 |

| | |
|----------------------|----|
| 5.3 外发包的使用..... | 58 |
| 5.4 查看外发记录..... | 60 |
| 5.5 常见问题..... | 61 |
| 第六章 明文邮件配置..... | 62 |
| 6.1 邮件白名单介绍及其作用..... | 62 |
| 6.2 邮件白名单的创建..... | 62 |
| 6.3 白名单的导入与导出..... | 63 |
| 6.4 注意事项及常见问题..... | 65 |
| 第七章 文件备份管理..... | 66 |
| 第八章 系统维护..... | 69 |
| 8.1 系统维护菜单..... | 69 |
| 8.2 诊断工具菜单..... | 78 |

第一章 系统概述

1.1 系统简介

恒隆文档加密软件是无锡恒隆科技有限公司推出的一套比较完善的、安全的数据加密软件。该软件分为服务器和客户端，每个装有该系统的企业都包含一个服务器和若干客户端。在客户端上创建或修改的文件是被加密的，文件从企业流出以后，在其他地方是无法正常查看的，要想查看必须启动特定的解密流程，经过各级审核，到最终解密方可查看，这在很大程度上保证了企业数据的安全性。每个企业的密钥和服务器硬件信息完全捆绑，产生唯一的机器码做为不同企业的认证。任意客户端登陆到服务器上都会接受服务器的认证。

该系统采用了默认为加密，解密需授权，事事有记录的管理理念。在保证数据安全性的基础上，所有流程按大多数企业需求设计，企业可以自己设置加密策略，按需设置要加密的文件类型，对哪些应用程序进行加密以及对文件扫描加密的时间，系统还支持客户端自动扫描加密，只要设置好了加密策略，系统会定期自动扫描设置的路径，进行加密操作。在符合基本需求的基础上，该系统还提供了像明文邮件、外发控制等功能，满足了绝大多数客户的需求。

1.2 主要模块及其功能

| 模 块 | 功 能 | 说 明 |
|-------|----------|--|
| 服务端软件 | 多种后台数据库支 | 可以支持： SQL Server ORACLE ACCESS |
| | 文件备份传输 | 客户端若要求自动备份数据，服务器将自动接收这些数据并归档到服务器中 |
| | 企业加密密钥认证 | 不同企业的密钥是不一样的，每个企业的密钥和服务器硬件信息完全捆绑，捆绑的硬件有：网卡、CPU 及硬盘，三者经过加密运算得到一个唯一的机器码做为不同企业的认证 |
| | 客户端认证 | 对每台连接到服务器的客户端进行认证，检测是否是本企业的授权的机器 |

| | | |
|--------|----------|---|
| 客户端软件 | 内核驱动 | 内核驱动可以支持： 32 位 Windows 2000、XP、Win7 及 Win8 32 位 Windows Server 2003、2008 64 位 Windows XP、Win7 及 Win8 64 位 Windows Server 2008 |
| | 客户端软件自保护 | 保护内核驱动不被非法卸载 |
| | 手工加密文件 | 可以对文件进行手工加密，加密后的文件可以进行修改保存，用户无法感知客户端存在 |
| | 手工解密文件 | 经过授权，可指定某几台客户端可以直接解密文件（通过审批流程是另外一个模块），解密的文件记录用户日志可以查询 |
| | 文件强制加密 | 根据加密策略对受控的应用产生、保存的所有文件进行加密 |
| | 监控文件操作 | 监控文件的操作，对改动的文件备份进行监控，并通知服务器进行备份 |
| 用户管理 | 认证本企业用户 | 结合服务器机器码及本机机器码，通过认证服务器进行用户身份认证，属于本企业的用户才能打开本企业的文件 |
| | 加密密级管理 | 能够在同一企业内进行加密密级的划分，例如可以划分设计部可以打开行政部的所有文件，而行政部无法打开设计部的文件，即行政部产生的文件密级较低。通过密级定义，可以定义出复杂的级别关系 |
| | 行政部门划分 | 对行政机构进行划分，并按部门或组别的解密审批，只有有权限的人才能进行文件解密的审核及批准 |
| 加密策略定义 | 新增加受控的程序 | 若标准加密策略中没有一些的应用程序，可以将这些应用程序增加的加密策略中。可以支持 32 位及 64 位的 Windows 程序 |
| | 自动派发服务器加 | 服务器加密策略修改后，自动派发到客户端 |
| | 客户端可以选用不 | 加密策略可以按计算机进行派发，例如高层领导的文件不加密，但可以打开加密文件，而普通员工的文件需要强制加密 |
| | 屏幕录制控制 | 在打开密文的情况下，无法录制屏幕，也无法使用 PrintScreen 按键进行屏幕拷贝，并禁 |

| | | |
|--------|------------|--|
| | U 盘、移动硬盘控制 | 止 QQ 等的截图传输 可以完全禁止，或者将 U 盘、移动硬盘变只读盘，即只能从移动硬盘的文件复制到本机硬盘，反之则禁止 |
| | 打印机控制 | 禁止指定的计算机进行文件打印 |
| | | |
| 明文邮件 | 白名单定义 | 可以定义 3 种规则： (1) 指定发件人解密，凡是该发件人发送的附件，给任何人都自动解密； (2) 指定收件人解密，任何人将附件发送给该收件人都自动解密； (3) 同时指定发件人和收件人，符合某人发邮件给某人，附件自动解密。 |
| | Outlook 集成 | 可集成 32 位操作系统的任何 Outlook 版本的无缝集成，自动使用白名单规则； 可集成 64 位操作系统的 32 位 Outlook 程序 (64 位操作系统装 32 位程序) 的无缝集成； |
| | Foxmail 集成 | 可集成 32 位操作系统的任何 Foxmail 版本的无缝集成，自动使用白名单规则； 可集成 64 位操作系统的 32 位 Foxmail 程序 (64 位操作系统装 32 位程序) 的无缝集成； |
| | 其它邮件客户端 | 按客户需求开发定制 |
| 文件外发控制 | 自解压包 | 将需要外发到外部的文件制作成一个自解压包（是一个 exe 执行程序），自解压包可以在任何机器上运行自解压，也可以指定接收计算机的必须是给定的机器码才能进行自解压 |
| | 打开次数控制 | 可以控制外发的文件打开一定的次数后自动销毁并非删除文件，只是自解压失效，以前解压出来的文件也无法打开，复制出来的文件也无法打开 |
| | 控制打开时间 | 可以控制文件在一定时间内是可以打开的，过了有效期后无法再打开 |
| | 控制外发文件打印 | 可以指定外发的文件能否进行打印 |

| | | |
|--------|-----------|--|
| 解密流程管理 | 审核、解密权限定义 | 可以指定每个部门都有自己的审核人和解密人，跨部门不能选取其他部门的审核人或解密人为自己审核和解密文件 |
| | 解密审计功能 | 可以查看申请人、审批人、解密人的日志记录，汇总哪些人解密过多少文件 |
| | 任务提醒功能 | 解密任务可在线执行，流程流转至自己时，会有消息自动提醒 |
| | 控制外发文件打印 | 可以指定外发的文件能否进行打印 |
| 文件备份管理 | 备份策略定义 | 1、定义哪些计算机需要将文件自动备份到服务器 2、定义哪些类型的文件需要备份 3、可以定义备份文件版本的自动升级 4、定义服务器备份位置 |
| | 备份数据查询 | 备份后的文件按计算机名进行分类存在，在服务器上可以按原来的目录结构进行查询，例如原来保存在客户端桌面的文件，在服务器上也相应生成“计算机名\桌面”这样的目录 |
| | 备份文件可定义自 | 备份到服务器上的文件，可以保留其原来的加密状态，也可以对文件进行自动解密，备份一份解密的数据在服务器中 |
| 系统维护 | 远程目录维护 | 可以在客户端对服务器安装目录维护，包括补丁包安装、数据库维护等 |
| | 离线安装 | 当客户机无法连接到局域网时，可使用离线安装包及离线授权号直接在离线的机器上进行安装 |
| | 容灾恢复 | 实现自动备份运行环境，服务器遭受破坏时，短时间内即可将运行环境恢复到新的服务器中 |

表 1.1

第二章 安装与卸载

2.1 机器码

恒隆文档加密软件所采取的加密技术，是根据每台机器各自的硬件信息，通过公司内部的定制而生成的唯一标识本台机器的一串数字码，我们称之为机器码。无锡恒隆科技有限公司（以下简称恒隆科技）所采取的机器码，是根据机器的网卡的物理地址（Physical Address）、硬盘（Hard Disk Drive）ID 号和中央处理器（CPU）ID 号，生成的一串 30 位的数字码。用户在安装恒隆加密系统的时候可以通过系统安装程序查看自己机器的机器码。如图 2.1。

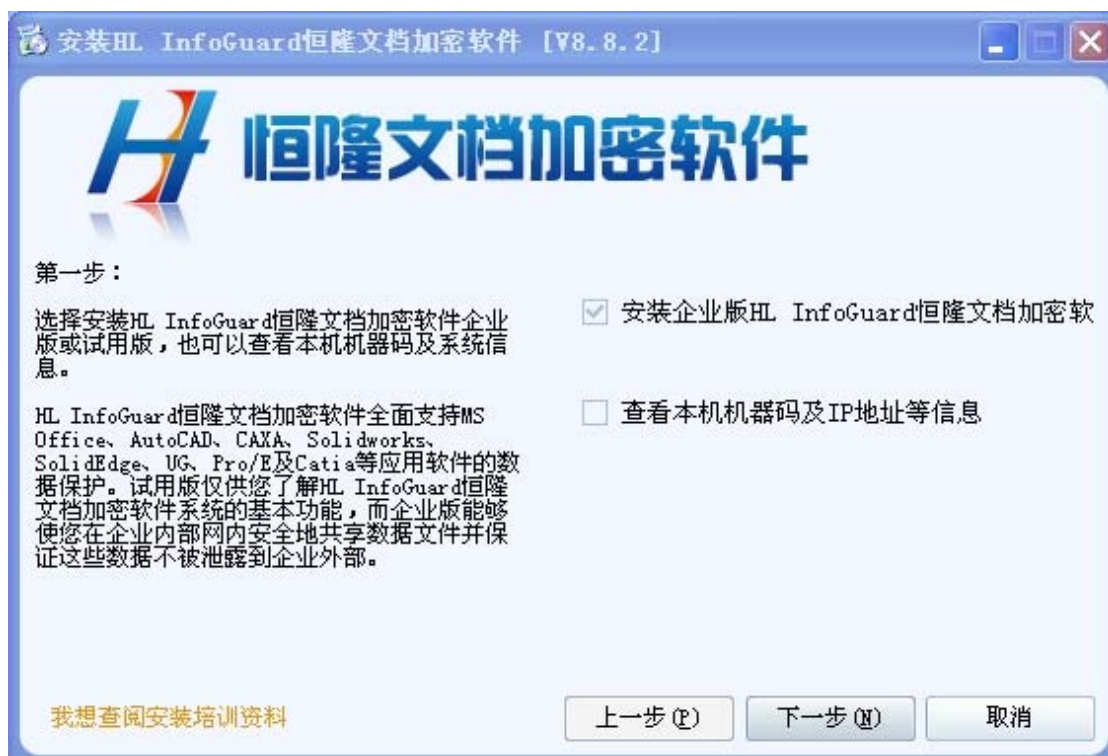


图 2.1

点击“下一步”，然后点击“详细信息”，可以查看到自己的机器码。如图 2.2 和图 2.3。



图 2.2

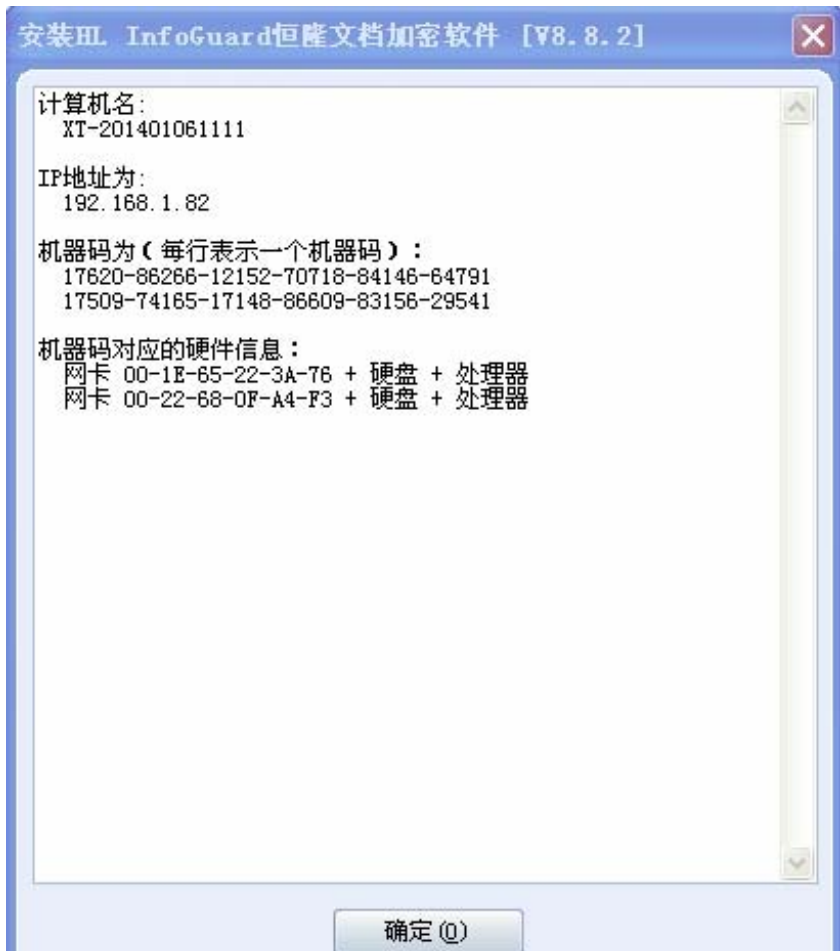


图 2.3

注意：由于不同的机器上可能安装有不同的应用程序（例如虚拟机），导致机器上可能会出现多块网卡，我们选择机器上最常用的那一块（我们正在使用的那一块网卡）。

2.2 服务端安装

本款软件可以运行的客户端版操作系统环境包括 WindowsXP (32位、64位)、WindowsVista (32 位、64 位)、Windows7 (32位、64位)、Windows8 (32位、64 位)，服务器版的操作环境系统包括 Windows Server 2003 (32 位、64 位) 和 WindowsServer 2008 (32 位、64 位)。我们在拿到恒隆文档加密软件的安装包之后，解压，打开文件夹，双击“setup.exe”，如果操作系统是Windows Vista (32 位、64位)、Windows7 (32位、64 位)、Windows8 (32 位、64 位) 或者Windows Server2003 (32位、64位)、WindowsServer 2008 (32位、64位)，则右击“setup.exe”，选择“以管理员身份运行”，会呈现出如图 2.1 的界面。我们选择“安装企业版恒隆文档加密软件”，点击“下一步”，选择“恒隆文档加密软件服务器”，再点击“下一步”，然后我们在文本框中输入我们想要安装系统所存放的路径，如图 2.4。

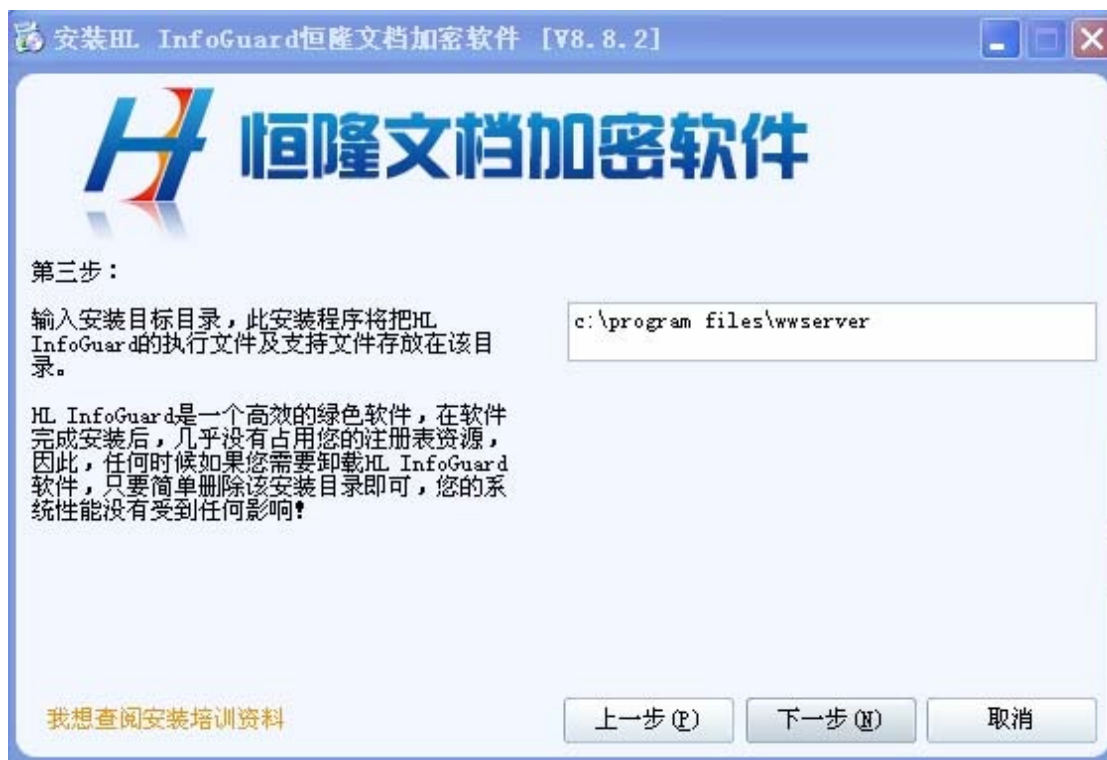


图 2.4

我们选择的是默认的路径，点击“下一步”，这个时候，我们就到了第四步，输入授权号，授权号是与客户的特定机器相关的，这种关系是通过我们在上面所说的机器码来体现。客户可以通过获取自己机器的机器码向恒隆科技申购正式授权号或申请试用授权号。我们在获取到授权号之后，将授权号输入到文本框中。如图 2.5。



图 2.5

然后点击“下一步”，准备将恒隆文档加密软件服务端安装到客户的机器上。点击“开始安装”后，进行加密系统的安装。如图 2.6。



图 2.6

然后，我们可以休息一会，等待着系统服务端的安装。在整个安装过程进行完成之后，会弹出如图 2.7 的界面，提示我们已经完成安装。点击“完成”，退出界面，此时整个服务端的安装完成。

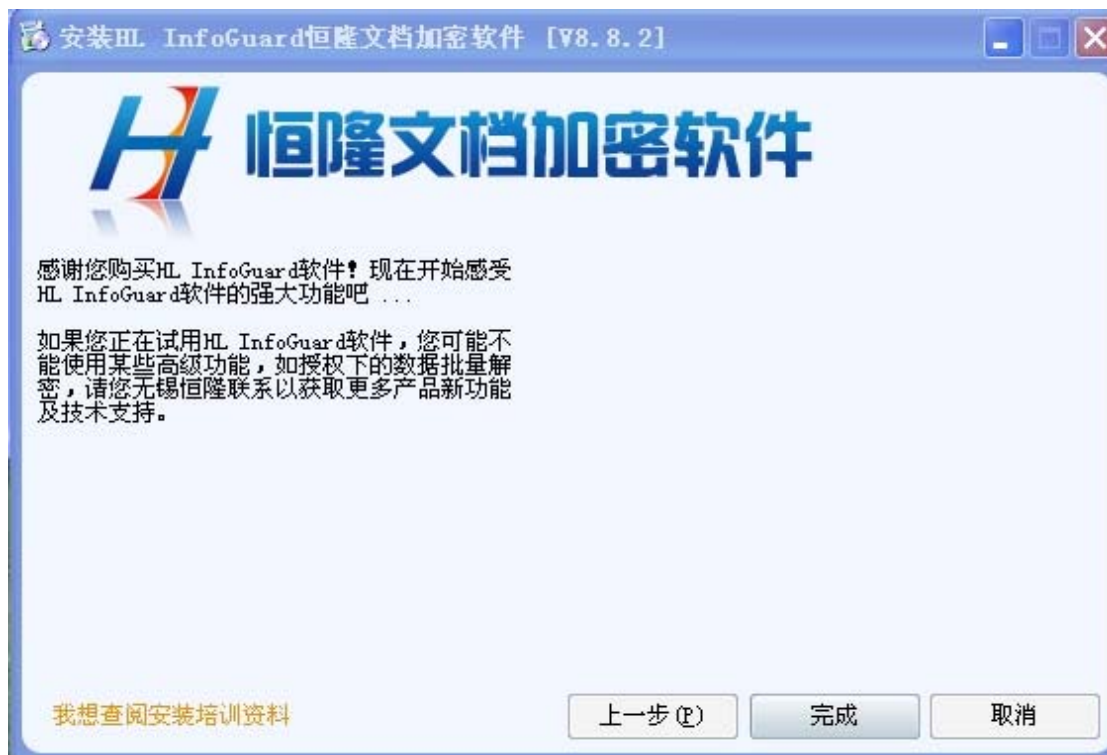


图 2.7

2.3 客户端安装

我们拿到恒隆文档加密软件的安装包之后，解压，打开文件夹，双击“setup.exe”，如果运行的操作系统是 Windows Vista（32 位、64 位）、Windows 7（32 位、64 位）、Windows 8（32 位、64 位），则右击“setup.exe”，选择“以管理员身份运行”，会呈现出如图 2.1 的界面。我们选择“安装企业版恒隆文档加密系统”，点击“下一步”，选择“恒隆文档加密软件客户端”，点击“下一步”，我们在文本框中输入我们想要安装系统所存放的路径，如图 2.8。



图 2.8

点击“下一步”，我们到了第四步，此时，我们要输入客户端的安装授权号。安装授权号由服务端的系统管理员生成，如果没有授权号，可以点击右边的“...”按钮来获取一个新的授权号。如图 2.9。



图 2.9

注意：获取授权号的时候，要输入服务器的 IP 地址或者计算机名，系统管理员和其设置的密码。（示例中服务端也安装在本机器上面，系统管理员为 adm，其设置的密码为空。）如图 2.10。



图 2.10

在点击“确定”后，会弹出如图 2.11 的对话框，分别在文本框输入机器码，授权用户的帐号和姓名，用户所属的密级，离线时最多能使用的天数，点击“确定”后，即可获得客户端的安装授权号。

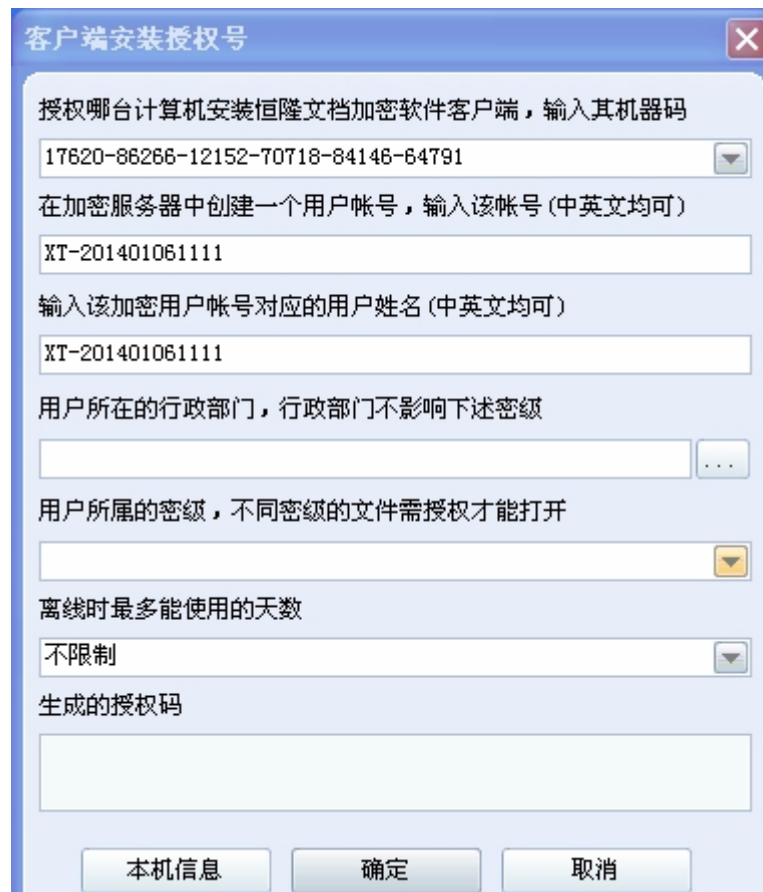


图 2.11

然后点击“下一步”，我们就开始准备将恒隆文档加密软件客户端安装到机器上。点击“开始安装”后，我们便进行加密系统的安装。如图 2.12。

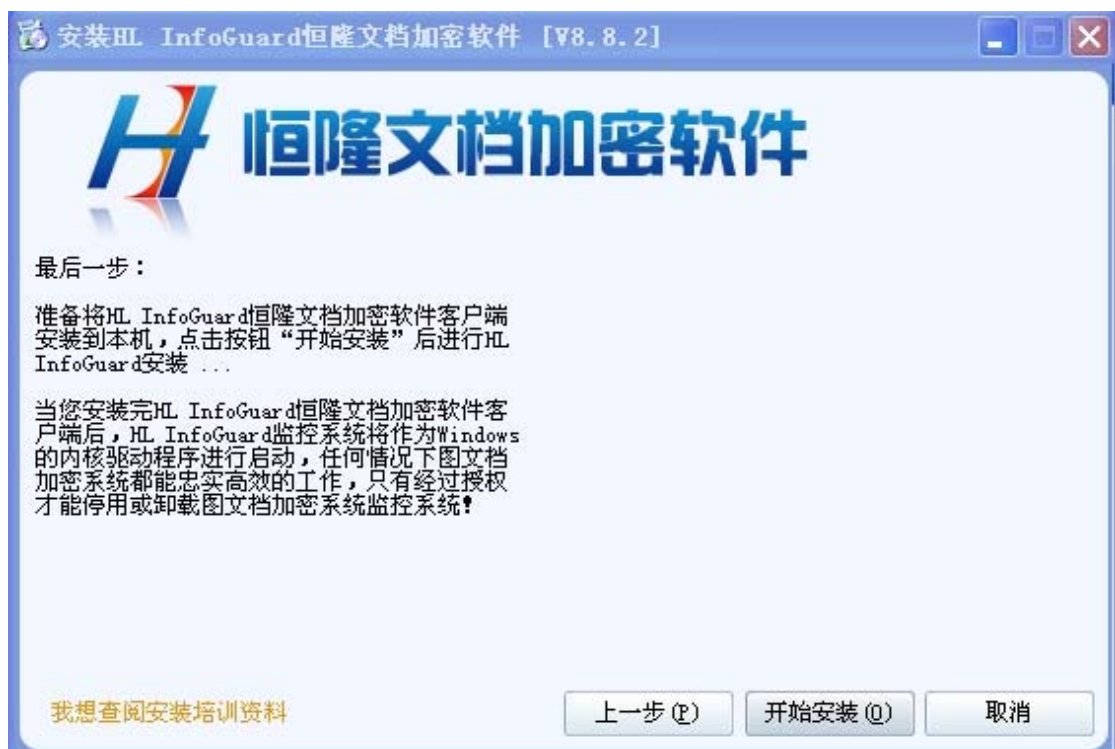


图 2.12

注意：在安装的时候可能会提示安装不成功，找到安装目录下的 wwall 文件夹，打开，找到wwhost.inf，右击安装，安装完成之后，重启机器，看到右下角的恒隆加密软件-Running，即表示客户端安装成功。

2.4 客户端卸载

在打开恒隆加密控制台之后，在菜单栏中显示有一个“卸载恒隆加密系统客户端”的图标，如图 2.13。点击进去，出现“登录恒隆加密服务器”的对话框，输入用户帐号、用户密码和服务地址，点击“OK”，成功连接到服务器之后，弹出一个“卸载客户端”的对话框，点击“确定”，弹出“卸载恒隆加密系统”的对话框，如图 2.14。点击“确定”，就可以开始对客户端的卸载。卸载完成后，弹出“成功卸载恒隆文档加密软件”。重启机器后，客户端就完全卸载掉。

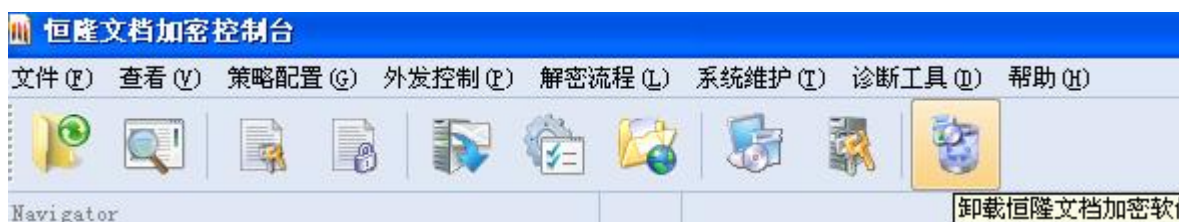


图 2.13

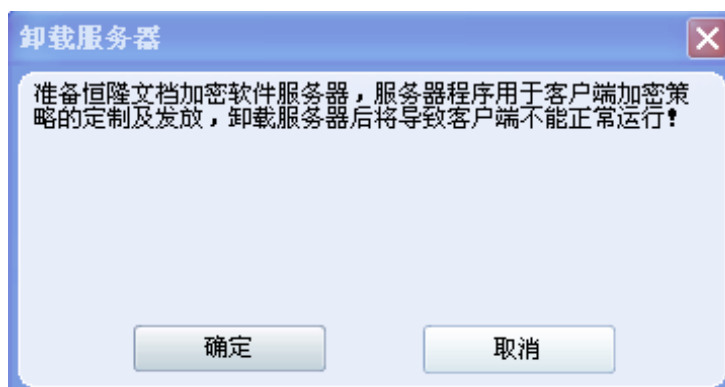


图 2.14

点击“远程卸载客户端”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务地址，点击“OK”，登录到服务端，弹出“远程卸载客户端”对话框，对话框下面有一个文本框和一些按钮，在文本框中输入所要查找的用户，点击“查找”，则会在原来树形列表中显示查到的部门和用户的用户帐号、用户名、类型以及查到的记录数量，如果没有记录，则显示“共找到 0 条记录”，点击“

切换”按钮，则会在查找记录和用户树形列表中切换显示。在“远程卸载客户端”对话框后，在树形列表中选择你要卸载的用户，然后点击“卸载选中用户”，就可以远程卸载选中的那个用户的客户端了。如图 2.15。



图 2.15

点击“生成卸载授权号”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“生成卸载客户端授权号”对话框，在“准备卸载哪台计算机上的恒隆加密系统”文本框中，输入我们想卸载的机器的机器码，点击右边的“...”按钮，弹出“选择用户”的对话框，选择用户后，点击“确定”后，就可以直接将所选的用户的机器码获取到文本框中，点击“确定”，就可以将系统生成的授权码显示到“生成的授权码”文本框中，我们可以将这个授权码保存下来。点击“使用授权号卸载”菜单之后，弹出“使用授权号卸载客户端”对话框，在“输入本机的卸载授权号”文本框中，输入上面生成的授权码，点击“确定”之后，便可以离线卸载客户端。如图 2.16。

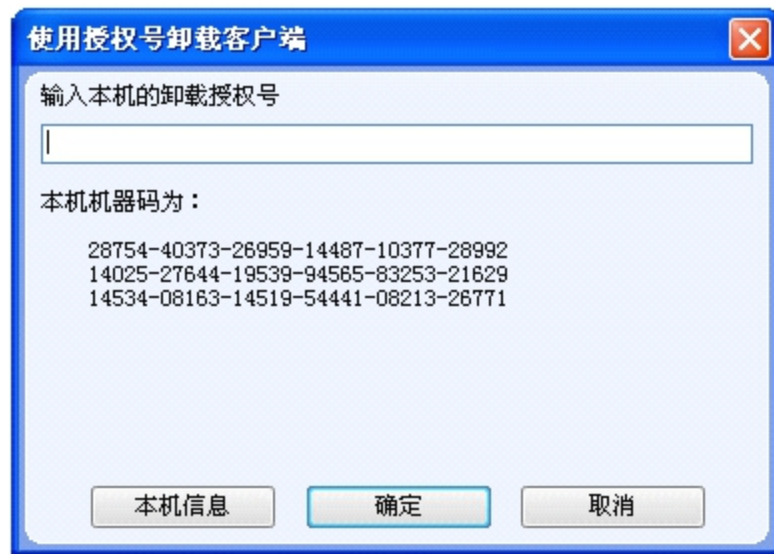


图 2.16

2.5 服务端卸载

在计算机上点击“开始”按钮，“运行”，文本框中输入“cmd”，点击“确定”按钮，进入到系统的控制台。在控制台中，输入命令，转到恒隆文档加密软件的安装目录下（例如 C:\Program Files\wwserver），然后输入 xdaemon /remove 命令，等到命令执行完毕之后，即可以卸载服务端。如图 2.17。

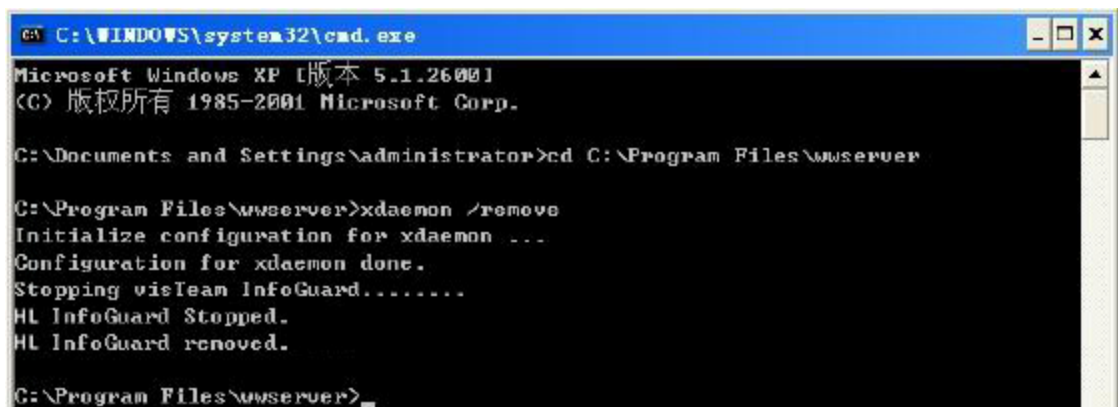


图 2.17

点击“卸载服务器”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“卸载服务器”的对话框，点击“确定”，就可以卸载服务器。如图 2.18。

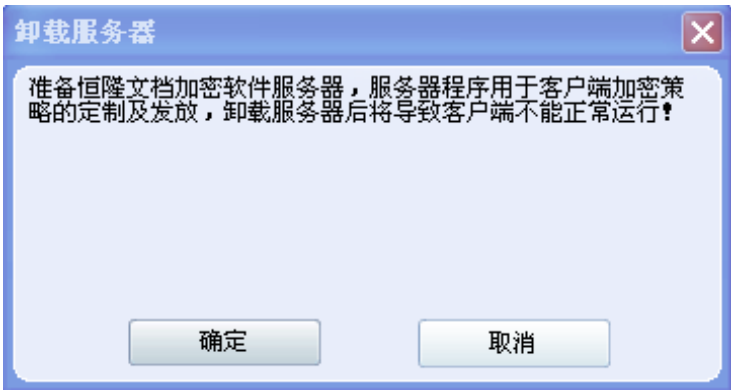


图 2.18

2.6 服务端及客户端升级

从 V7.0 以后，升级都可以在服务器完成，若从 V6.0 或更早版本升级到最新版本，则需要重新安装服务器，并重新卸载客户端及重新安装客户端。 本节讲述的是如果从 V7.0 或更新版本升级到当前最新的版本的基本步骤，从 V7.0 及更新版本升级，只需要升级服务器即可，服务器更新完成后，客户端会自动同步。

第 1 步：停止服务器后台服务

- 1、登陆加密软件服务器计算机，
- 2、“开始” — “控制面板” — “管理工具” — “服务”
- 3、在界面中找到“HL InfoGuard ”服务。

如下图：

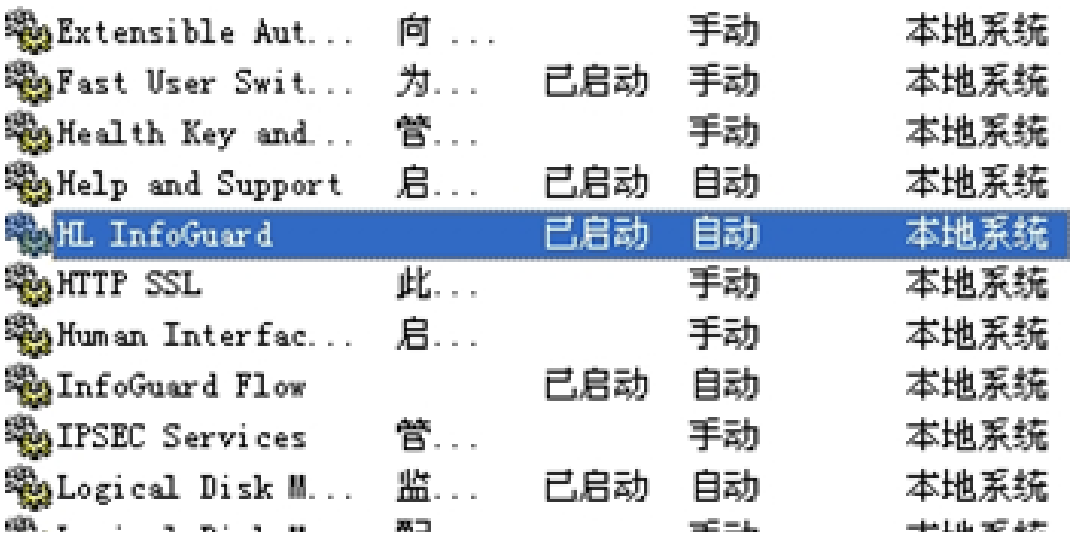


图 2.19

- 5、在“服务”的属性菜单中，可以找到服务端的安装路径。如下图

| | | | | |
|-------------------|-------|-----|-----|------|
| Extensible Aut... | 向 ... | | 手动 | 本地系统 |
| Fast User Swit... | 为... | 已启动 | 手动 | 本地系统 |
| Health Key and... | 管... | | 手动 | 本地系统 |
| Help and Support | 启... | 已启动 | 自动 | 本地系统 |
| HL InfoGuard | | 已启动 | 自动 | 本地系统 |
| HTTP SSL | 此... | | 手动 | 本地系统 |
| Human Interfac... | 启... | | 手动 | 本地系统 |
| InfoGuard Flow | | 已启动 | 自动 | 本地系统 |
| IPSEC Services | 管... | | 手动 | 本地系统 |
| Logical Disk M... | 监... | 已启动 | 自动 | 本地系统 |
| ... | ... | ... | ... | ... |

图 2.20

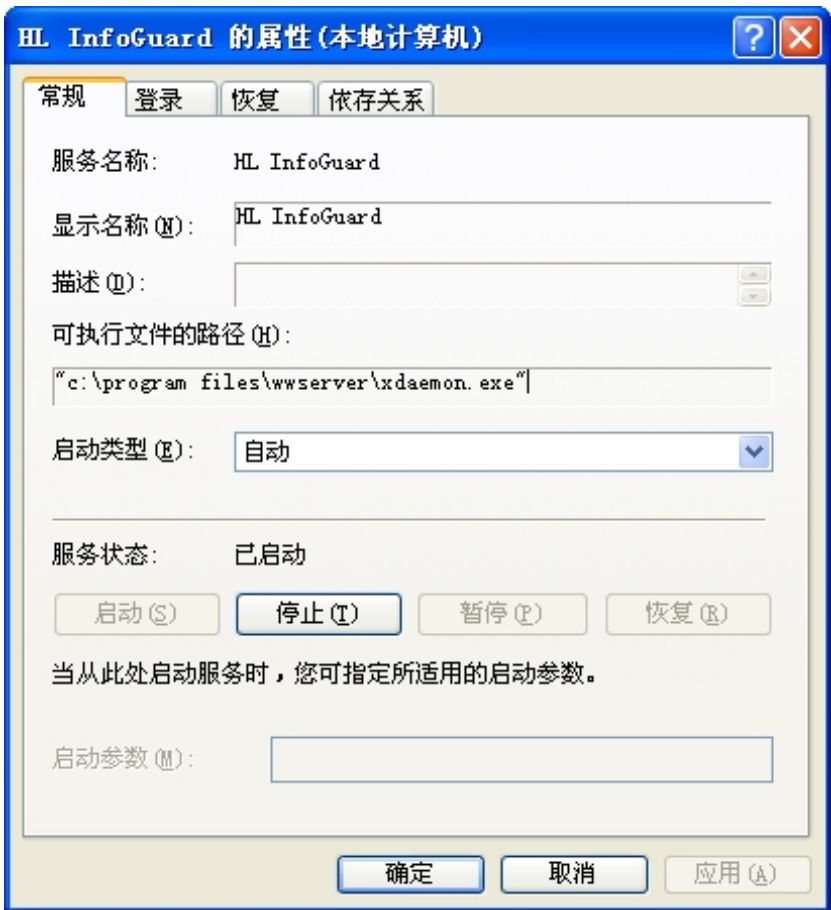


图 2.21

第 2 步：备份原服务端的文件

- 1、找到并打开原服务端的安装路径（一般是 Program Files\wwserver）；
- 2、先备份原服务端安装程序文件夹，例如备份成 backup\wwserver 目录。

第 3 步：解压最新的安装包并覆盖原服务端的文件

- 1、下载最新安装包，并解压得到最新的 setup 目录；
- 2、打开 setup\wwsetup\wwall 目录，选中该目录下所有文件及文件夹，复制粘贴到原服务端安装路径文件夹中（一般是 Program Files\wwserver）；

第 4 步：还原授权文件、数据库文件、连接文件

- 1、打开备份目录（上述说的 backup\wwserver 目录），将以下文件逐个还原到服务端 wwserver 安装目录：

- xsvrcnt.xcf（加密服务器授权文件）
- xsvrodbc.xcf（加密服务器数据连接配置文件）
- wwkrm.xcf（加密服务器加密策略文件）
- wwmail.xcf（加密服务器邮件白名单）
- xsvrlics.xcf（服务器模块授权，如外发控制）
- 整个 xvtdata 目录（数据库目录）
- xsvrcnt.xcf（解密流程授权文件）
- xsvrodbc.xcf（解密流程数据连接配置文件）
- wwflwlgn.xcf（解密流程数据连接地址配置）

- 2、打开还原好的服务端 wwserver 安装目录，逐个检查以下文件，若曾经改过这些文件，则需要手工再改一次：

- wwshell.xcf（右键菜单显示定义）
- xsvrini.xcf（服务器初始化文件）

第 5 步：重新启动服务，并根据最新安装包中的 **readme.txt** 指导完成最后更新

- 1、找到“HL InfoGuard”服务，并启动服务，如下图：



图 2.22

2、打开最新安装包解压后的 setup 目录，打开 readme.txt 文件，将滚动条拉到最后，并依次向前查看是否需要更新一些内容，主要的更新为 SQL 语句，即新版本的数据库结构可能有所变化；

3、刷新服务。启动“恒隆加密控制台”，点击“刷新服务器”按钮，如下图：



图 2.23



图 2.24

第 6 步：测试升级是否完成

- 1、找一台客户端重启一下，到 Windows 登陆界面时，等待 3 分钟左右再输入密码进行登陆 Windows；
- 2、启动客户端的“恒隆加密控制台”，点“帮助 -> 关于”，看看两个更新版本是否相同：

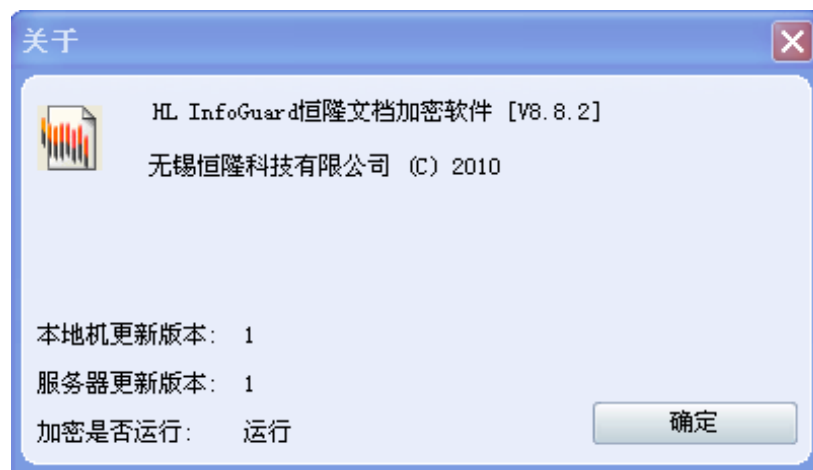
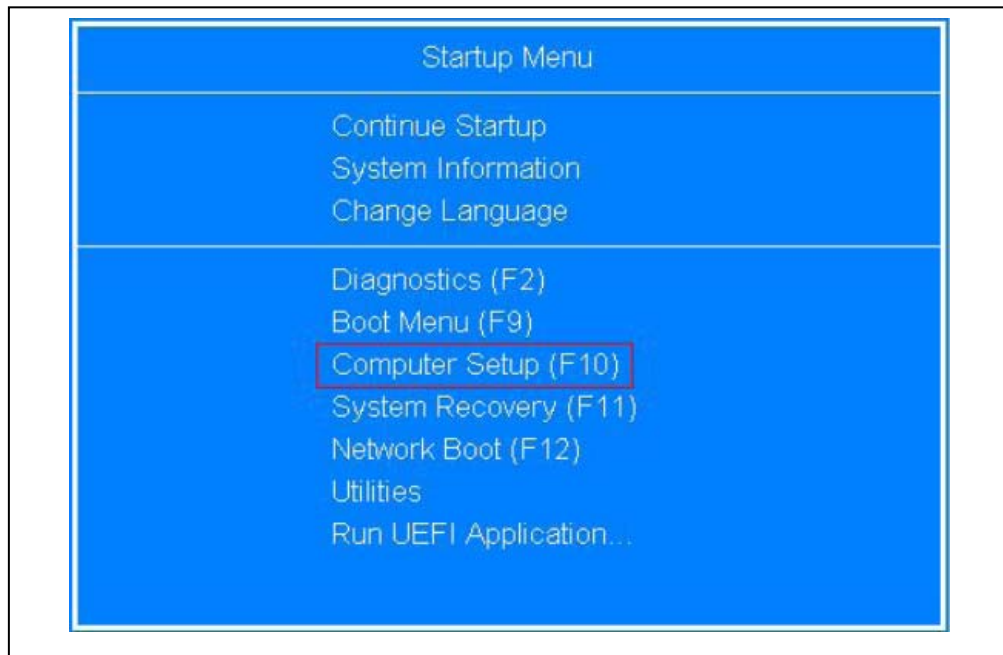


图 2.25

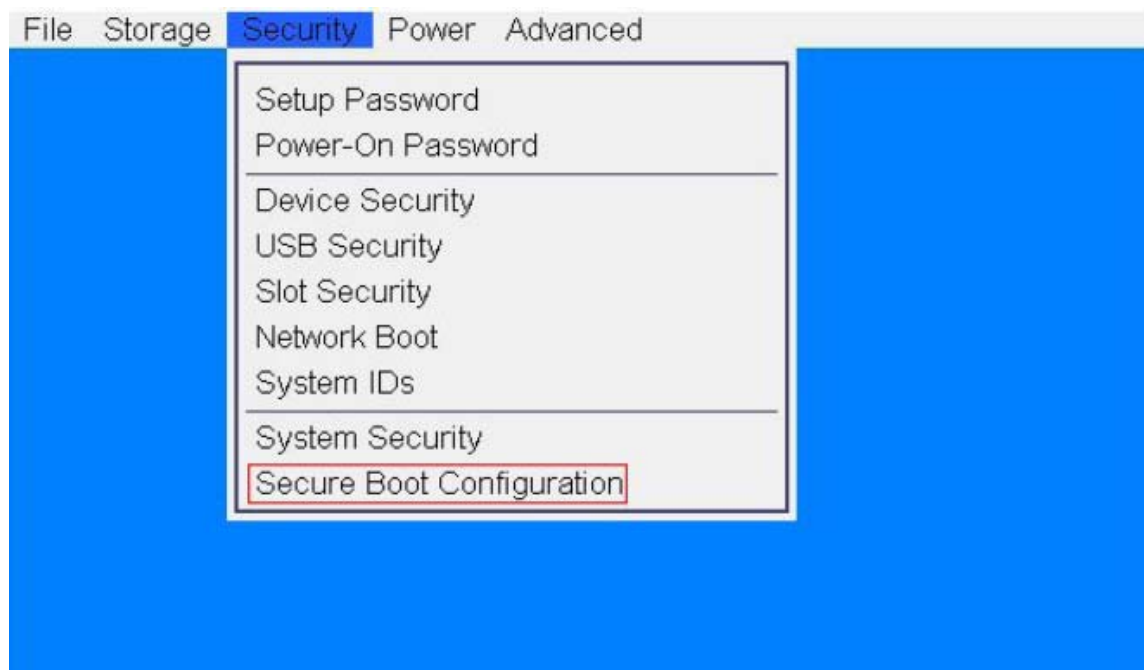
2.6 win8 64位系统配置

在Windows 8 的64 位系统中（少量Windows 7 的64 位系统），若安装过程出现提示“配置64位计算机BIOS认证加密驱动”，”，则按以下步骤设置BIOS 后再安装。

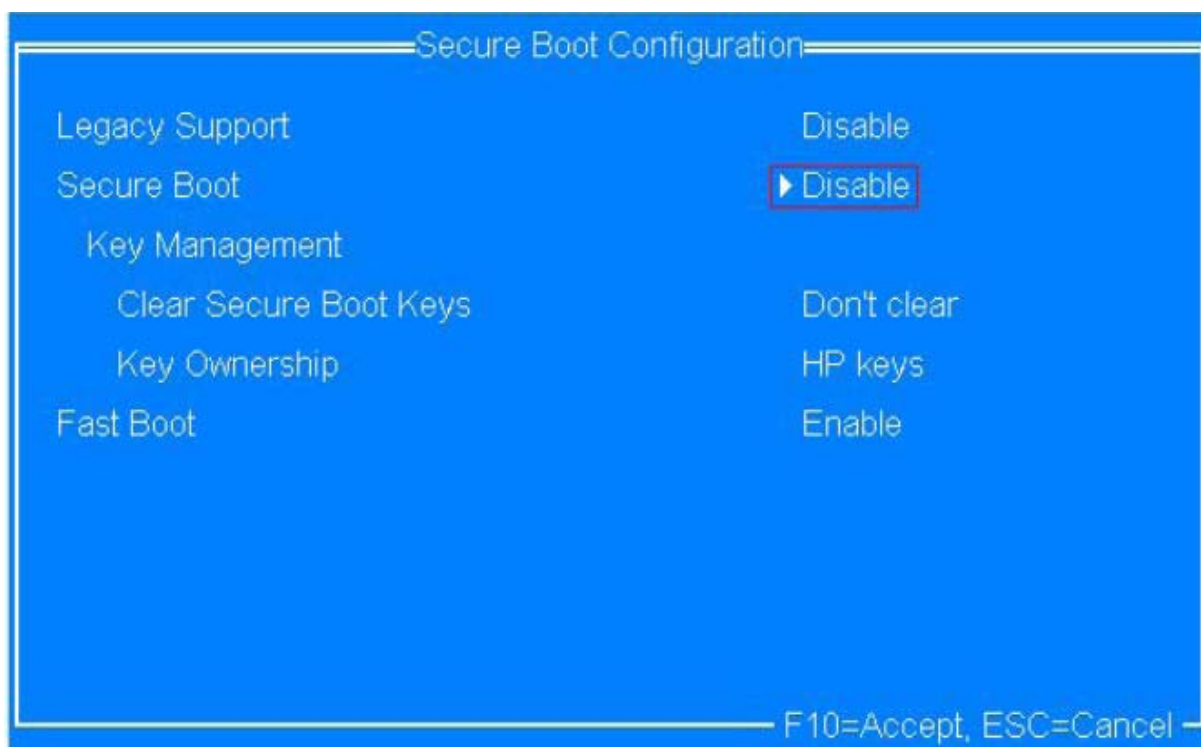
第一步：关机重启计算机，一直按着ESC（或F8）进入BIOS 设置界面（不同品牌的计算机不一样，但大同小异，以下是惠普PC 机的拍照截图）：



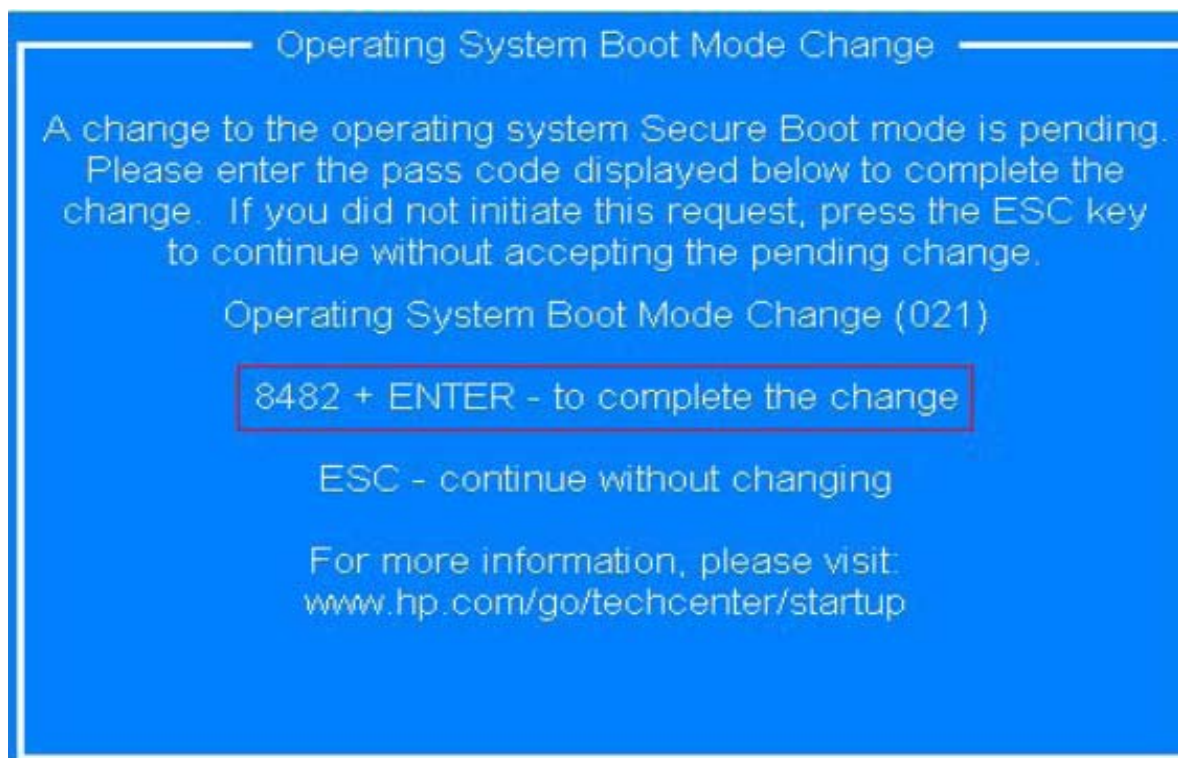
第二步：进入BIOS 设置界面，点击如下图菜单（不同品牌的计算机不一样，但大同小异，以下是惠普PC 机的拍照截图）：



第三步：进入BIOS 设置界面后，将“Secure Boot”改为“Disable”（不同品牌的计算机不一样，但大同小异，以下是惠普PC 机的拍照截图）：



第四步：设置好上述BIOS 项后，重启计算机，有些品牌的计算机会提示输入一个验证码再次确认，重启后安装加密软件即可（不同品牌的计算机不一样，但大同小异，以下是惠普PC 机的拍照截图）：



第三章 定义加密策略配置

3.1 服务器加密策略

在计算机上点击“开始”按钮，选择“恒隆加密系统”，点击“加密控制台”，如图 3.1。



图 3.1

进入到“恒隆加密控制台”中，在菜单栏中“策略配置”中选择“服务器加密策略”选项，如图 3.2。

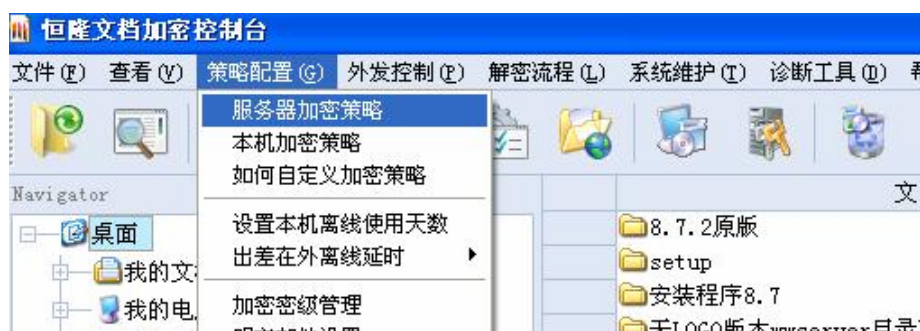


图 3.2

进入到“定义服务器加密策略”中，如图 3.3。在对话框中，我们可以看到本服务器已经包含的一些加密策略，如系统设置、图片（Pictures）、软件（Softwares）、办公软件（Offices）等等一些系统中的主加密策略，我们可以对其中的一些加密策略进行配置。例如勾选“禁止屏幕截屏录制”，保存后，服务端就实现了“禁止屏幕截屏录制”这一策略。另外，除开树形图所包含的这些解密策略之外，我们还可以自己定义一些加密策略，来管理我们机器上面的与之对应的应用程序。对话框右边有一些操作的按钮：“增加应用程序”，表示我们可以增加一些应用程序到加密策略

中，进行加密管理；“增加子程序”，表示我们可以增加子程序到指定的应用程序中；“修改应用程序”，表示我们可以修改应用程序名、分类、文件类型等等；“增加加密策略”，表示我们可以增加一些加密策略；“添加用户”指存在子加密策略时，可以对子加密策略进行添加用户（不同的用户对应的加密策略不同）；“删除选中节点”，表示我们可以删除那些我们想要删除的节点；“保存”，表示我们可以保存自己设置的策略；“关闭”，表示关闭这个对话框。



图 3.3

在图 3.3 所示的“定义服务器加密策略”对话框中，点击右边的“增加应用程序”按钮，弹出“增加应用程序”对话框，就可以增加一个应用程序。我们来做个示例，我们打开画图工具。在“开始”，“所有程序”，“附件”，点击“画图”，打开画图工具。当我们不知道画图所对应的应用程序时，我们可以打开“任务管理器”，选到那个我们要查看的任务，右键“转到进程”，单击，就可以查看到所对应的

程序。我们可以看到“画图”所对应的应用程序是“mspaint.exe”。在“应用程序执行文件”文本框中，输入“mspaint.exe”，“应用程序名”中输入“画图”，这个只是作为在系统面板上显示的作用，“应用程序分类”中，可以选择输入主加密策略中已经定义的类别，也可以输入我们自己定义的一些类，还可以不输入（增加应用程序成功后显示为“其他”）。在“文件后缀名列表”中，输入我们想加密的文件类型，例如“jpg, bmp, gif”等。下面有两个选项，勾选“仅加密上述指定类型的文件”，就表示只加密刚刚输入的那些类型的文件，不勾选，则表示可以加密所有类型的文件；勾选“遍历文件时减去加密头大小”，就表示在遍历文件的时候会减去一个加密头所占的空间。如图 3.4。

注意：“应用程序执行文件”文本框，“应用程序名”文本框和“文件后缀名列表”文本框里面必须填写内容，否则，会弹出“数据输入不合法”。

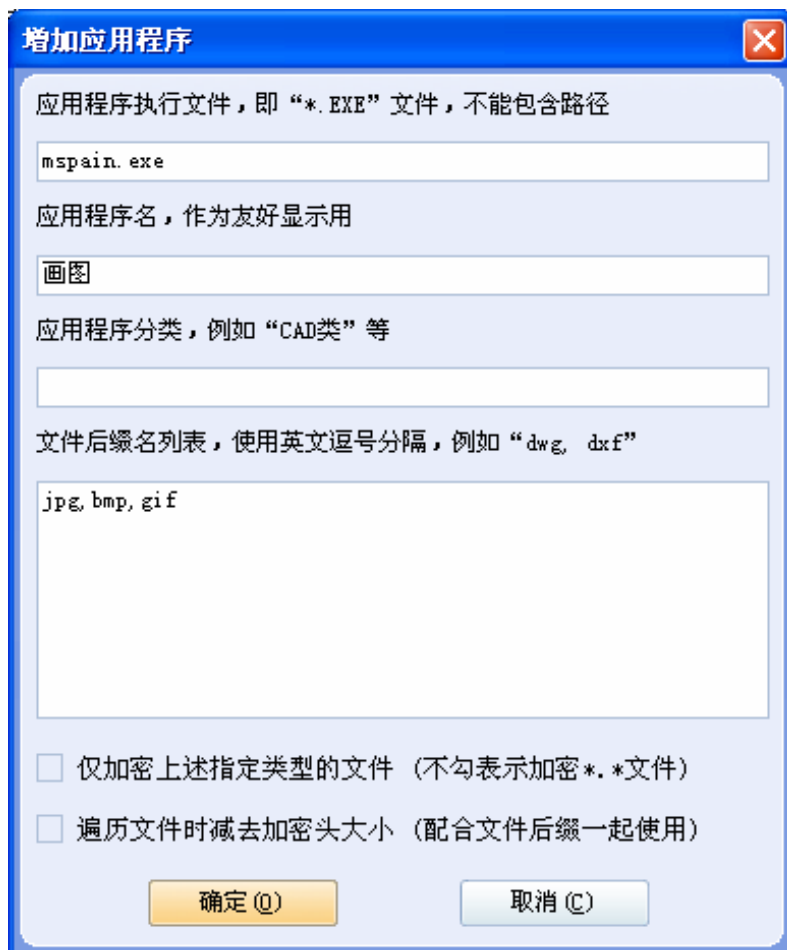


图 3.4

在每一个加密策略类别下面的应用程序下，我们展开可以看到四个功能：“保存文件时加密”，表示我们在保存文件的时候就对文件进行加密；“允许打开加密文件”，表示我们有权限打开一个加密的文件；“自动备份归档”，表示我们可以自动的将我们的文件归档到服务端的电子仓库里进行备份；“关闭打印功能”，表示我们不能打

印这个文件。如图 3.5。可以根据不同的需求进行不同的配置不同的功能。

另外，我们还可以在我们上面建立的那个应用程序中增加子进程，在配置完成之后，点击“保存”，“关闭”按钮。

在每一个加密策略类别下面的应用程序下，我们展开可以看到四个功能：“保存文件时加密”，表示我们在保存文件的时候就对文件进行加密；“允许打开加密文件”，表示我们有权限打开一个加密的文件；“自动备份归档”，表示我们可以自动的将我们的文件归档到服务端的电子仓库里进行备份；“关闭打印功能”，表示我们不能打印这个文件。如图 3.5。可以根据不同的需求进行不同的配置不同的功能。

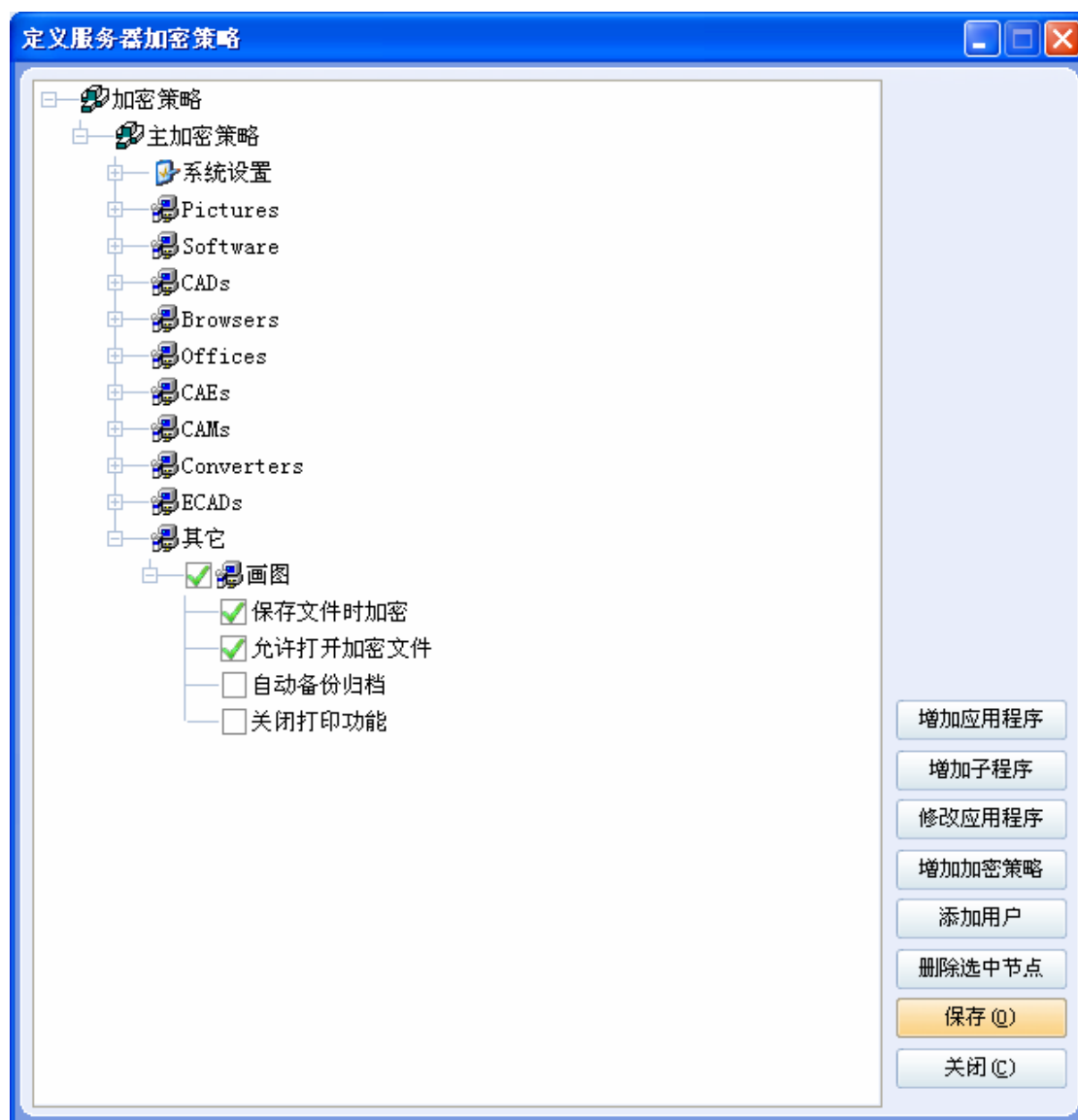


图 3.5

另外，我们还可以在我们上述建立的那个应用程序中增加子程序，点击右边的“增加子程序”按钮，弹出“增加子程序”对话框，我们可以在其中增加子程序，同样我们可以使用任务管理器查看所要执行的程序在计算机中所对应的应用程序名

称（例如我们所用的 Microsoft Visual C++ 6.0 的名称是“MSDEV.EXE”）。我们先按照上述操作，将这个程序加入到加密策略中，然后选中“画图”，点击“增加子程序”，将这个“msdev.exe”加入进去使其成为子应用程序，点击“确定，”如图 3.6。

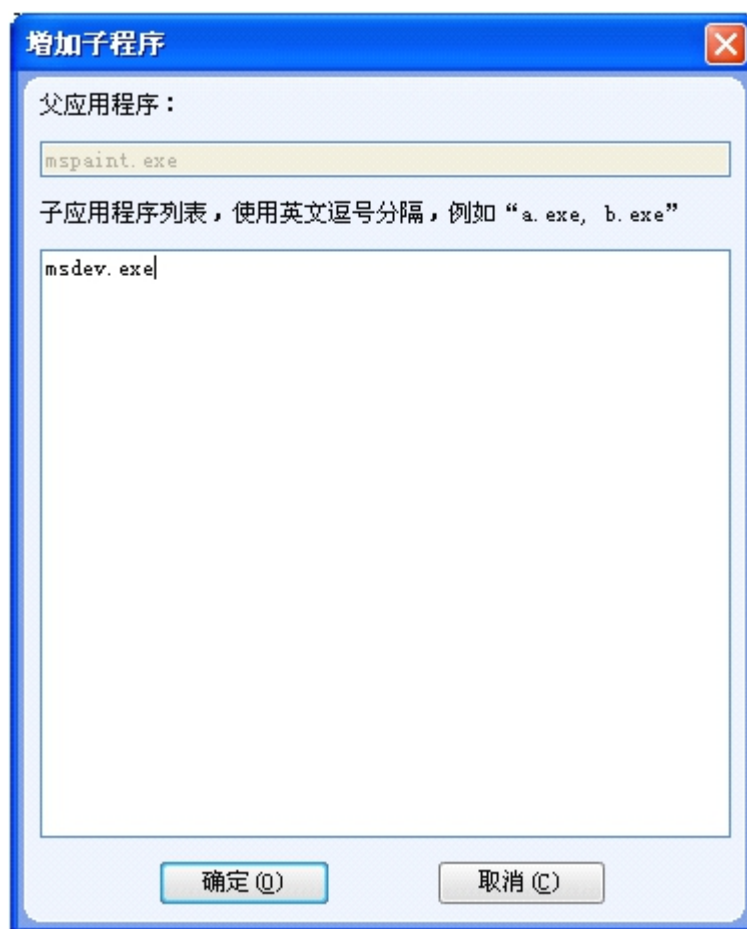


图 3.6

这样 VC++ 6.0 就成为画图程序的子程序。在配置完成之后，点击“保存”，“关闭”按钮。这样我们新增了一个新的加密策略。如图 3.7。完成之后，点击菜单栏的“策略配置”，选择“手动更新本机加密策略”，点击，就能将服务端的策略配置更新，并且派发到连接到本服务端的客户端上面。

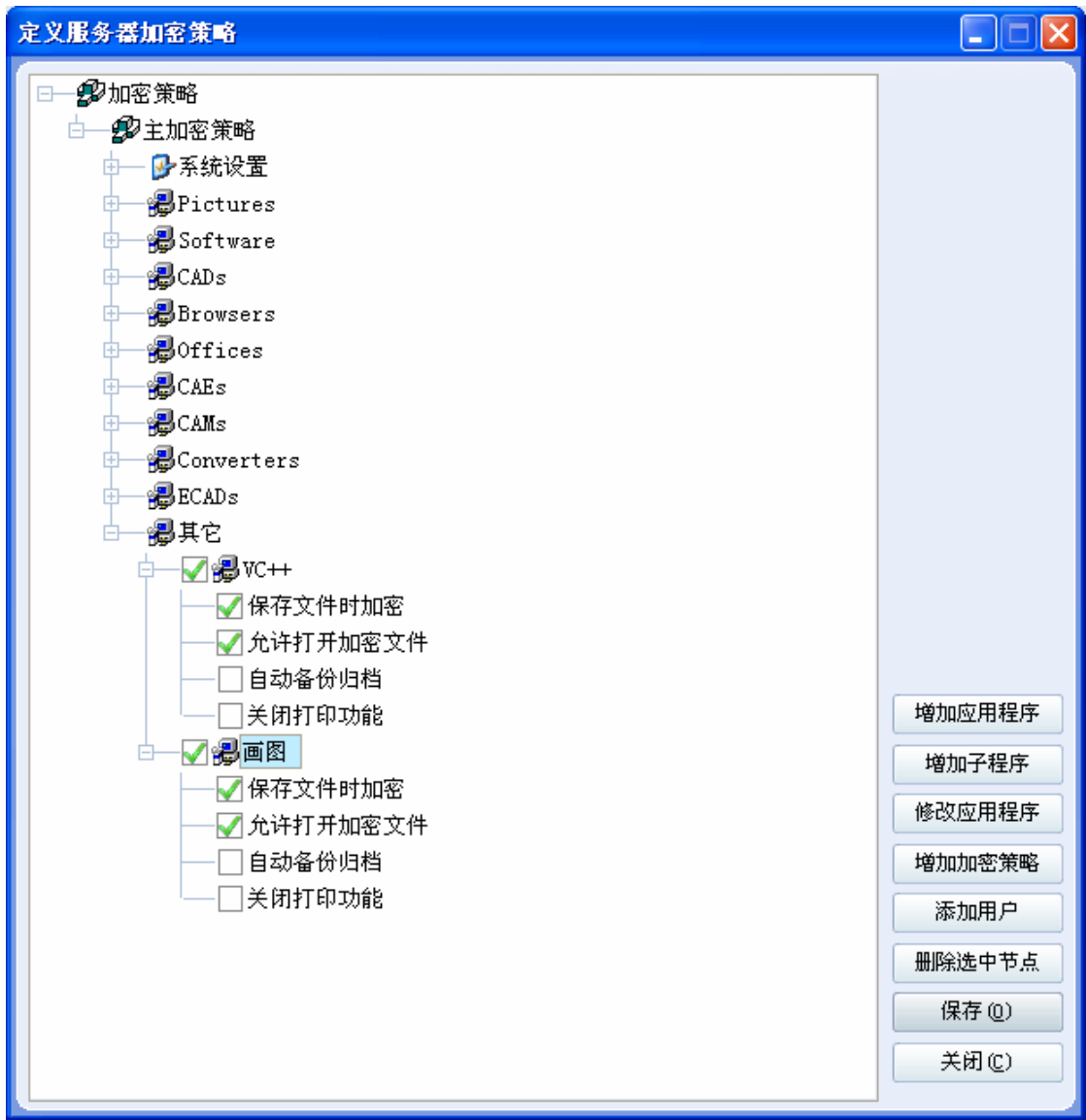


图 3.7

3.2 本机加密策略

点击“本机加密策略”菜单之后，可以查看到由服务端派发下来的加密策略里面所包含的策略内容。如图 3.8。

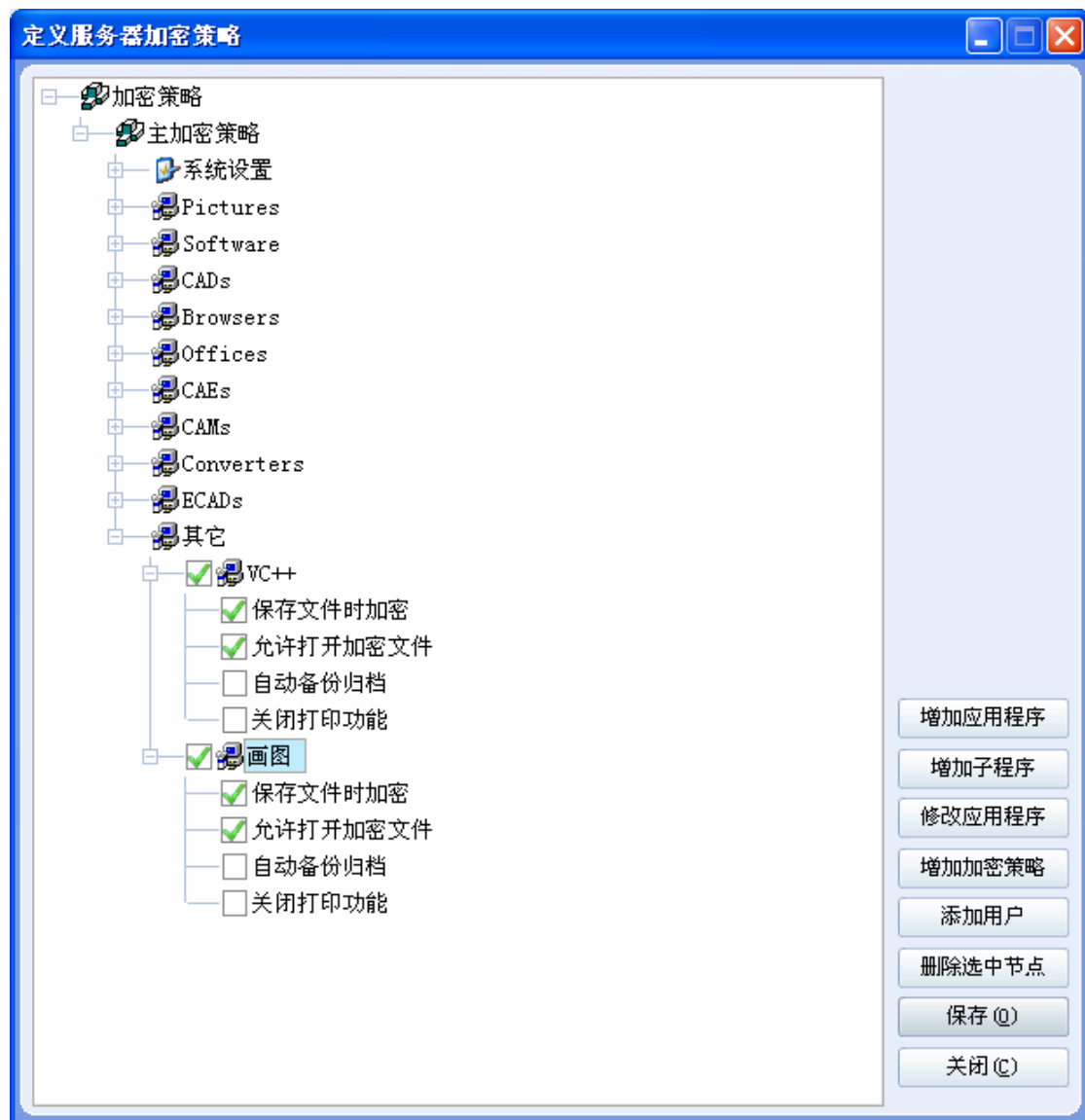


图 3.8

3.3 如何自定义加密策略

点击“如何自定义加密策略”菜单之后，会播放自定义加密策略的培训视频。

3.4 设置本机离线使用天数

点击“设置本机离线使用天数”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务地址，点击“OK”，登录到服务端，弹出“本机加密授权属性”的对话框，在“离线时最多能使用的天数”的文本框，选择或输入我们所选择的天数或者不限制或者必须在线，就可以设置最多能使用的天数。如图 3.9。



图 3.9

3.5 出差在外离线延时

点击“出差在外离线延时”菜单之后，会有一个二级菜单。

点击“创建离线延时授权号”菜单之后，会弹出“创建离线激活授权号”对话框，在“准备激活哪台计算机上的加密系统，输入其机器码”文本框中，输入选择输入的机器码，或者点击右边的“...”按钮，弹出“选择用户”的对话框，选择用户后，点击“确定”后，就可以直接将所选的用户的机器码获取到文本框中，在“延时多少天”文本框中，输入我们需要延时的天数，点击“确定”按钮之后，就可以生成一个离线延时授权码，显示到“生成的授权码”文本框里面。如图 3.10。

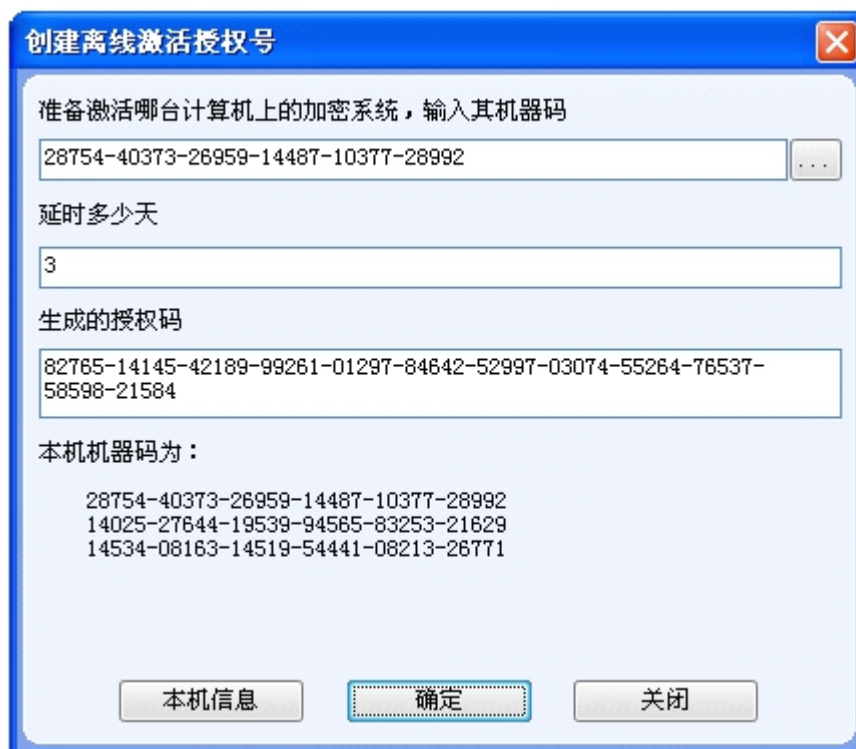


图 3.10

点击“查看离线使用剩余天数”菜单之后，会弹出“使用离线激活授权号”对话框，在“输入离线激活授权号”文本框，输入离线延时授权码，点击“确定”后，就可以查看离线使用剩余天数。如图 3.11。

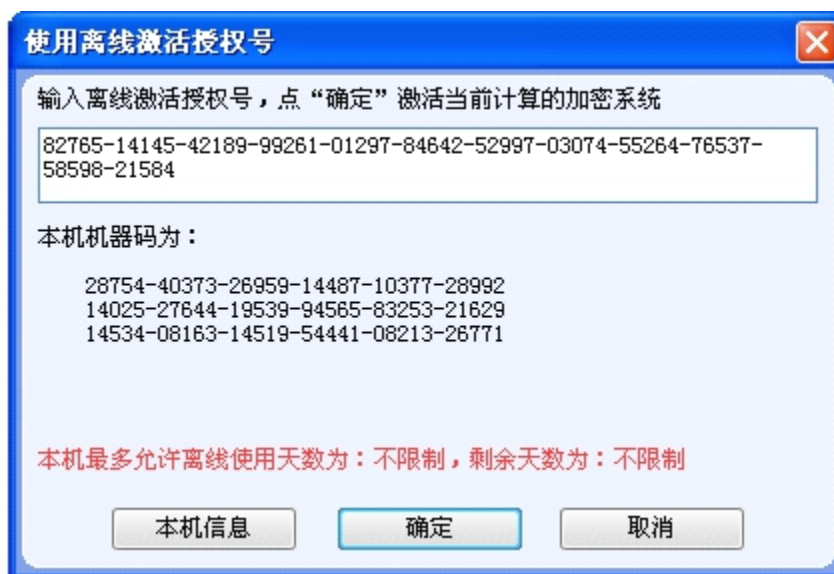


图 3.11

点击“使用离线延时授权号”菜单之后，会弹出“使用离线激活授权号”对话框，在“输入离线激活授权号”文本框，输入离线延时授权码，点击“确定”后，就可以离线延时授权号。如图 3.12。

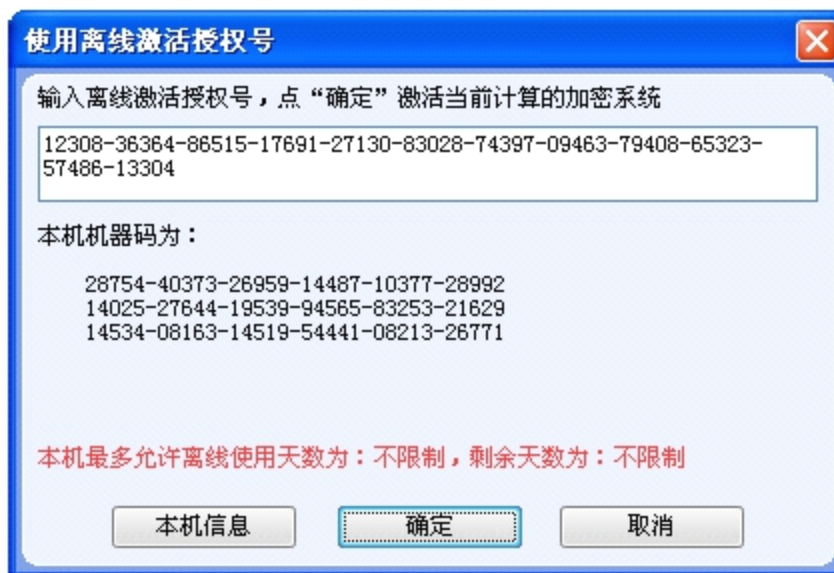


图 3.12

点击“手工连接服务器以延时”菜单之后，会弹出“连接到服务器以激活加密”对话框，在“服务器地址”文本框，输入服务器的 IP 地址，或选择“连接恒隆科技服务器激活”（需要从恒隆申请帐号密码），点击“确定”之后，就可以连接到客户安装的服务端或者恒隆科技服务器来激活加密。如图 3.13。



图 3.13

3.6 加密密级管理

点击“加密密级管理”菜单之后，弹出“加密密级管理”对话框，对话框左边是密级的列表，右边是密级的详细信息，包括密级内码（自动产生）、密级代码、密级名称、能打开哪些密级的文件、属于该密级的用户列表。左下边是“点击这里查阅如何定义密级”，点击可以查看定义加密密级的帮助视频。右下边是一些按钮，点击“新建密级”之后，我们可以新建一个密级；选中密级，点击“删除密级”之后，我们可以删除选中的密级；点击“加入用户”之后，会弹出“选择用户”的对话框，可以从中选择一个用户，点击“确定”后，将选择的用户加入到设置的密级中；选中用户，点击“移去用户”之后，我们将选中的用户从密级中移去；点击“刷新”，可以刷新密级和用户；点击“保存”，我们可以保存设置的密级；点击“关闭”，则关闭对话框。如图 3.14。

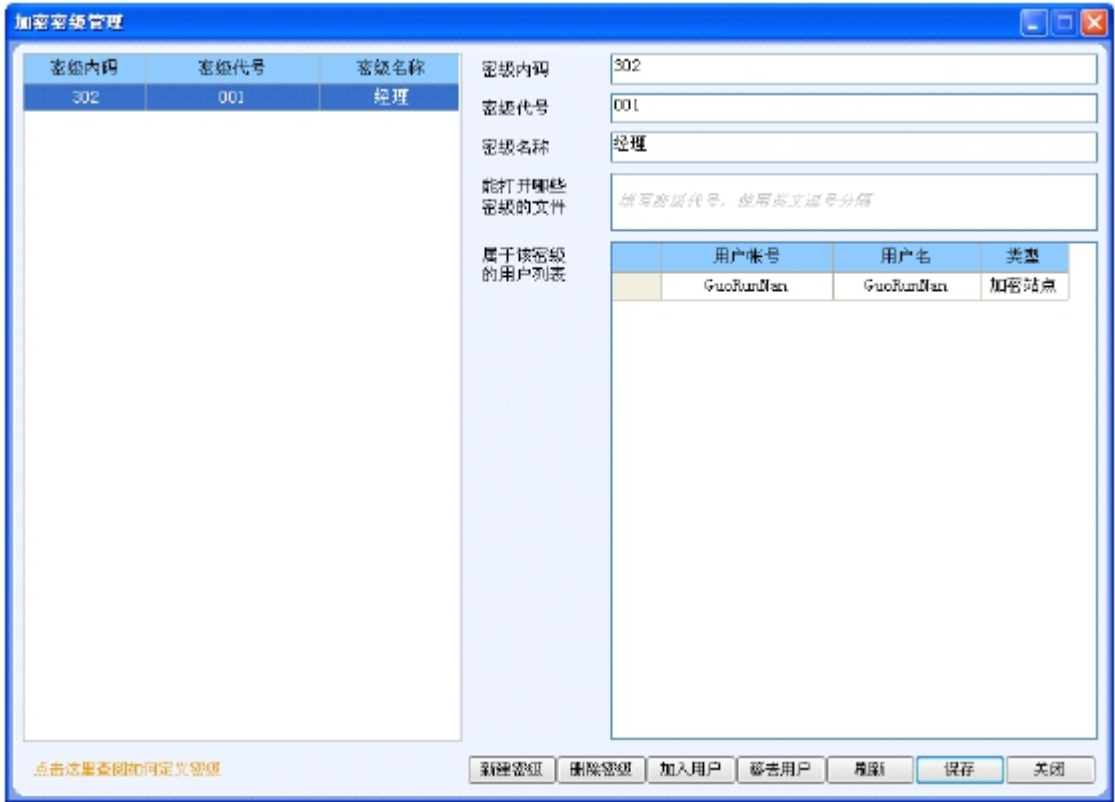


图 3.14

3.7 禁用或只读 U 盘

点击“禁用或只读 U 盘”菜单之后，会弹出“定义服务器加密策略”对话框，并自动选中“U 盘或移动硬盘状态：完全开放（双击修改）”，双击词选项之后，会弹出“禁用或只读 U 盘、移动硬盘”，下面的单选框中选择“U 盘或移动硬盘状态：完全开放”、“U 盘或移动硬盘状态：只读”、“U 盘或移动硬盘状态：禁用”，可以选择其中的一个状态，来设置移动存储设备的状态：完全开放、只读、禁用。如图 3.15。

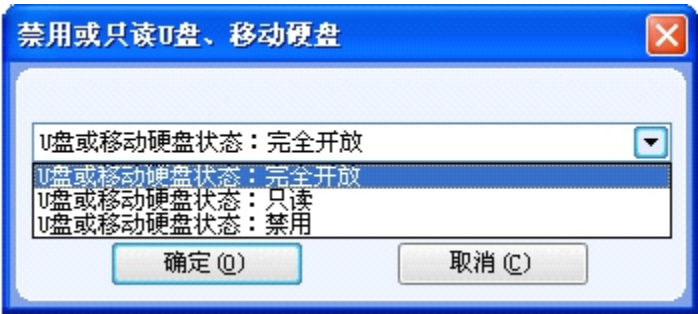


图 3.15

3.8 显示加密锁标记

点击“显示加密锁标记”菜单之后，会弹出“显示加密锁”对话框，在“显示加密锁”的单选框中，可以选择“显示”和“不显示”两个选项，选择之后，点击“确定”，就可以选择加密是否显示。如图 3.16。

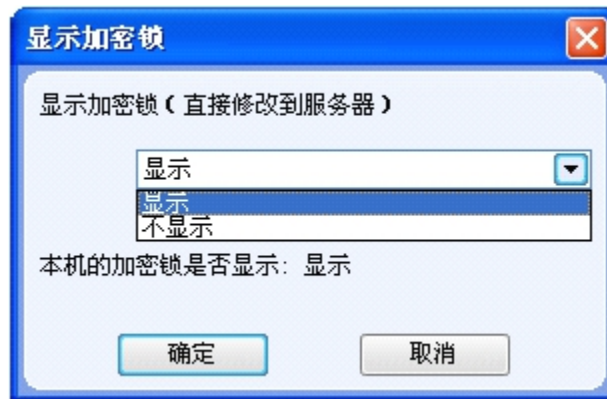


图 3.16

3.9 设置少量文本拷贝

点击“设置少量文本拷贝”菜单之后，会弹出“设置少量文本复制粘贴”，在“允许拷贝少量文本”文本框中输入我们允许拷贝的文本字符，为空表示禁止，点击“确定”，我们就可以设置允许拷贝文本的字符数。如图 3.17。

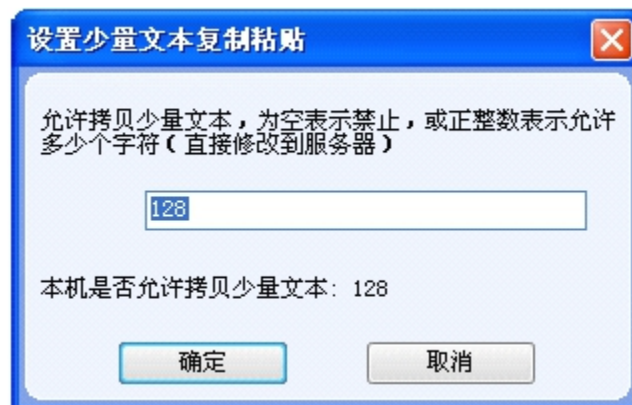


图 3.17

3.10 设置程序定向拷贝

点击“设置程序定向拷贝”菜单之后，会弹出“设置程序定向复制粘贴”对话框，我们只能修改服务器的配置，不能修改客户端本机的配置。下面有个列表，显示的是“加密受控的程序”、“允许定向拷贝的程序”、“拷贝类型”。点击“增

加一行”，会弹出“增加定向复制粘贴程序”对话框，我们可以增加一行的定向复制粘贴程序。在“增加定向复制粘贴程序”对话框中，我们在“定向复制粘贴的源程序”文本框中输入源程序或者点击右边的“任何程序”，可以设置为我们输入的源程序或者所有的程序；在“允许定向复制粘贴到哪个目标程序”文本框中输入源程序或者点击右边的“任何程序”，可以设置为我们输入的目标程序或者所有的程序；在“定向复制粘贴内容的类型”单选框中，可以选择“仅拷贝文本”和“拷贝任何数据”，就选择复制粘贴内容的类型。点击“确定”后可以保存这个设置。如图 3.18。这样在“设置程序定向复制粘贴”对话框中就增加了一行我们设置的配置。如图 3.19。选中这个配置后，点击“删除一行”，可以删除这个配置。点击“保存”，我们可以保存这个配置。点击“关闭”之后，关闭对话框。

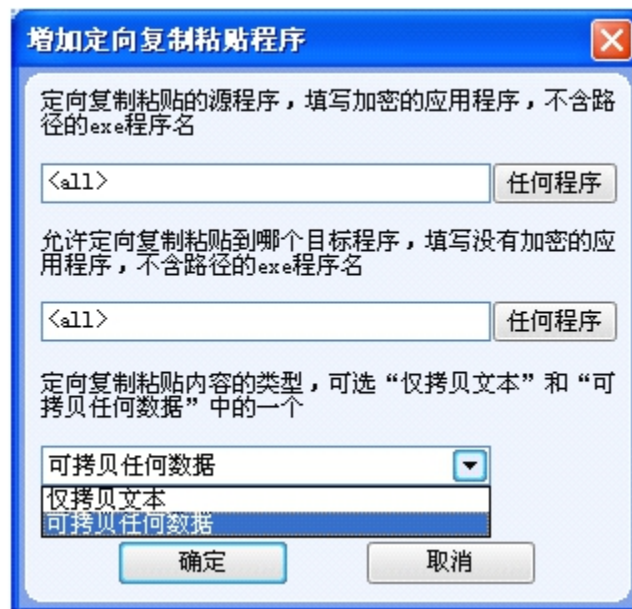


图 3.18

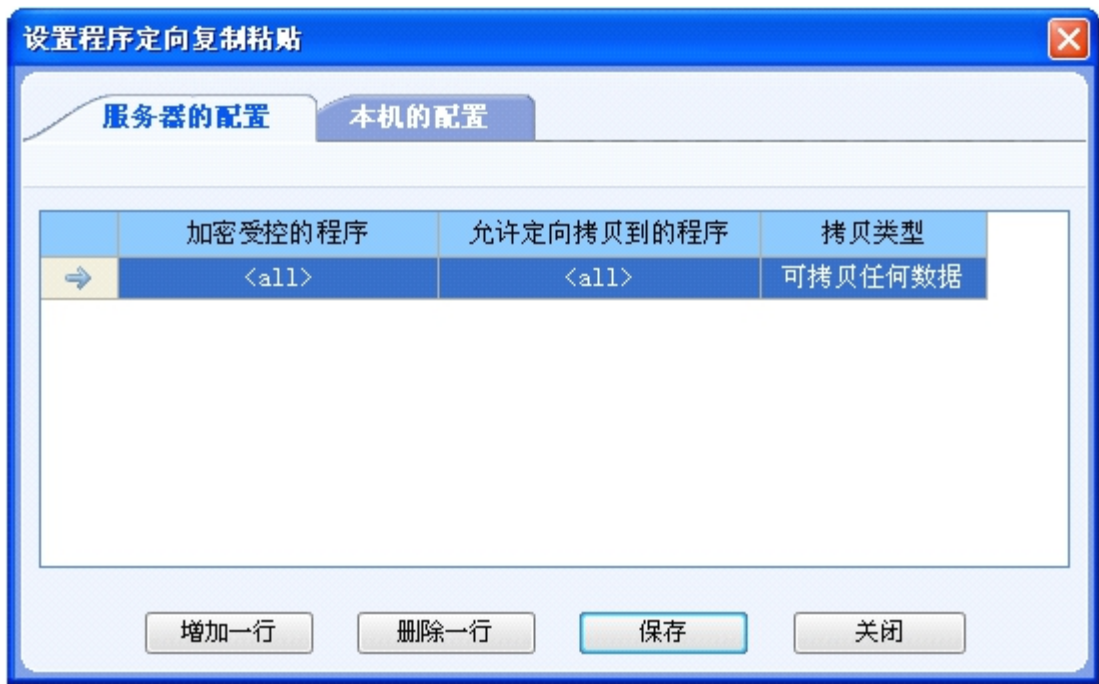


图 3.19

3.11 设置备份目标目录

点击“设置备份目标目录”菜单之后，会弹出“设置备份数据服务器路径”对话框，在“备份数据到哪个服务器目录”文本框中，输入我们想保存的目录，点击“确定”，就可以设置备份数据到服务器的目录。点击“帮助”，我们可以看到设置备份目标目录的帮助视频。如图 3.20。



图 3.20

3.12 客户端扫描加密策略

点击“客户端扫描加密策略”菜单之后，会弹出“客户端自动扫描加密策略”

对话框。在“文件扫描时间”文本框中，我们可以设置每天扫描的时间；选中“安装加密后重启计算机立即扫描”，文件扫描时间那个框就变灰了，而且将写回配置文件的文件扫描时间定为当前扫描时间（即写回“now”）；在“是否备份”单选框中，我们可以设置是否对文件进行备份；在“文件扫描类型”文本框中，我们可以输入需要扫描的类型或者点击“默认类型”，可以设置需要扫描的类型或者所有类型；在“文件扫描路径”文本框中，我们可以输入需要扫描的路径或者点击“...”按钮或者“默认路径”，可以设置需要扫描的路径或者选择路径或者所有的路径。点击“确定”，我们可以保存所做的设置。点击“帮助”按钮，我们可以查看客户端自动扫描加密策略的视频。如图 3.21。

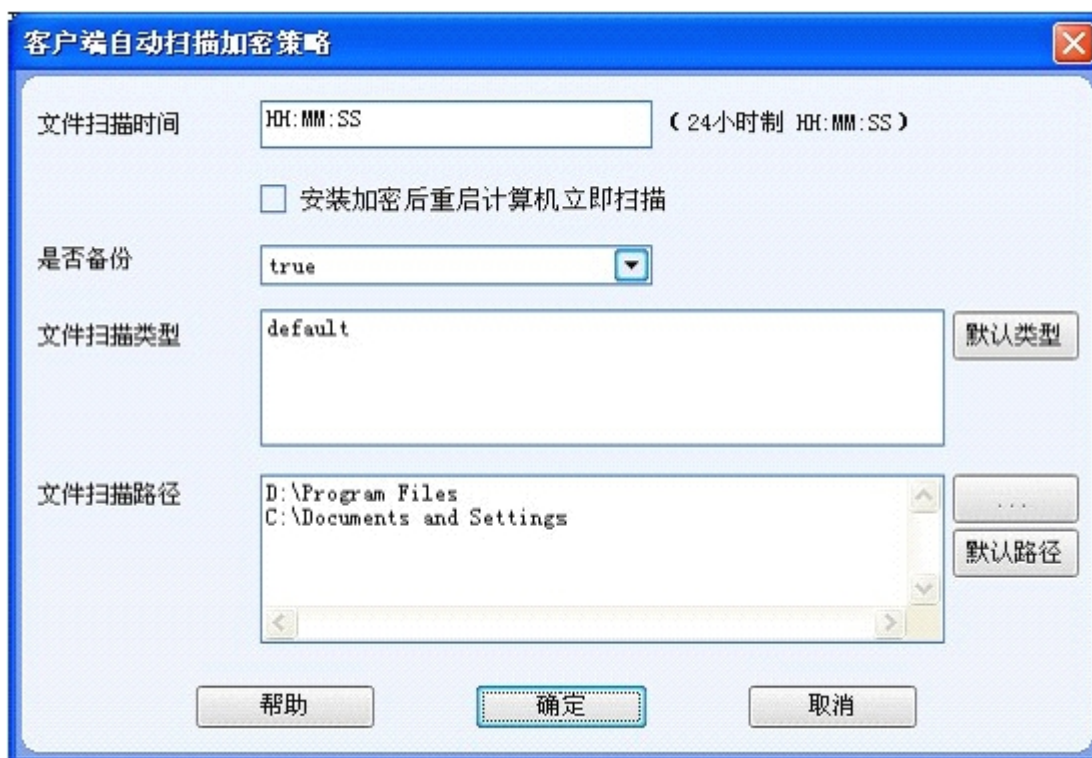


图 3.21

3.13 手动更新本机加密策略

点击“手动更新本机加密策略”菜单之后，会弹出“Renew Encryption”的窗口，这样我们就可以将设置的策略重新加载，并派发到所有连接这个服务器的客户端上。

第四章 解密流程使用配置

首先，对一个文件的解密，需要有人申请解密，然后由特定的人进行审批，之后再由特定的人进行解密，所以，我们要先建立几个账户（注意：这里分为两种用户，一是 Windows 账户，二是恒隆加密系统的用户，这里虽说是两种用户，但是名字相同的账户一一对应）。

4.1 启用解密流程

8.7.0 包括之后的版本在安装的时候默认是没有启用解密流程的，若想启用解密流程，用户只需在客户端上登录到加密控制台，选择“解密流程”菜单中的“配置解密流程服务器”

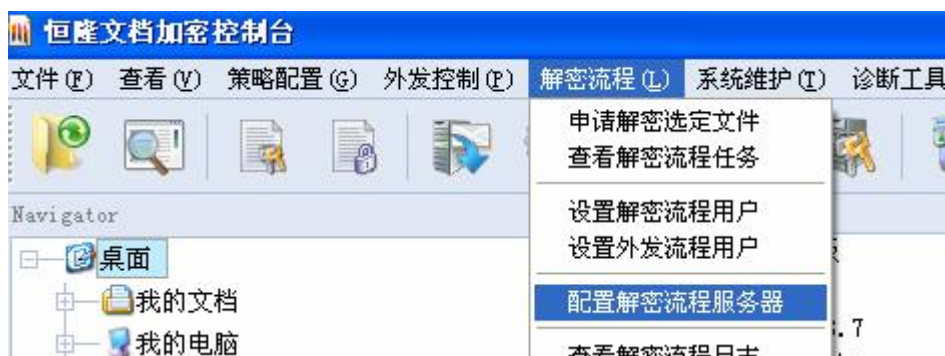


图 4.1

在“启用及配置解密流程”对话框中，填写主解密授权号、服务器地址及端口，以及相关的配置信息，然后点击保存。

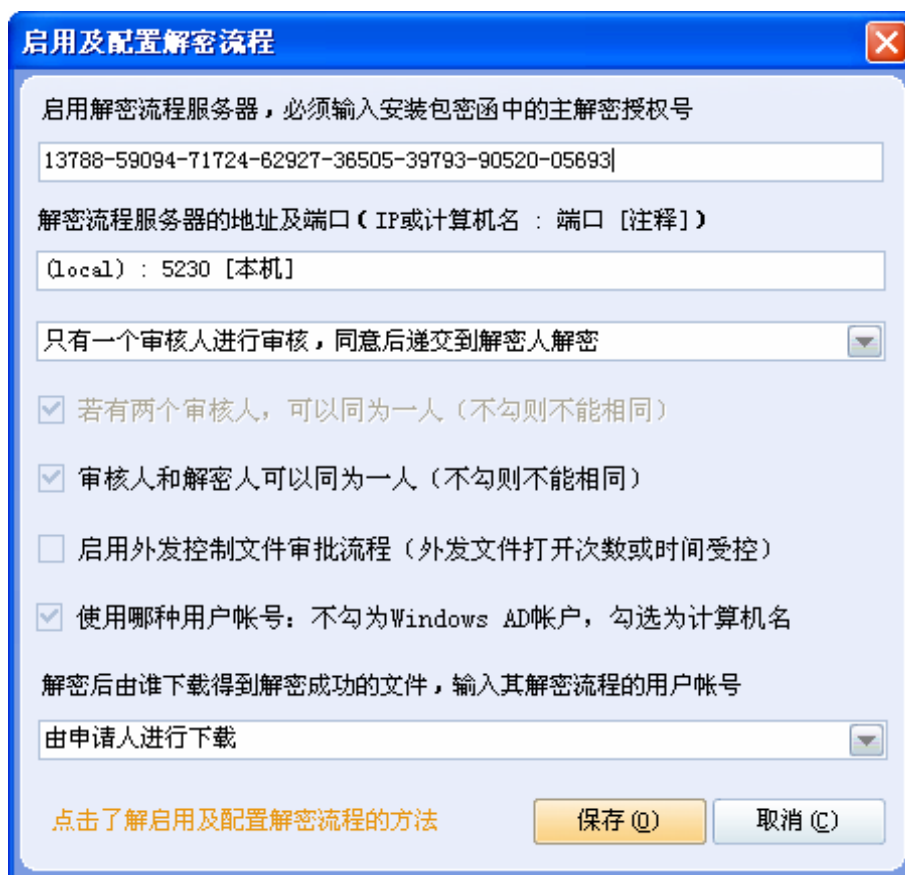


图 4.2

会弹出如下图所示提示框

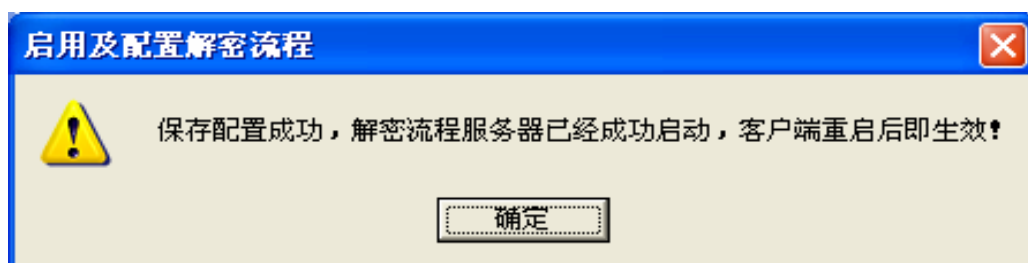


图 4.3

点击“是”则进行密码修改，“否”则不修改。

此时，解密流程已经成功启用。

4.2 创建恒隆加密系统的用户

用户只需在客户端上登录到加密控制台，选择“解密流程”菜单中的“解密流程用户管理”

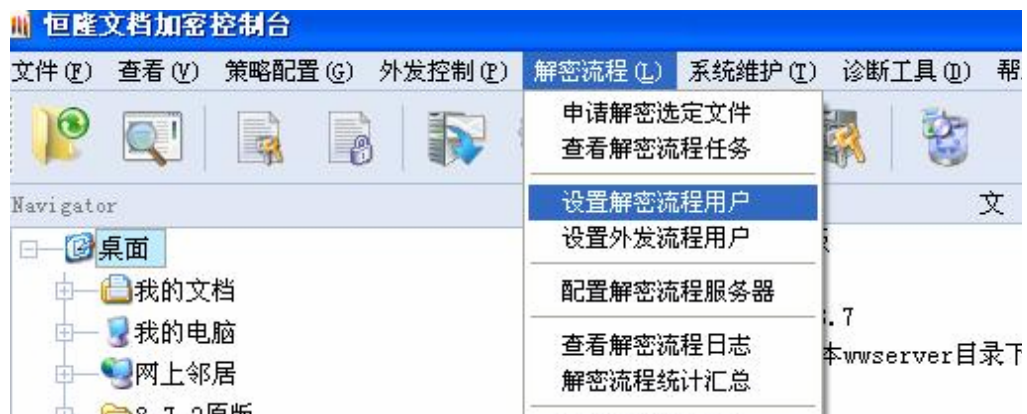


图 4.4

打开解密流程管理器之后，用 adm 身份重新登陆。

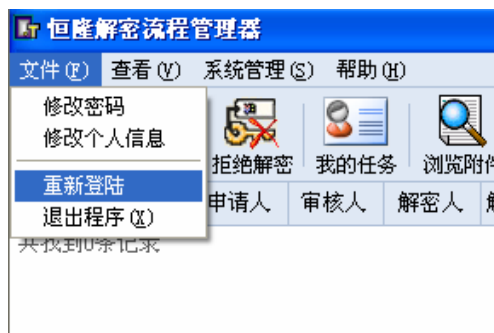


图 4.5



图 4.6

登陆进去以后，选择左上角“系统管理”-->“用户管理”菜单，进入用户管理窗口，首先建立两个部门（以技术部和销售部为例），点击“新建部门”按钮，填写部门代号和部门名称，点击“保存”按钮，部门就创建成功了。然后我们开始创建

新用户，点击“新建用户”按钮，填写帐号和用户姓名（注意：这里的姓名必须与某一台机器上的真实 windows 帐户名称相同）以及相关信息，点击保存按钮，一个用户就新建好了。以同样的方法再建立两个用户（用户名分别为张三，李四，王五），并将不同的人分配到特定的部门。建立结果如下图所示：



图 4.7

到此，我们新建用户工作就完成了，接下来需要做的是为他们分配权限。首先，我们假定他们的权限如下表所示：

| 所属部门 | 用户名 | 审 批 | 解 密 |
|------|-----|-----|-----|
| 设计部 | 张 三 | | √ |
| | 李 四 | √ | |
| 销售部 | 张 三 | | √ |
| | 王 五 | √ | |

表 4.1

接下来，我们依据上表来分配权限。选择“系统管理”-->“功能权限管理”，在各用户所拥有的对应权限处进行勾选。如张三只有解密权，就在对应权限的下载/修改权一列打勾（第一列为浏览权，第二列下载/修改权，第三列为授权人）。示例如下：

| | | | | |
|---|--------|--|---|-----|
| → | 数据解密权限 | | ✓ | adm |
| | 解密审核权限 | | | |

图 4.8

至此，用户部分操作结束。

4.3 解密流程

在装有恒隆加密系统客户端的机器上创建一个文件（以 word 文档为例），对其进行修改后保存，此时我们得到的是一个被加密的文件。现在我们想对其解密，其具体解密步骤如下：

1 申请人发送解密申请

1) 在文件上右击，选择“启动加密流程”。

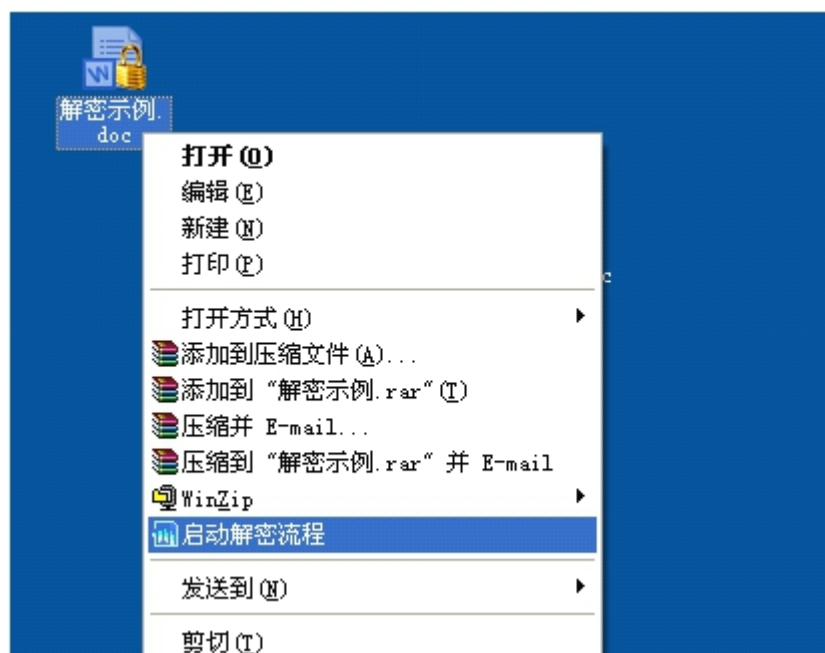


图 4.9

2) 第一次使用时会出现要求输入中文用户名，选择相应部门，输入完成后点击确定会出现如下图所示对话框，点击确定。

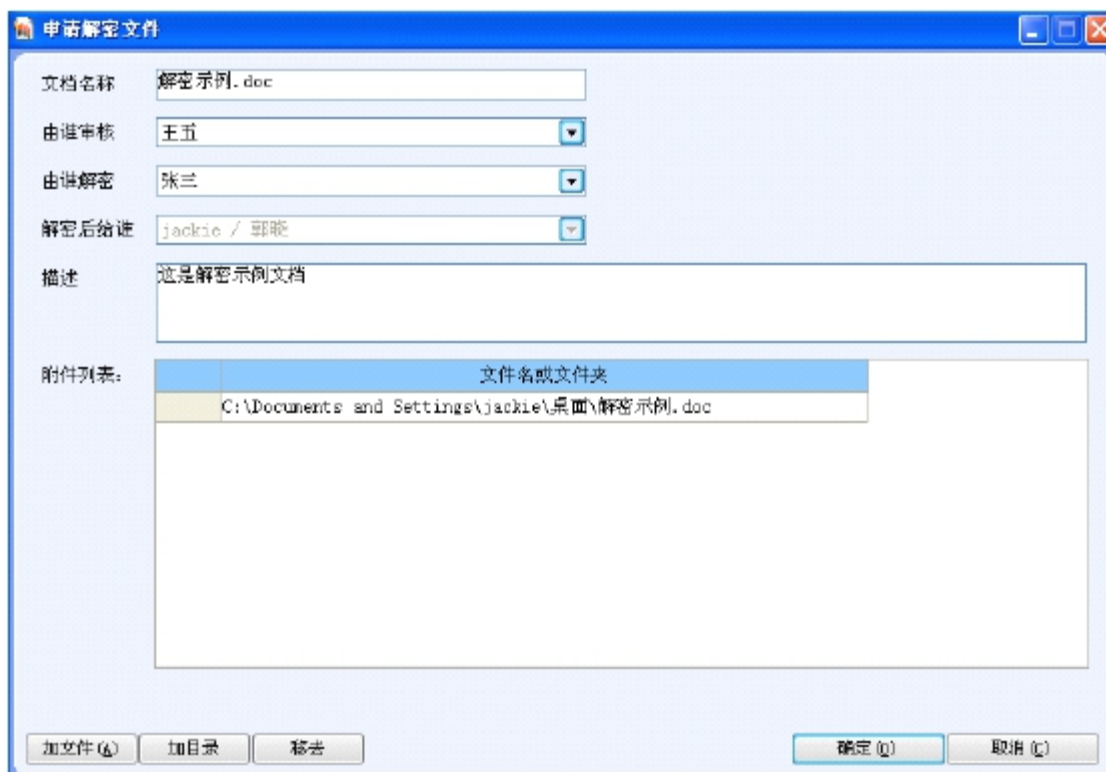


图 4.10

若弹出如下图所示提示框，则表示申请发送成功，王五即可收到此申请，并得知有解密申请需要审批。

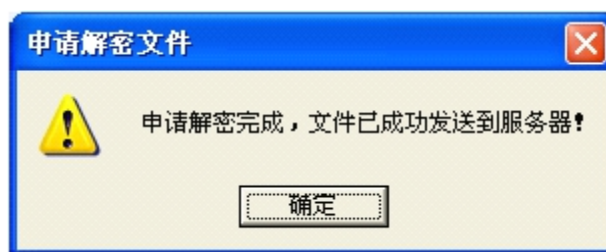


图 4.11

2 审批人进行解密审批

当上述解密申请发送成功后，王五会收到如下申请通知框，由此得知有审批任务。



图 4.12

点击该框，进入图档安全解密管理界面。此时，王五就可以看到有一个文档解密申请，如下图所示



图 4.13

在对该解密申请进行处理之前，王五必须先修改自己的密码（默认密码为空，为安全起见并且处理时要求密码输入，要求必须修改密码），点击文件菜单中的修改密码，对密码进行修改。



图 4.14

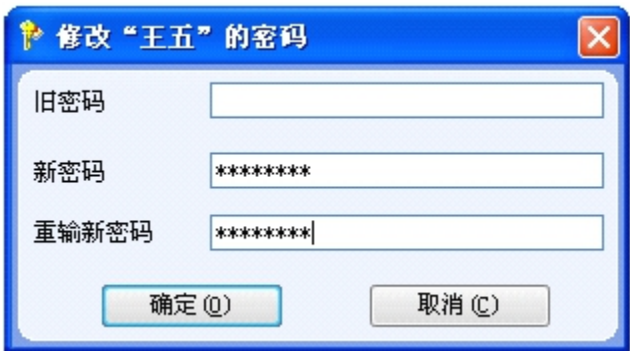


图 4.15

修改密码完成后，点击确定，会提示密码修改成功。



图 4.16

此时，点击菜单中的“同意解密”（或者“拒绝解密”），会进行密码确认，如图。



图 4.17

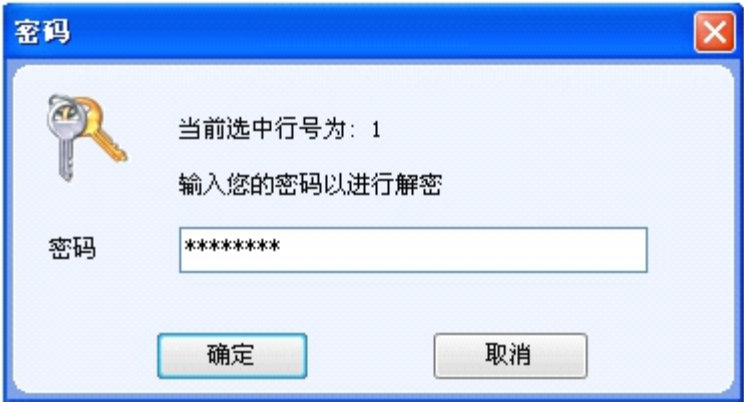


图 4.18

密码确认成功后，会出现对申请的解密操作完成提示框。



图 4.19

当然，这里并非已经完成整个解密流程，只是审批流程结束。

3 解密人释放最终解密权

上述审批结果完成后，解密人张三会收到一个申请解密的消息提示（类似于王五收到申请消息框）。张三进入图档安全解密管理界面以后，可以看到有一个解密任务，如下图所示。



图 4.20

同样的，在首次对任务进行处理前，张三需要修改密码（参照上一步），密码修改完成后，点击“同意解密”。

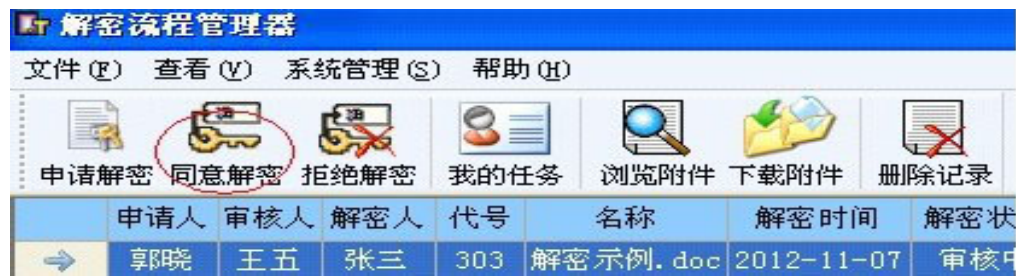


图 4.21

在进行密码确认之后，会提示解密操作完成提示。

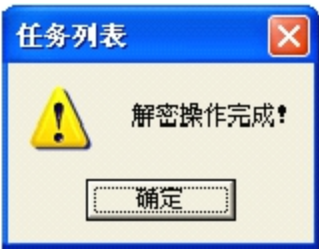


图 4.22

至此，解密流程基本结束。申请人会收到如下消息提示。



图 4.23

4 申请人自己解密

申请人在要解密的文档上右击，菜单中会有“直接解密文件”一项（之前没有），如图



图 4.24

点击进行最终文件解密，注意，这里要求必须填写解密密码（此密码为对服务器进行解密授权时填写的解密密码）。

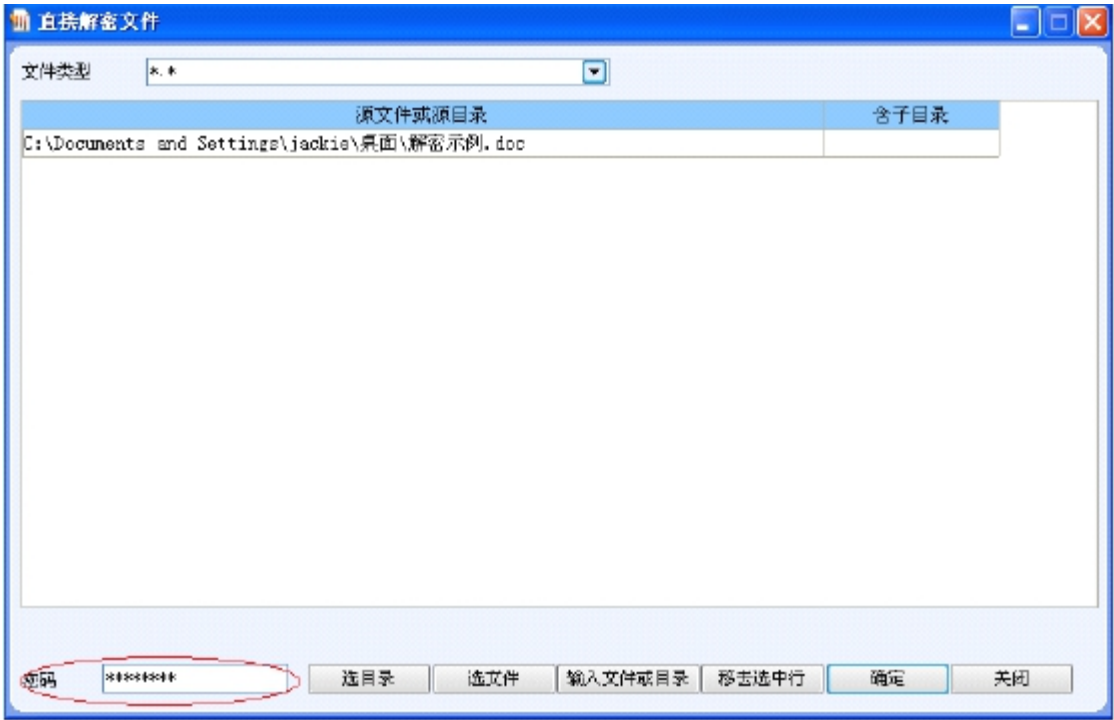


图 4.25

点击确定，提示解密成功。

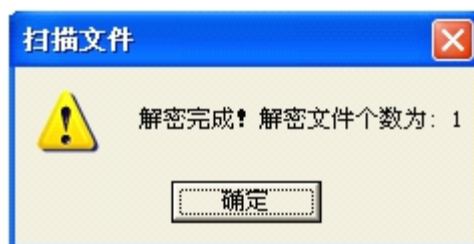


图 4.26

解密成功后，进行刷新操作，文档图标右下角的小锁消失，此时，该文件为未加密文件。



图 4.27

4.4 常见问题

1) 服务器没有解密授权

审批人或者解密人进行处理任务时出现如下提示框，说明没有对服务器进行解密授权。

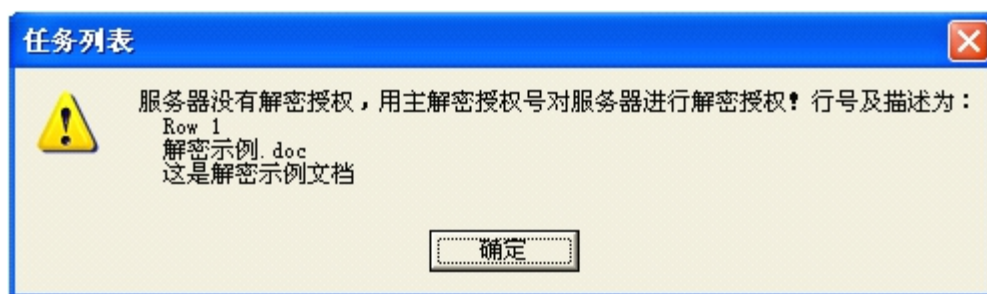


图 4.28

解决办法：对服务器进行解密授权

具体步骤：

- a. 以管理员身份登录恒隆加密控制台



图 4.29

b. 点击“授权解密”图标，如下图

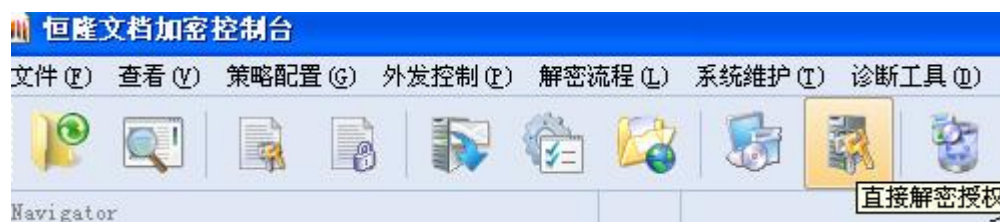


图 4.30

会出现“授权解密”对话框，填写安装包密函中的主解密授权号，以及需要解密授权的机器的机器码（本例中为批准人的机器码），有效期限可以自己选填，不添表示永久有效，注意，这里的“解密文件前需要输入的密码”必须填，而且很重要（申请人最终解密文件时需要输入）！！！！



授权解密

安装包密函中的主解密授权号

13788-59094-71724-62927-36505-39793-90520-05693

授权哪台计算机可以解密，输入其机器码

33002-07688-56974-23270-00362-90533

有效期限（天数），空白表示永久有效

解密文件前需要输入的密码（重复）

能解密的文件类型（英文逗号分隔的exe列表，空为全部）

本机机器码为：

20504-00649-54362-69883-45434-68342

本机信息 取文件类型 在线申请 离线申请 关闭

图 4.31

点击“在线申请”，会提示成功生成授权号（注销或者重启后才能解密）。

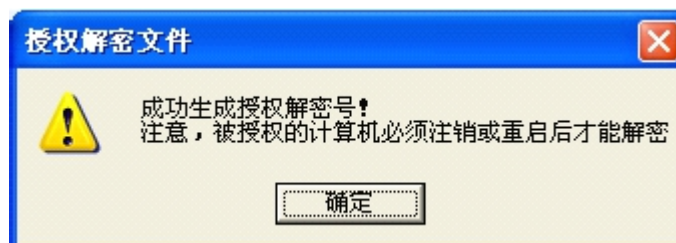


图 4.32

第五章 文件外发配置

5.1 文件外发的 4 大特点

a、自解压包

将需要外发到外部的文件制作成一个自解压包（是一个 exe 执行程序），自解压包可以在任何机器上运行自解压，也可以指定接收计算机的必须是给定的机器码才能进行自解压

b、打开次数控制

可以控制外发的文件打开一定的次数后自动销毁并非删除文件，只是自解压失效，以前解压出来的文件也无法打开，复制出来的文件也无法打开

c、控制打开时间

可以控制文件在一定时间内是可以打开的，过了有效期后无法再打开

d、控制外发文件打印

可以指定外发的文件能否进行打印

5.2 如何将外发文件做成外发包

步骤一：外发服务器授权

登录恒隆加密控制台，选择“外发控制”菜单中的“外发服务器授权”



图 5.1

填写由恒隆科技提供的安装包密函中的外发授权号

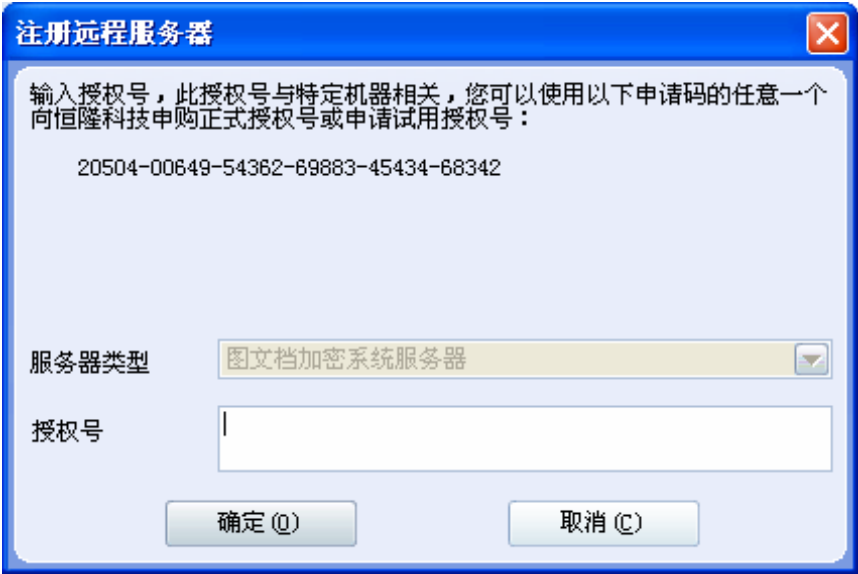


图 5.2

点击确定，完成外发服务器授权，弹出如下提示，表明成功注册服务器。



图 5.3

步骤二：设置外发用户帐号

选择“外发控制”菜单中的“设置外发用户帐号”。

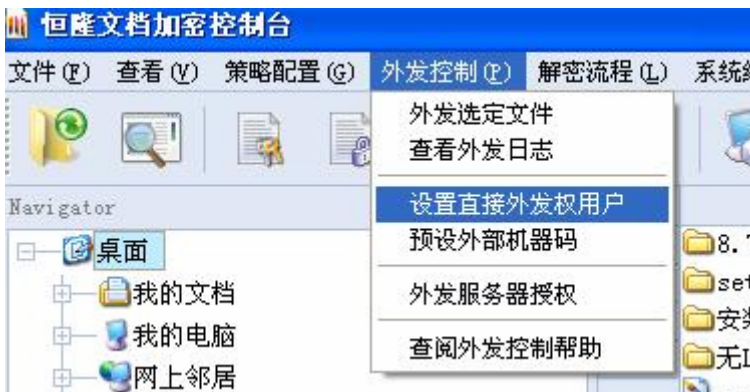


图 5.4

在设置外发文件的用户帐号框左侧给账户设置外发权限（以王五为例）

| 设置可外发文件的用户帐号 | | | | |
|--------------|------|-------|----|------|
| (4, 4) | 用户帐号 | 用户名 | 类型 | 外发权限 |
| | adm | 系统管理员 | 用户 | |
| | 李四 | 李四 | 用户 | |
| | 张三 | 张三 | 用户 | |
| ➡ | 王五 | 王五 | 用户 | ✓ |

图 5.5

或者在右侧直接填写用户信息

用户帐号

用户姓名

用户类型

用户密码

确认密码

电子信箱

所属密级

状态

机器码

授权码

图 5.6

可外发账户设置完成后点击保存，关闭。

步骤三：选定外发文件，进行打包

选择“外发控制”菜单中的“外发选定文件”

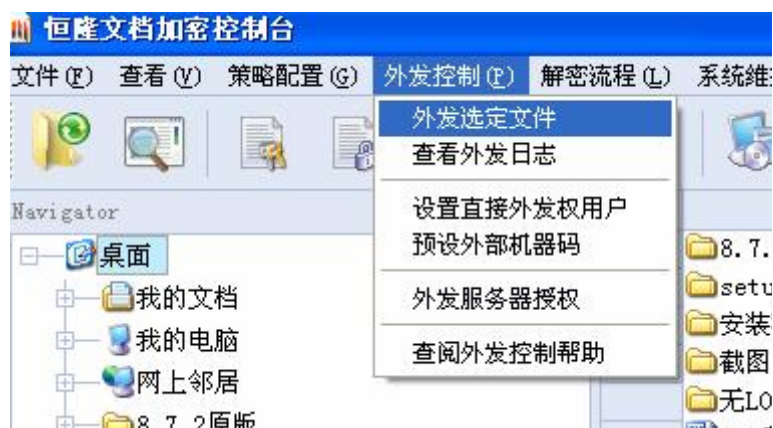


图 5.7

以王五的身份登陆。



图 5.8

将出现如下窗口，具体步骤如下：

- 填写打包外发后的文件名称（如外发示例.exe）
- 填写指定机器码（即指定能打开外发包的机器）
- 选择要外发的文件（如外发示例 1，外发示例 2）
- 设置文件的外发权限（举例如图所示）

注意：打包后的外发文件名只支持后缀名为.exe 或.wbs 格式

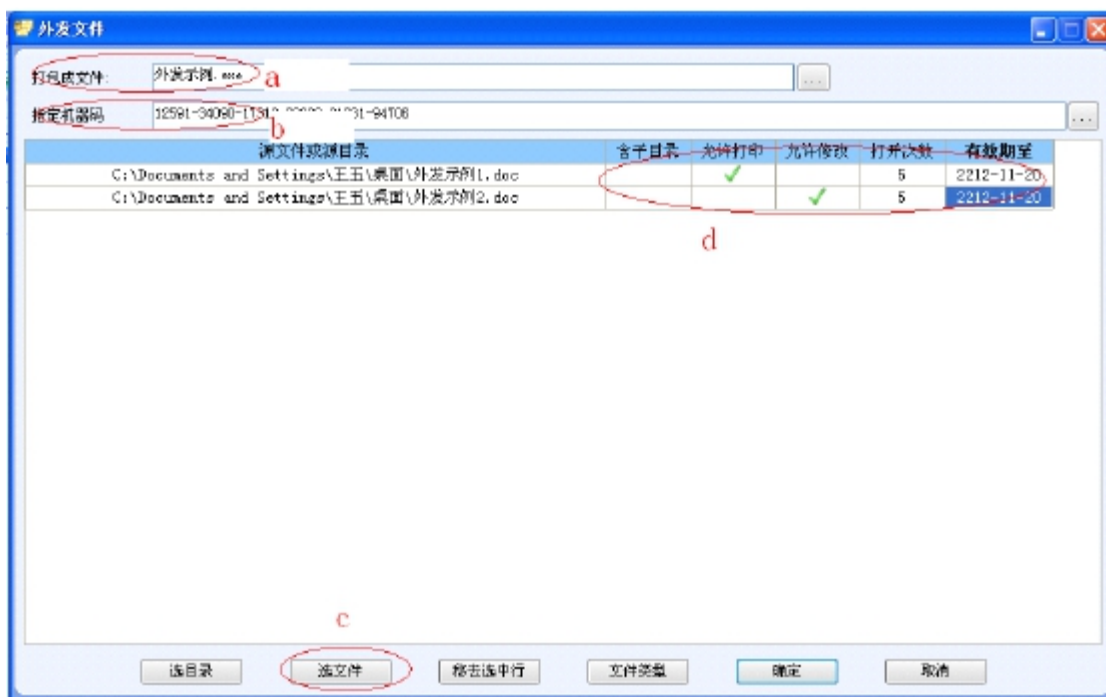


图 5.9

设置好之后点击确定按钮，会出现打包外发文件成功提示

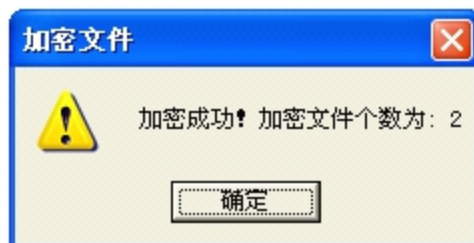


图 5.10



此时，桌面上会出现一个名为外发示例的打包文件

接下来要做的就是将该外发包发（直接拷贝）给特定的人（本例中为王五）。

5.3 外发包的使用

王五拿到外发包以后，直接双击打开，会出现如下图所示对话框。

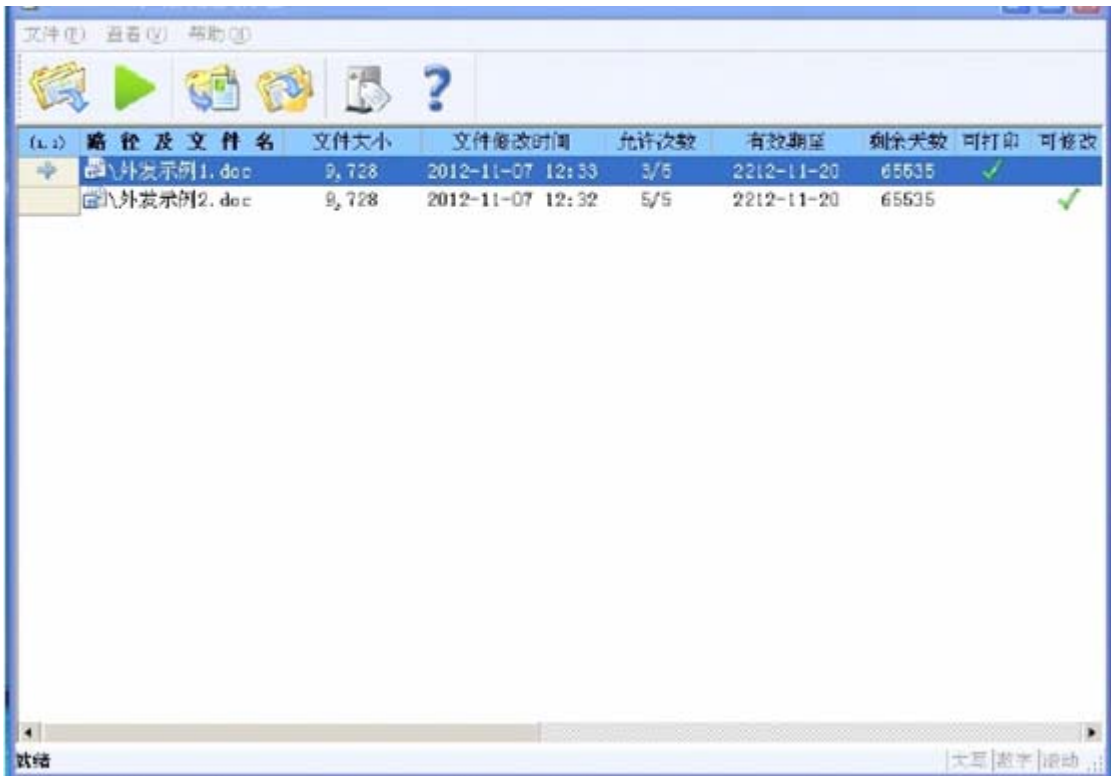


图 5.11

点击菜单栏的“下载选中文件”

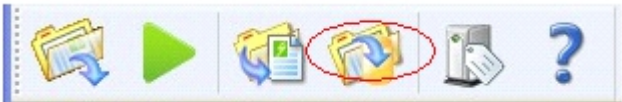


图 5.12

会弹出选择下载存放路径对话框

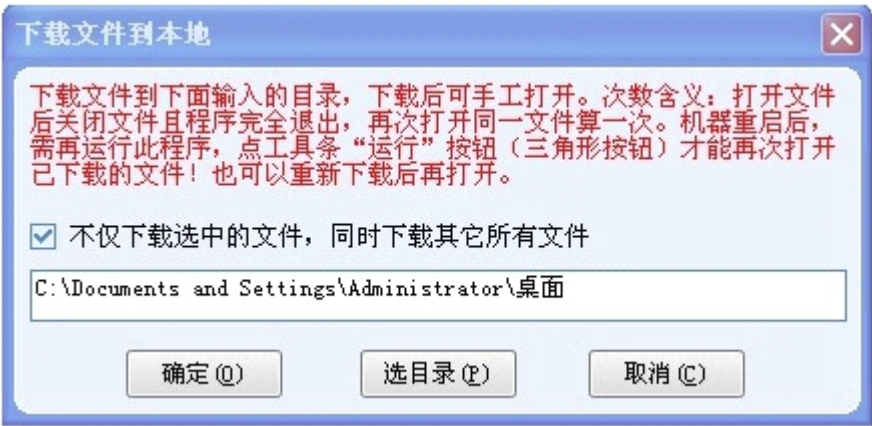


图 5.13

选择路径后点击确定按钮，会弹出下载成功提示，

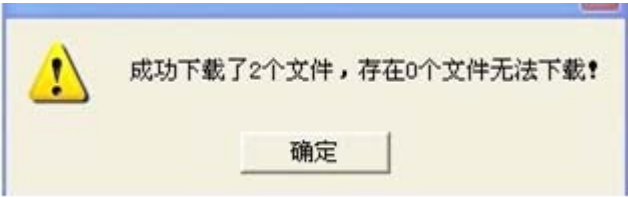


图 5.14

此时，两个文件已经成功下载到桌面上了。

5.4 查看外发记录

选择“外发控制”菜单中的“查看外发日志”，可以对之前的外发详情进行查看

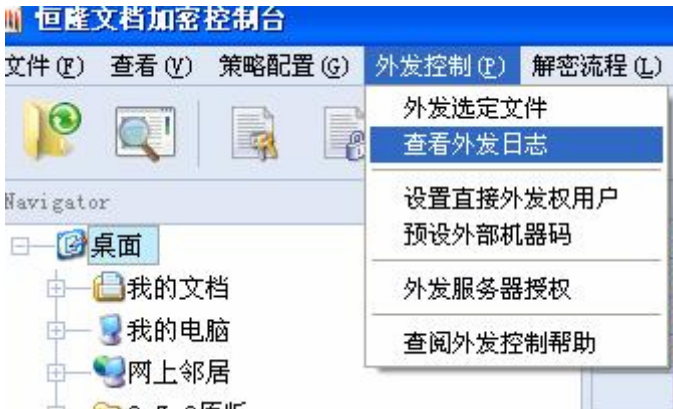


图 5.15

例如，在查找内容里输入王五，即可查看与王五有关的文件外发记录。



图 5.16

也可以点击下面的“查看详情”按钮，将上述查看到的外发记录以文本文档的形式显示。



图 5.17

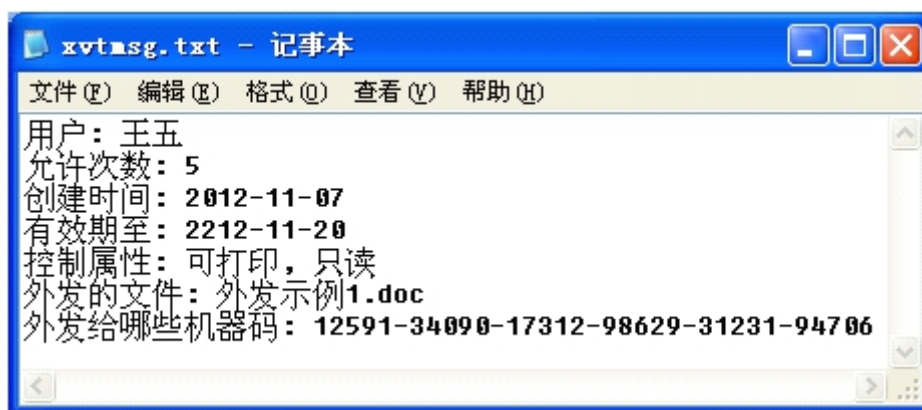


图 5.18

也可以选择将记录信息“导出”，导出的格式为 Excel 表格。

5.5 常见问题

a、无法运行外发包

解决方法：首次运行时需要 windows 管理员，若是 Win7 用户，则需右键点击外发包“以管理员身份运行”

b、在打开外发包文件之后再打开其他文件，保存后无法打开

解决方法：问题原因是文件被加密了，将外发程序退出后即可恢复正常

c、重启机器之后无法打开外发文件

解决方法：重新打开外发包，点击菜单中的“启动外发控制驱动”



第六章 明文邮件配置

6.1 邮件白名单介绍及其作用

邮件白名单就是列有邮件发件人和邮件接收人的一个表单，其作用是，当邮件发件人和邮件接收人完全匹配时，发件人所发给收件人的附件（暂时不支持压缩包）是经过解密处理的，也就是收件人可以正常打开这个附件，当发件人或收件人有一者不匹配，发出去的附件就是被加密的，收件人将无法打开或查看附件。

6.2 邮件白名单的创建

步骤一、打开恒隆加密控制台，点击“策略配置”菜单中的“明文邮件设置”

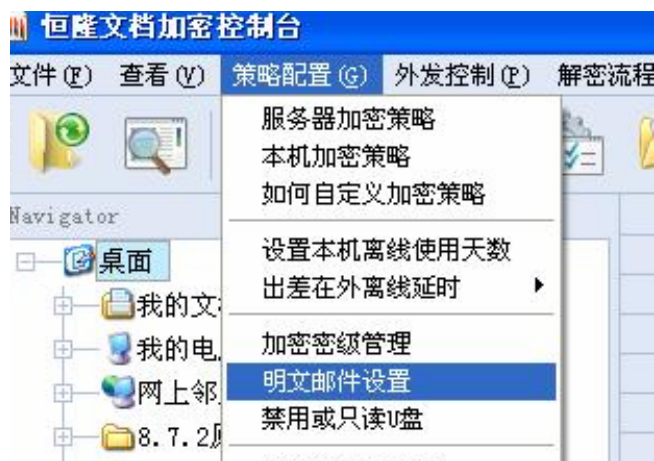


图 6.1

步骤二、在明文邮件设置中点击下面的“增加邮件”按钮，弹出如下图所示对话框，填写发件人和收件人地址以及备注。点击确定。



图 6.2

这时，明文邮件设置中就会有一条记录（即白名单）。



图 6.3

邮件白名单添加好了以后点击保存。

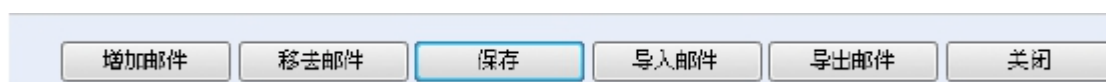


图 6.4

您可以点击“增加邮件”按钮继续添加记录，也可以点击“移去邮件”来删除记录。

6.3 白名单的导入与导出

1、邮件导入：

可以事先写好要导入的信息（格式为.txt 文本，3 列，中间以英文逗号，英文分号或者 Tab 键隔开），例如，我在桌面上事先写好了要导入的文件 mail.txt（此例中文件内部各列是以英文逗号分开的）



图 6.5

在上述明文邮件设置对话框中点击“导入邮件”按钮，在弹出的“导出明文邮件地址”对话框中的分隔符中选择“英文逗号”，然后将我们事先写好的导入文件（mail.txt）选上



图 6.6

点击确定，两条记录就被成功导入进去了。

| 明文邮件设置 | | |
|-------------|-------------|-------------|
| 明文邮件发件人地址 | 明文邮件收件人地址 | 明文邮件收备注说明 |
| *@hl158.net | * | 恒隆科技成员发给任何人 |
| *@hl158.net | *@hl158.net | 恒隆科技内部 |
| * | *@hl158.net | 任何人发给恒隆科技 |

图 6.7

2、邮件导出：

在上述明文邮件设置对话框中点击“导出邮件”按钮，填写导出文件的名称及存放路径。

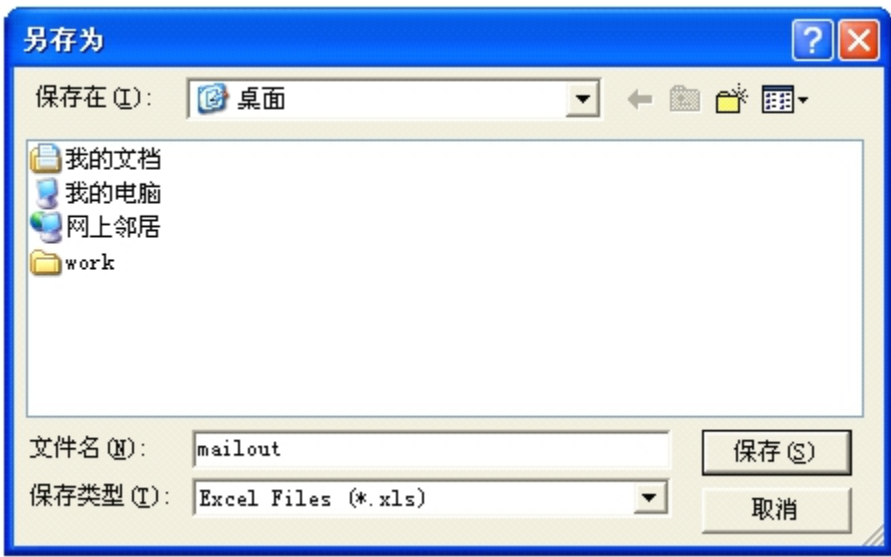


图 6.8

点击“保存”，邮件导出成功。打开导出的文件，可查看详细的记录。

| | A | B | C |
|---|-------------|-------------|-------------|
| 1 | 明文邮件发件人地址 | 明文邮件收件人地址 | 明文邮件收备注说明 |
| 2 | *@hl158.net | * | 恒隆科技成员发给任何人 |
| 3 | *@hl158.net | *@hl158.net | 恒隆科技内部 |
| 4 | * | *@hl158.net | 任何人发给恒隆科技 |
| 5 | | | |

图 6.9

6.4 注意事项及常见问题

- a、该明文邮件功能只支持 outlook 或者 foxmail。
- b、明文邮件发件人地址和明文邮件收件人地址要完全地匹配

说明：当发件人给收件人发送邮件时，如果两者的地址有任意一个与白名单上的记录匹配不上，则邮件中的附件是被加密的，收件人是无法打开的。有些邮箱后缀名不同但是它们所对应的 IP 地址却只有一个，对于这样的情况，我们需把每一个邮箱地址都加入到白名单中，例如一台机器上有后缀名不同的两个邮箱地址（如 jackie@hl158.net 和 jackie@hl158.com.cn），此时，我们需要把这两个邮箱地址分别写如白名单。

- c、一个发件人给多个收件人发送邮件，若其中有任何一个收件人地址不符合邮件白名单，则所有收件人收到的邮件都是被加密过的，无法正常打开。

第七章 文件备份管理

加密系统除了能加密文件外，还可以实现对修改过的文件进行自动备份到服务器，对话框“设置备份数据服务器路径”用于设置将客户端修改过的文件备份到哪个目录，这个目录必须位于服务器上。

缺省情况下，该目录被自动设置为“<APPPATH>\XVTDATA”（不含引号），该目录是一个相对目录，其中“<APPPATH>”表示服务器的安装目录，例如加密服务器软件安装在“D:\WWSERVER”，则客户端修改的数据将自动备份到“D:\WWSERVER\XVTDATA”中。



图 7.1

该对话框“设置备份数据服务器路径”可以在客户端调用，但设置的目录必须是服务器本地的目录，即客户端的设置界面只是为了方便维护人员，不用进入服务器机房进行服务器维护，维护人员操作设置的目录等同于在服务器端直接操作服务器的目录。例如，该路径设置为“D:\BACKUP”，则表示加密客户端的数据将自动备份到服务器的“D:\BACKUP”目录。

该目录不能被设置为共享目录映射硬盘，例如 IGSERVER 是加密服务器，而另外一个服务器叫 BACKUPSERVER，而 BACKUPSERVER 共享了一个 BACKUP 目录，在 IGSERVER 上将“\\BACKUPSERVER\BACKUP”映射为 Z 盘，则该 Z 盘不能作为为备份目录。

但该目录可以设置为网络共享目录，例如设置为“\\BACKUPSERVER\BACKUP”目录，设置好共享目录后，还必须将后台加密系统的服务改用系统管理员登录（而设

置为服务器本机目录不需要做以下操作），具体操作如下：

- (1) 打开“控制面板 性能和维护 管理工具 服务”（也可以使用命令行执行“SERVICES.MSC”来弹出服务列表，如下图）；




图 7.2

- (2) 找到“HL InfoGuard”服务，选中，点右键查看属性，点中“登录”页，勾选“此帐户”，然后输入服务器本机的 Administrator 及密码，点确定；



图 7.3

(3) 重启该服务。

设置上上述备份目录后，需要在加密控制台的工具条上点击以刷新服务器，也可以到服务器端重启“HL InfoGuard”后台服务，这样，新的备份目录就生效了。

备份的效果如下，假设备份目录“D:\BACKUP”，客户端机器名为“DESIGN01”，编辑的文件为“D:\MYWORK\任务报告.DOC”。则修改该客户端文件 10 分钟后，在加密服务器上可以找到此文件，具体为“D:\BACKUP\ DESIGN01\D\ MYWORK\任务报告.DOC”。

还必须注意，若客户端修改的是共享目录上的文件，则该文件不会被备份，备份功能只针对本地的文件进行，因为共享目录上的文件属于“他人”所有，在他人本机编辑时，已经被备份过。

第八章 系统维护

在打开恒隆加密控制台之后，点击“系统维护”菜单，在下拉列表中可以看到我们可以对系统进行一系列的维护操作。下面我们来一一列举这些功能，以便客户使用。

8.1 系统维护菜单

1)修改用户密码

点击“修改用户密码”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“修改用户密码”对话框，我们可以输入原密码和新密码，来修改当前用户的密码，点击“确定”，修改成功。如图 8.1。



图 8.1

2)客户端站点管理

点击“客户端站点管理”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“用户管理”的对话框，我们可以对当前服务端下的所有用户进行管理。在左边的树形列表中，可以查看到用户部门和部门下的用户。在点击这些树形分支元素之后，右边的文本框里面会显示部门和用户的信息。如果点击的是部门分支，则会显示部门代号和部门名称；如果点击的是用户分支，则会显示用户帐号、用户姓名、用户类型、所属密级、机器码和授权码等信息。对话框下面有一个文本框和一些按钮，在文本框中输入所要查找的用户，点击“查找”，则会在原来树形列表中显示查到的部门和

用户的用户帐号、用户名、类型以及查到的记录数量，如果没有记录，则显示“共找到 0 条记录”，点击“切换”按钮，则会在查找记录和用户树形列表中切换显示。右边的按钮是一些对用户和部门的一些操作。点击“新建部门”，我们就可以通过在右边的文本框中通过输入部门代号和部门名称来增加部门；点击“新建用户”，我们就可以在右边的文本框中通过输入用户帐号、用户姓名、用户密码、所属密级、机器码和授权码等信息来增加用户；在选中部门名称后，点击“加入用户”，弹出“选择用户”的对话框，我们就可以向选中的部门中增加我们已有的用户，同样有个文本框，可以供我们输入所要查找的用户，点击“查找”，则会显示查找到的部门和用户信息，“切换”，会在查找记录和用户树形列表中切换显示，点击“刷新”，则会刷新当前的用户树形列表，选中用户后，点击“确定”，则该用户会被增加到我们刚刚所选中的部门之中，点击“取消”，关闭对话框；在选中用户名称后，点击“移去”，则会从当前的用户部门中移去所选择的用户；点击“删除”，我们就可以删除所选择的用户或者部门；选择用户，点击“反查”，我们就可以查看到当前选择的用户属于哪一个部门；点击“刷新”，我们可以刷新当前的用户管理对话框；点击“保存”，我们就对我们所做的操作进行保存；点击“关闭”，则关闭当前用户管理对话框。如图 8.2。

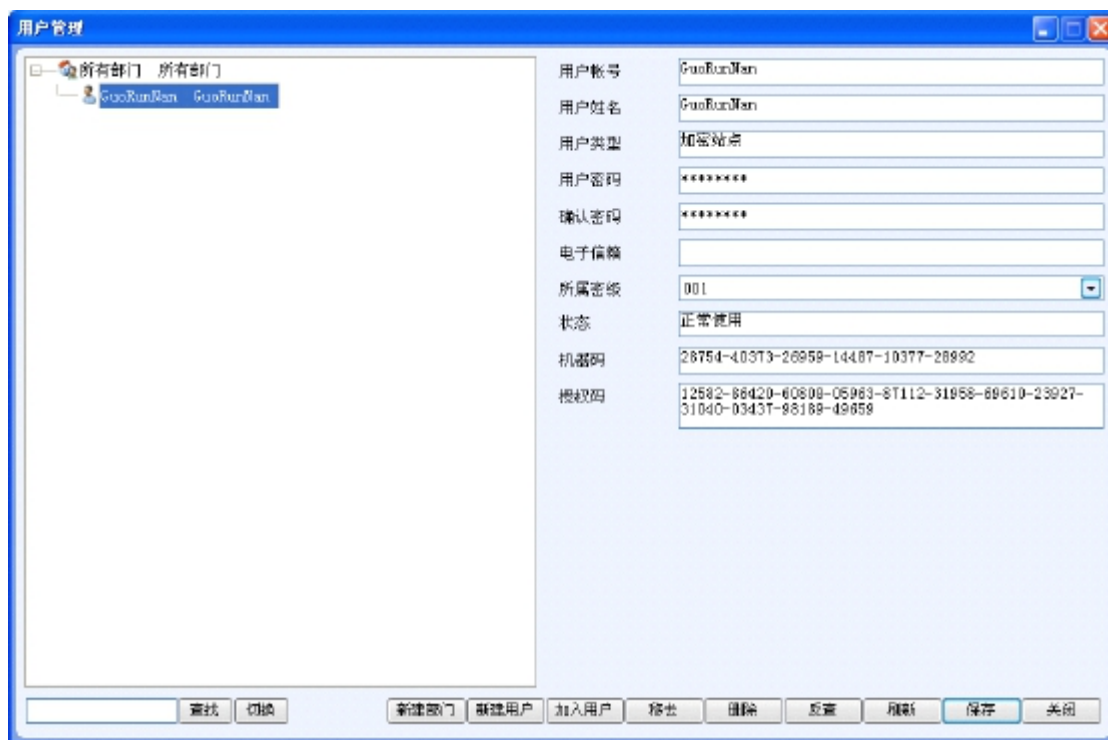


图 8.2

3) 查看已安装的加密站点

点击“查看已安装的加密站点”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“查

看已安装的加密站点”对话框，在对话框中我们可以查看到已经安装的加密站点的一个列表，在下面的还可以将当前站点数量统计出来。点击 “导出” 按钮后，可以将这个列表导出来保存在 Excel 电子表格或者 TXT 文本文档中，点击“确定”，关闭对话框。如图 8.3。

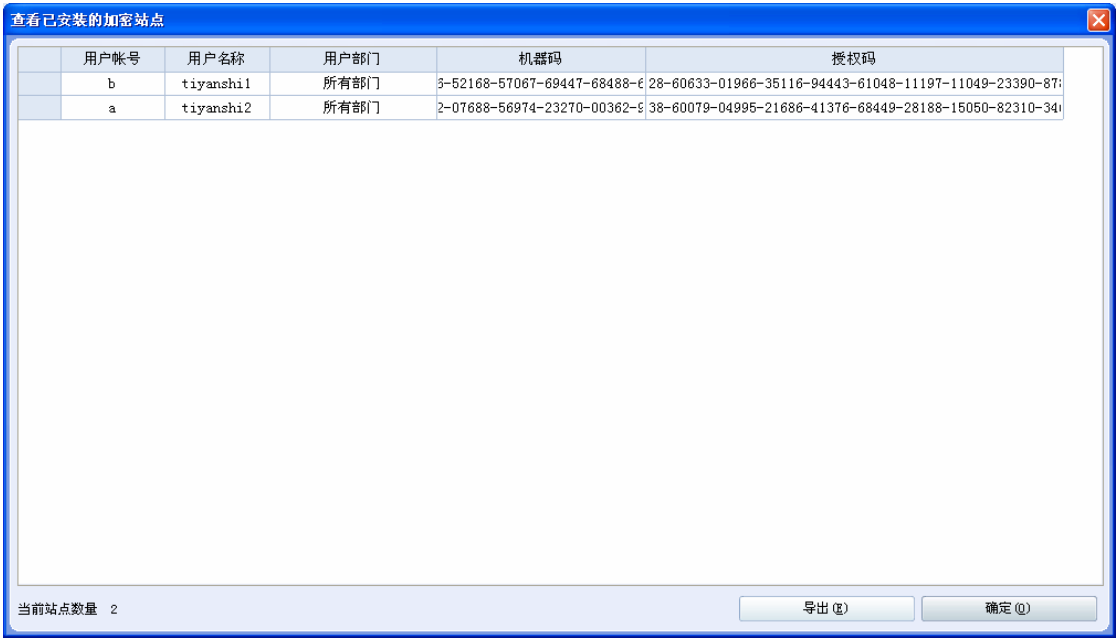


图 8.3

4) 修改解密密码

点击“修改解密密码”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“修改解密密码”对话框，我们可以输入原密码和新密码，来修改当前用户用来解密文件的密码（若有解密权限），点击“确定”，修改成功。如图 8.4。

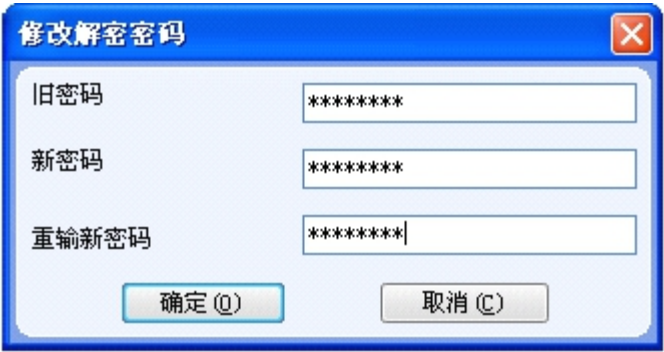


图 8.4

5) 撤销解密授权

点击“撤销解密授权”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“撤销解密

授权”对话框，在“撤销哪台计算机可以解密”文本框中，输入我们想撤销的机器的机器码，点击右边的“...”按钮，弹出“选择用户”的对话框，选择用户后，点击“确定”后，就可以直接将所选的用户的机器码获取到文本框中，点击“确定”，则能撤销所选机器的解密授权。如图 8.5。



图 8.5

6) 查看已有解密授权

点击“查看已有解密授权”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“查看已授权直接解密的站点”对话框，在对话框中我们可以查看到已经有授权直接解密的站点的一个列表，在下面的还可以将当前站点数量统计出来。点击“导出”按钮后，可以将这个列表导出来保存在 Excel 电子表格或者 TXT 文本文档中，点击“确定”，关闭对话框。如图 8.6。

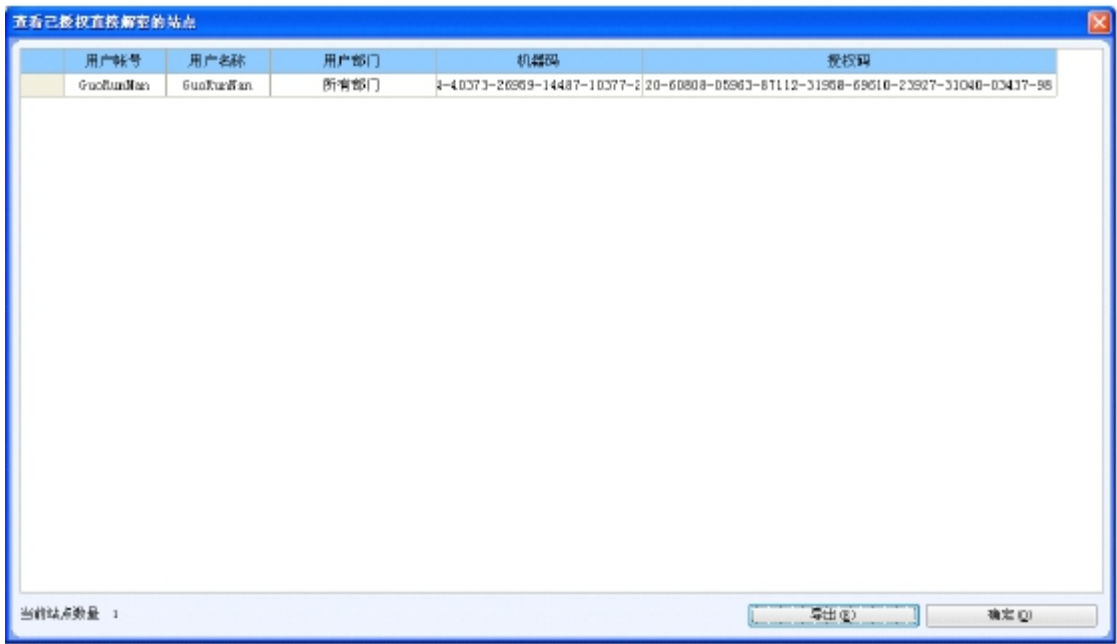


图 8.6

7)生成离线维护号

点击“生成离线维护号”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“生成离线维护客户端授权号”对话框，在“准备离线维护哪台计算机上的加密系统”文本框中，输入我们想撤销的机器的机器码，或者点击右边的“...”按钮，弹出“选择用户”的对话框，选择用户后，点击“确定”后，就可以直接将所选的用户的机器码获取到文本框中，点击“确定”，就可以将系统生成的授权码显示到“生成的授权码”文本框中，我们可以将这个授权码保存下来，在离线的环境下，对系统的一些策略进行维护。如图 8.7。

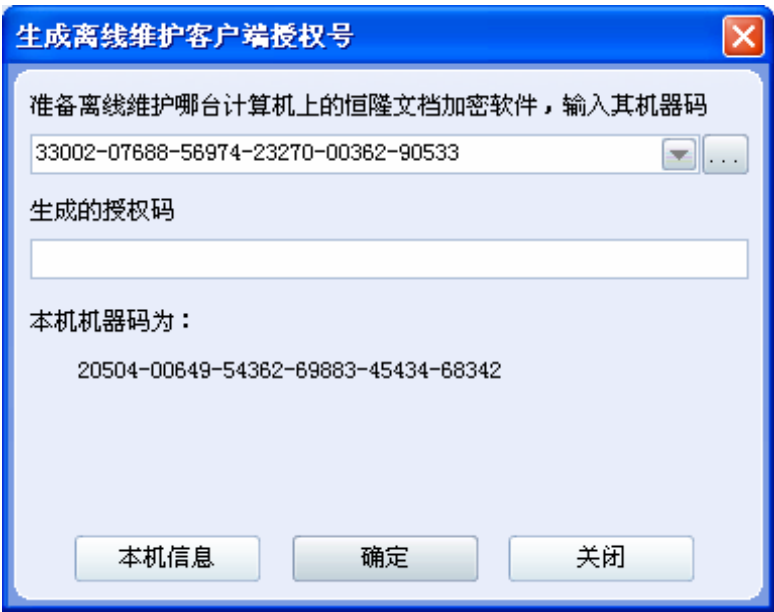


图 8.7

8)远程卸载客户端

点击“远程卸载客户端”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“远程卸载客户端”对话框，对话框下面有一个文本框和一些按钮，在文本框中输入所要查找的用户，点击“查找”，则会在原来树形列表中显示查到的部门和用户的用户帐号、用户名、类型以及查到的记录数量，如果没有记录，则显示“共找到 0 条记录”，点击“切换”按钮，则会在查找记录和用户树形列表中切换显示。在“远程卸载客户端”对话框后，在树形列表中选择你要卸载的用户，然后点击“卸载选中用户”，就可以远程卸载选中的那个用户的客户端了。如图 8.8。



图 8.8

9)生成卸载授权号

点击“生成卸载授权号”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“生成卸载客户端授权号”对话框，在“准备卸载哪台计算机上的恒隆加密系统”文本框中，输入我们想卸载的机器的机器码，点击右边的“...”按钮，弹出“选择用户”的对

话框，选择用户后，点击“确定”后，就可以直接将所选的用户的机器码获取到文本框中，点击“确定”，就可以将系统生成的授权码显示到“生成的授权码”文本框中，我们可以将这个授权码保存下来，对客户端进行离线卸载。如图 8.9。

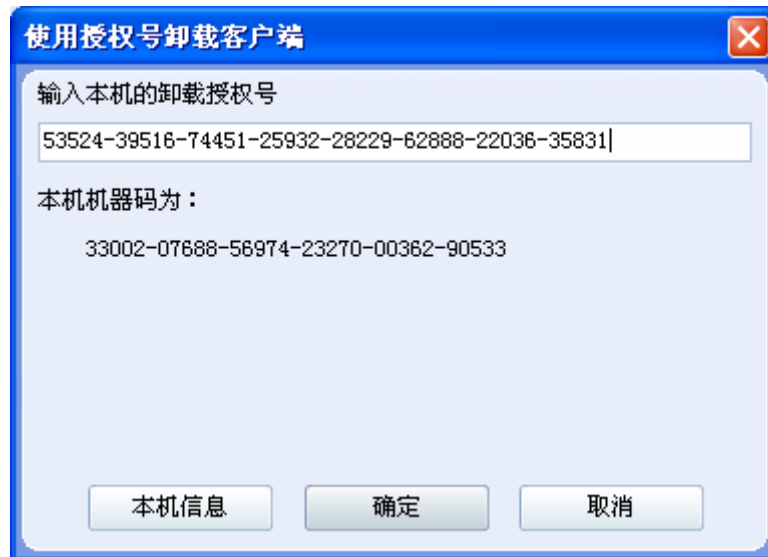


图 8.9

10) 使用授权号卸载

点击“使用授权号卸载”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“使用授权号卸载客户端”对话框，在“输入本机的卸载授权号”文本框中，输入第 8 步生成的授权码，点击“确定”之后，便可以离线卸载客户端。如图 8.10。

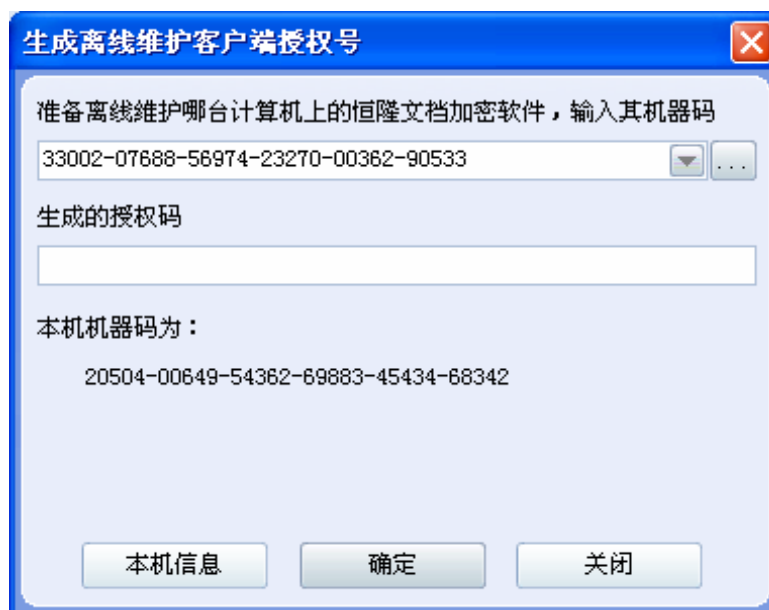


图 8.10

11) 卸载服务器

点击“卸载服务器”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“卸载服务器”的对话框，点击“确定”，就可以卸载服务器。如图 8.11。

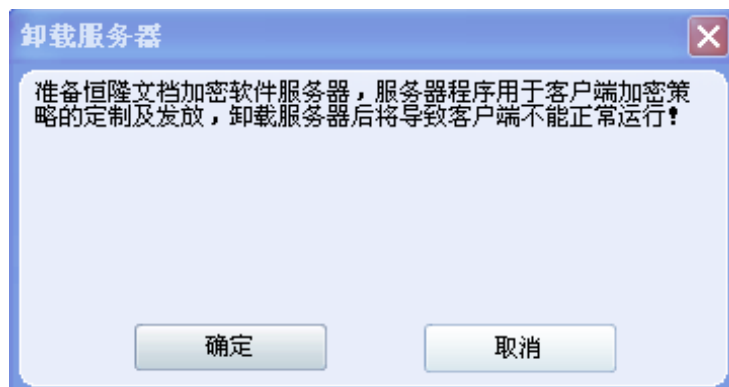


图 8.11

12) 设置服务器地址

点击“设置服务器地址”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，就弹出“成功设置服务器地址”，此时服务器地址为安装服务端的机器的 IP 地址。如图 8.12。

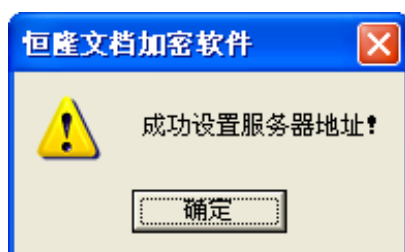


图 8.12

13) 注册加密服务器

点击“注册加密服务器”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“注册加密服务器”的对话框，“服务器类型”和“服务器所在目录”选择默认，“授权号”文本框输入向恒隆科技申购的正式授权号或申请的试用授权号，点击“确定”后，即可成功注册加密服务器。如图 8.13。



图 8.13

8.2 诊断工具菜单

在打开恒隆加密控制台之后，点击“诊断工具”菜单，在下拉列表中可以看到我们可以对系统进行一系列的诊断操作。下面我们来一一列举这些功能，以便客户使用。

1)检测加密客户端状态

点击“检测加密客户端状态”菜单之后，弹出“检测加密运行状态”对话框，对话框中有一些服务器的信息可供查看。在点击“开始检测 Start”按钮之后，系统会自动地检测服务端的信息。如系统无问题，则显示字体为绿色；如系统出现一些问题，则显示字体为红色，可以点击右边的黄色字体的“修复 Repare”，进行修复。点击“查看错误日志 Log”可以查看我们之前的错误日志。点击“关闭 Close”，关闭对话框。如图 8.15。



图 8.15

2)文件驱动诊断台

点击“文件驱动诊断台”菜单之后，弹出“文件驱动诊断台”对话框，对话框是一个单文档结构的程序。在菜单栏中点击“文件”，选择“选择内核类型”，

弹出“选择跟踪内核的类型”的对话框，其中有三个单选选项，“使用 PDM 内核进行跟踪”，“使用加密内核进行跟踪”，“启动独立的跟踪内核进行跟踪”，可以根据不同的需求，选择跟踪的项目，选择之后点击“确定”，则保存我们所选择的内核类型。点击“保存”，则将我们文件诊断的日志保存下来；点击“退出程序”，则退出文件驱动诊断台。点击“查看”，会有一些设置显示的格式和显示的内容，“显示所有进程”，就会显示当前运行的所有进程。点击“工具”，选择“过滤条件”，弹出“设置过滤条件”的对话框，可以分别在“跟踪哪些后缀的文件”、“跟踪哪些程序”、“不要跟踪一下程序”、“跟踪哪些操作类型”所对应的文本框中设置我们的条件，点击“确定”，就保存退出，“清空”就清空输入内容，“取消”就不保存退出。点击“清空所有行”，就会清空控制台所有的记录，“跟踪所有信息”就会跟踪下面所列举出来的要跟踪的进程，“停止所有跟踪”就会停止所有的跟踪的进程。如图 8.16。

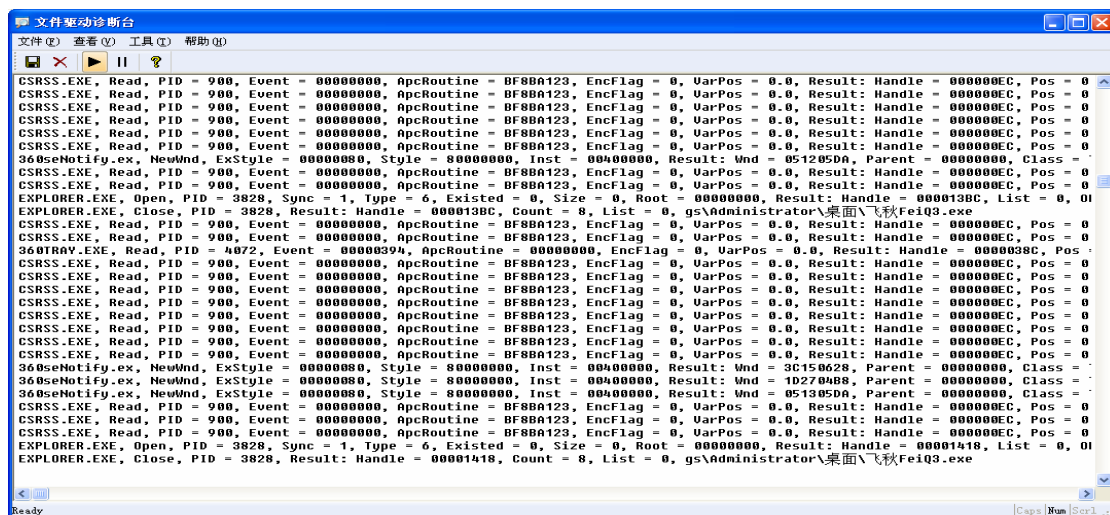


图 8.16

3) 明文邮件调试信息

点击“明文邮件调试信息”菜单之后，弹出“恒隆加密系统”的对话框，点击“确定”后，退出重启 Outlook 或 foxmail，就可以开始调试跟踪发送邮件。发送带加密附件的邮件后，会在桌面产生 wwmail.txt 文件，我们可以根据这个文档来分析邮件发送中所出现的一些问题。如图 8.17。

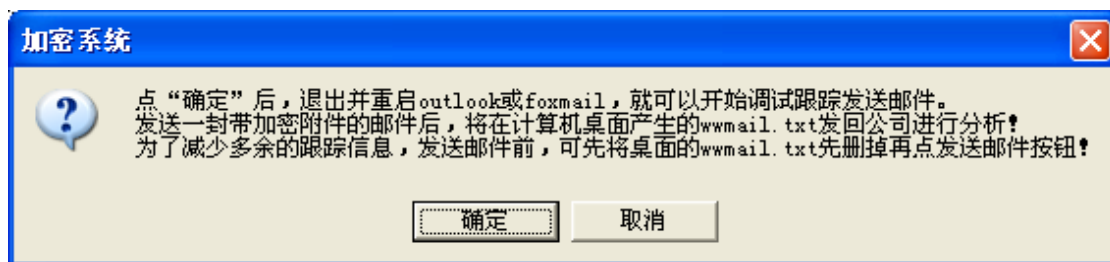


图 8.17

4) 允许屏幕录制

点击“允许屏幕录制”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“是否确定设置本地硬盘可以进行写操作”对话框，点击确定之后，我们就可以允许屏幕录影了。如图 8.18。



图 8.18

5) 允许修改驱动文件

点击“允许修改驱动文件”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务端地址，点击“OK”，登录到服务端，弹出“是否确定设置本地硬盘可以进行写操作”对话框，点击确定之后，我们就可以允许对系统中的文件进行修改的操作了。如图 8.19。



图 8.19

6) 允许离线维护加密策略

点击“允许离线维护加密策略”菜单之后，弹出“设置本地可保存”对话框，在文本框中输入加密系统中申请的离线维护授权号，点击“确定”后，就可以设置本地可保存文件，并可以直接修改加密策略等问价。如图 8.20。



图 8.20

7) 暂停加密内核

点击“暂停加密内核”菜单之后，会弹出“程序启动密码”对话框。此功能一般为软件服务商使用。如图 8.21。

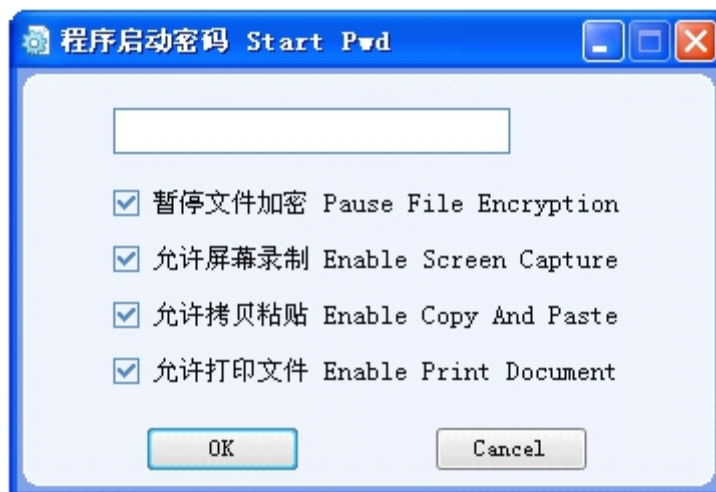


图 8.21

8) 设置另存解密目录

点击“设置另存解密目录”菜单之后，弹出“登录恒隆加密服务器”对话框，输入用户帐号、用户密码和服务器地址，点击“OK”，登录到服务端，弹出“设置解密文件”对话框，左边的文本框输入应用程序名称，右边输入保存不加密的文件或目录，点击“确定”之后，就可以将解密的文件放在我们自己特定指定的目录或者文件格式。如图 8.22。

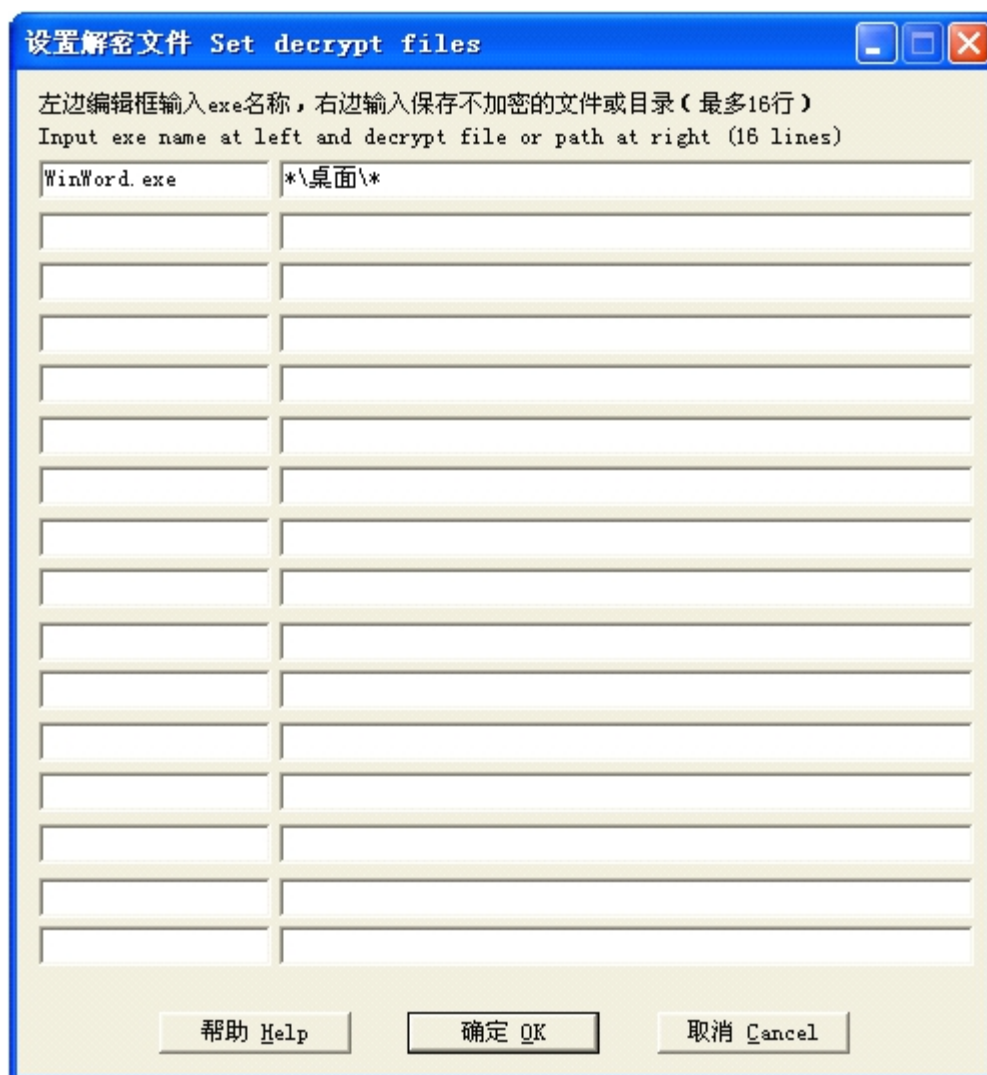


图 8.22

9) 查看在线用户

点击“查看在线用户”菜单之后，弹出“在线用户”的对话框，在对话框的列表中，会显示在线的用户信息，包含用户帐号，IP 地址、Windows 用户、登陆时间、网卡地址。点击“刷新”，可以刷新用户列表。如图 8.23。

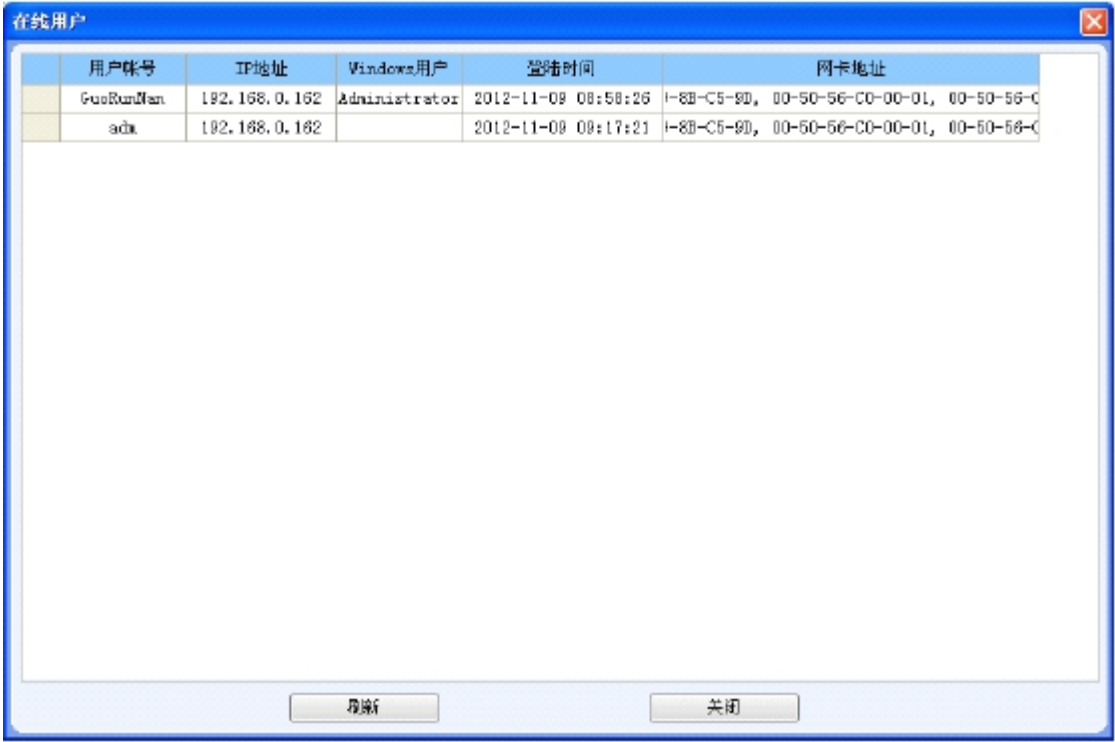


图 8.23

10) 查看用户日志

点击“查看用户日志”菜单之后，弹出“用户日志”对话框。在对话框中，我们可以看到用户对系统的一些操作日志。“用户”单选框中，我们可以选择所要查看日志的用户；“操作类型”单选框中，我们可以选择操作类型；“备注”单选框中，我们可以选择操作的条件；“开始时间”文本框中，我们可以选择所要查看的开始时间（精确到秒）；“结束时间”文本框中，我们可以选择所要查看的结束时间（精确到秒）。下面的列表就会显示出用户的操作日志。点击“查询”，我们可以按照上述条件，来查询用户操作日志；点击“清空条件”，我们可以将上述所选择的条件清空；点击“查看”，我们可以对某一选项进行查看；点击“Excel”，我们可以将查询的操作记录导出为一个电子表格（Excel）；点击“Text”，我们可以将查询的操作记录导出为一个文本文档（txt）；点击“删除查询结果”，我们可以删除查询的结果；点击“删除全部”，我们可以将所有的日志全部删除（查询结果仅是所有的日志的一部分）；点击“删除冗余记录”，我们可以删除冗余的记录；点击“关闭”，关闭对话框。如图 8.24。

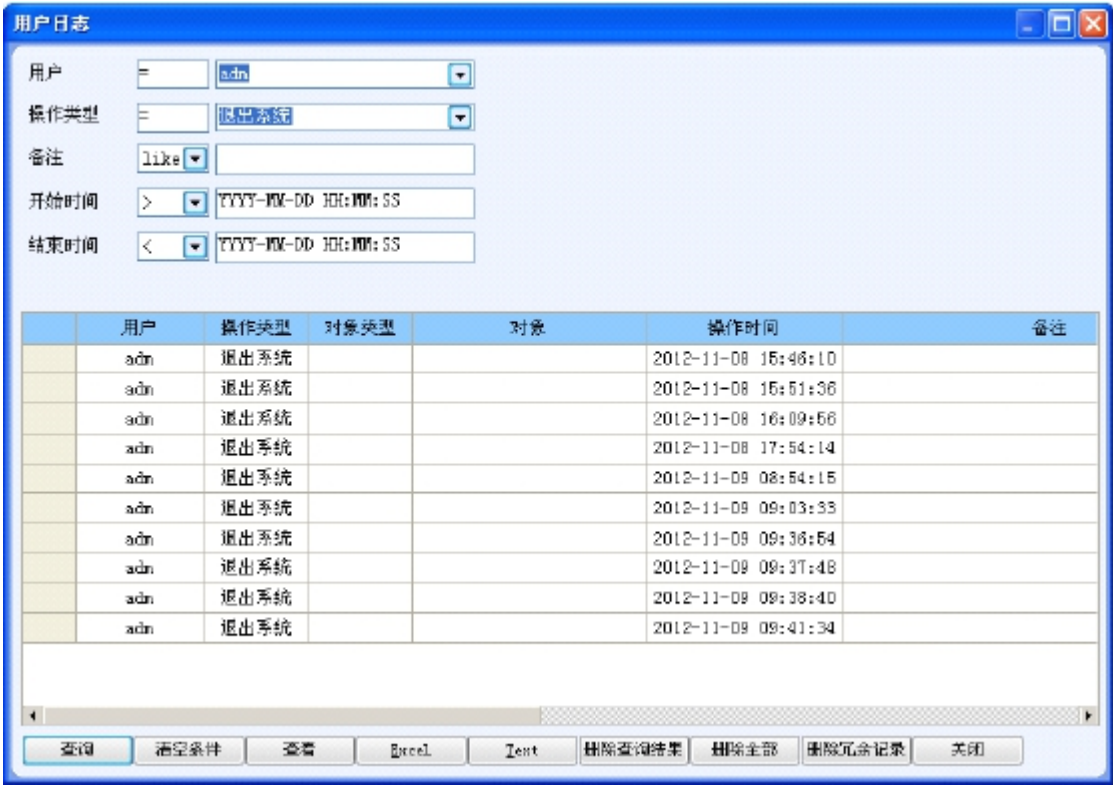


图 8.24

11) SQL 查询工具

点击“SQL 查询工具”菜单之后，弹出“SQL Query”对话框，在文本框中输入查询语句，可以对系统的数据库进行操作，点击“OK”或者“Enter”键可以，查询到所要的查询结果。如图 8.25。



图 8.25

12) 查看本机机器码

点击“查看本机机器码”菜单之后，弹出“查看本机信息”对话框。在对话框中，显示本机的计算机名，IP 地址，机器码和机器码对应的硬件信息。如图 8.26。

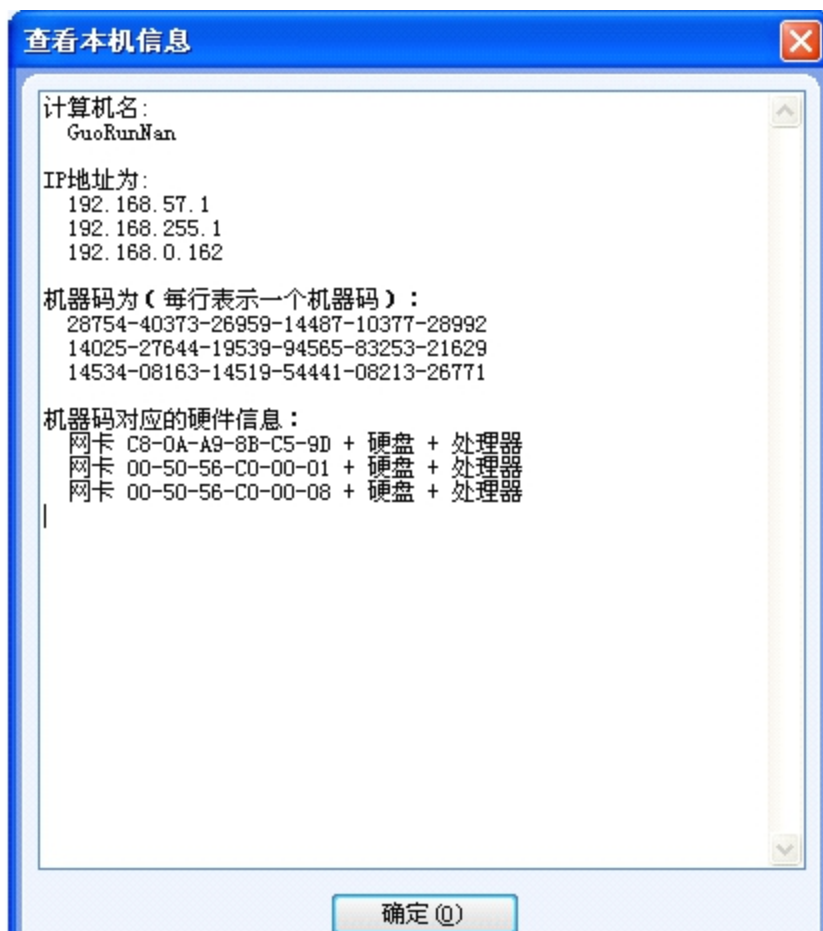


图 8.26

13) 查看服务器信息

点击“查看服务器信息”菜单之后，弹出“服务器信息”对话框。在对话框中，我们可以查看到服务器的信息，包括授权站点数，在线用户数，服务器代号，安装授权号，服务器安装目录。如图 8.27。

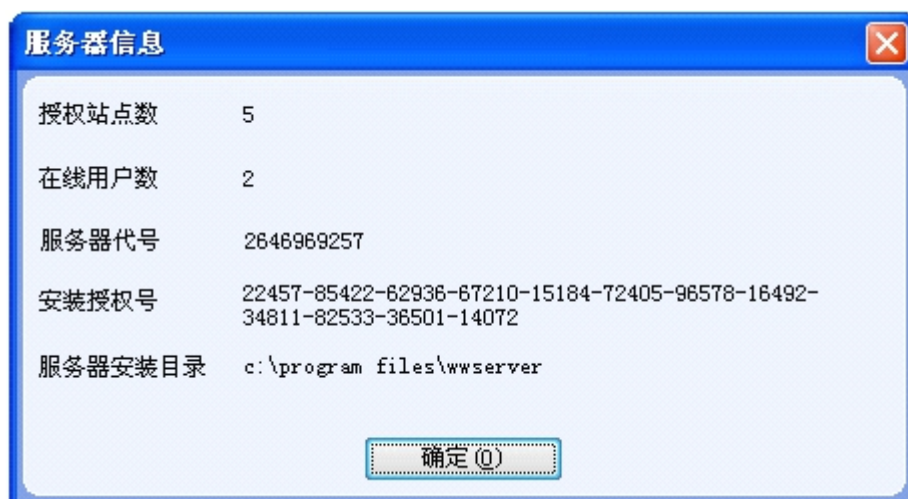


图 8.27