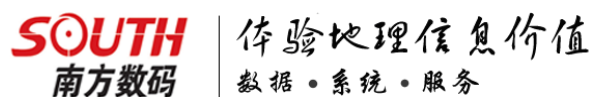


南方金盾网络版 解决方案

广东南方数码科技有限公司



©版权所有 · 广东南方数码科技有限公司

目录

| | |
|--------------------------|----|
| 1. 前言..... | 3 |
| 2. 软件介绍..... | 3 |
| 2.1 软件简介 | 3 |
| 2.2 软件安装与卸载 | 4 |
| 3. 技术方案..... | 5 |
| 3.1 软件部署 | 5 |
| 3.2 支持环境 | 6 |
| 3.3 技术选型 | 6 |
| 3.4 技术框架图 | 7 |
| 4. 内网透明加解密..... | 8 |
| 4.1 安装部署（服务器端） | 8 |
| 4.2 安装部署（客户端） | 9 |
| 4.3 功能说明 | 10 |
| 5 策略编辑器..... | 11 |
| 5.1 全局设置 | 13 |
| 5.2 进程策略编辑 | 14 |
| 5.3 AutoCAD 进程策略示例 | 16 |
| 6. 手动加解密..... | 17 |

1.前言

如今，企业机密信息大多以电子文档的方式存在，而电子文档在方便共享的同时也使得泄密变得容易。

目前电子文档常见的泄密途径有：内部人员出售电子文档以牟取利益、外部人员通过非法拷贝或网络盗取电子文档、人员离职带走电子文档等。

本产品在不影响使用者操作习惯的情况下，实现电子文档的透明加密存储，加密后的文件可以在公司内部正常流通使用，一旦脱离公司网络，文件将无法打开。带文件外出需经公司专人解密或利用加密狗授权，才能正常使用。这样就将企业中的一些核心数据牢牢限定在了本企业中，有效的保证了核心数据的安全。

2.软件介绍

2.1 软件简介

南方金盾网络版为广东南方数码科技有限公司开发的用于内网安全的软件产品。

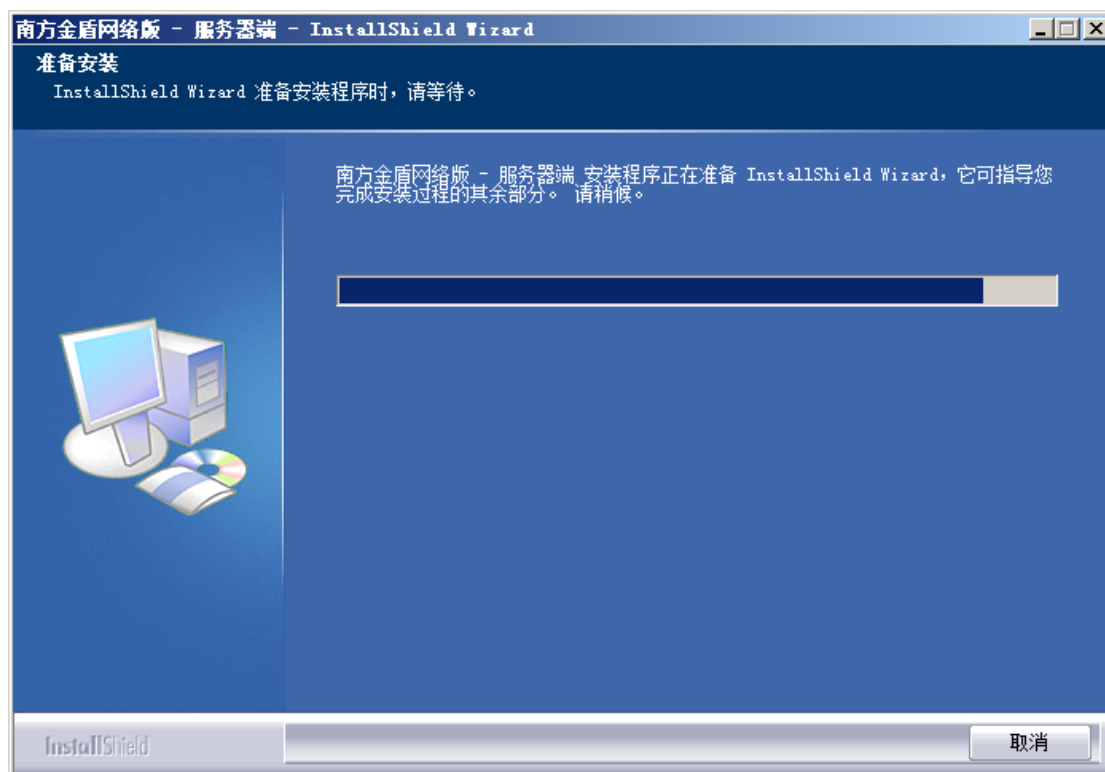
本产品主要采用了文件过滤驱动、透明加解密、多缓冲管理等技术。

本产品的主要功能有：

- 1、实现电子文档的透明加解密，使之在内网可正常使用，出网失效；
- 2、加密策略的自定义及授权进程的细节控制；
- 3、可禁止某些进程的运行（例如 QQ 等）；
- 4、可禁止访问移动设备；
- 5、可禁止访问网上邻居或其他人通过网上邻居访问本机；
- 6、手动单个或批量加解密电子文档；
- 7、用户管理；

2.2 软件安装与卸载

软件的安装分为服务器端安装和客户端安装，安装过程类似，以安装服务器端为例。



同大部分软件安装一样，遵循向导即可完成安装



双击安装包即可完成卸载

3. 技术方案

3.1 软件部署

服务器端和客户端通过 IP 地址进行通讯，局域网 IP 或者外网 IP 只要能够连通皆可进行本产品的部署。

服务器端和客户端可能需要安装 VC++ 2008 可再发行包 (Microsoft Visual C++ 2008 Redistributable Setup)。



Microsoft Visual C++ 2008 Redistributable Setup

3.2 支持环境

支持 NT 架构的系列操作系统 (32/64 位)：

- Windows7.
- Windows 2008 .
- Vista.
- Win2003.
- WinXP.

支持的应用软件：

- 编程类： VC6/VB/Delphi/VS2003/Vs2005
- 办公类： MS Office 系列办公软件(Word/Excel/PowerPoint)、记事本软件

(NotePad)

- 制图类： Photoshop 系列、CorelDraw 系列 、画图 (Mspaint)
- 二维 CAD 类： AutoCAD2004、AutoCad2006、基于 AutoCAD 二次开发的圆方 BtoCAD 等
- 三维 CAD 类： Pro/E、CATIA、Protel 99E 等

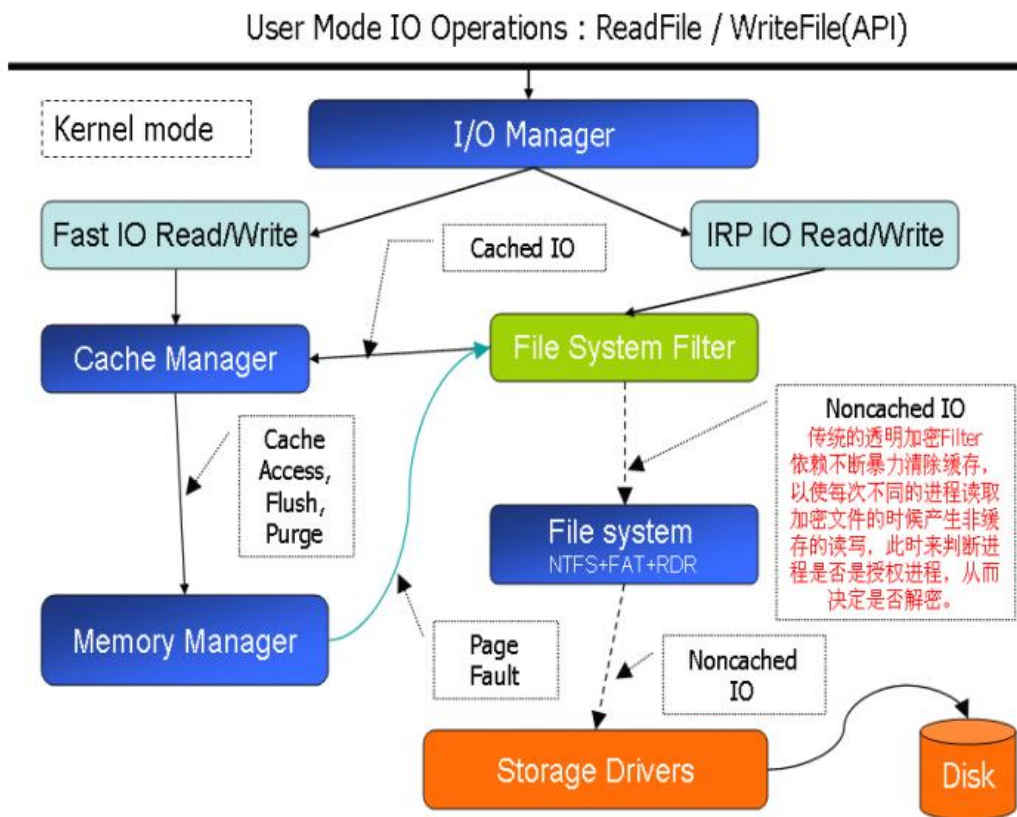
未列出的应用软件可以通过自定义策略来支持。

3.3 技术选型

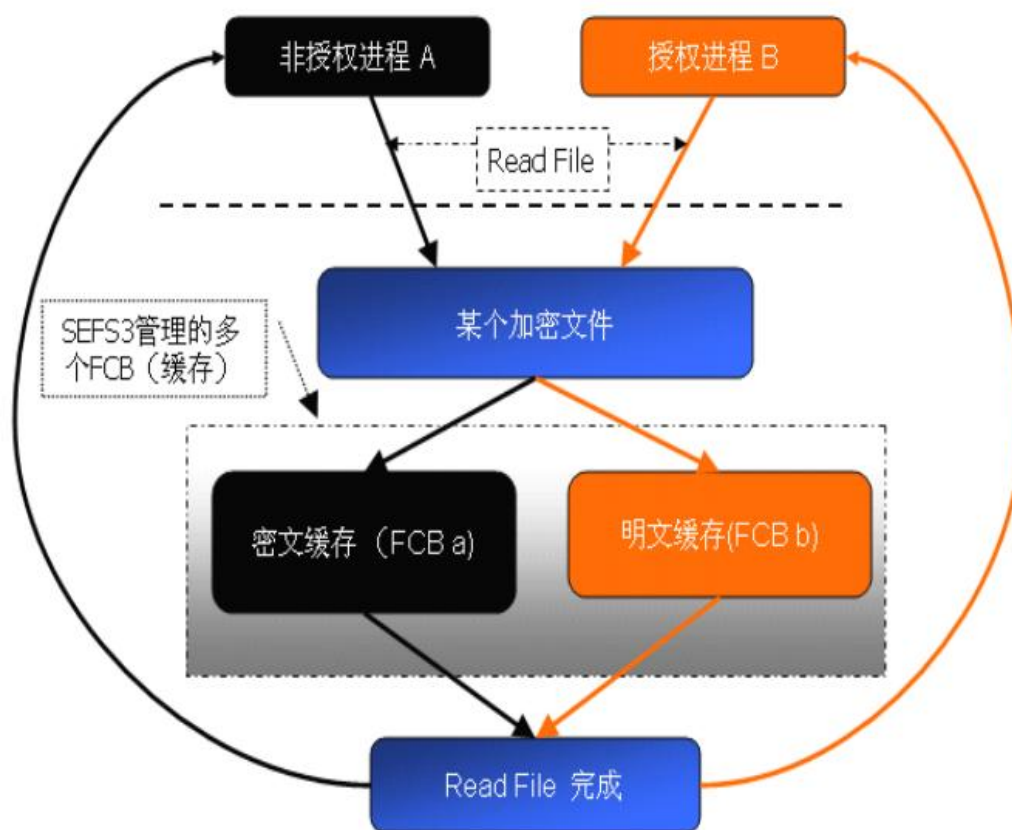
本产品的开发环境为： Visual Studio 2008 (C++)。

主要采用的技术有：文件过滤驱动、透明加密、多缓冲管理

3.4 技术框架图



透明加解密结构图

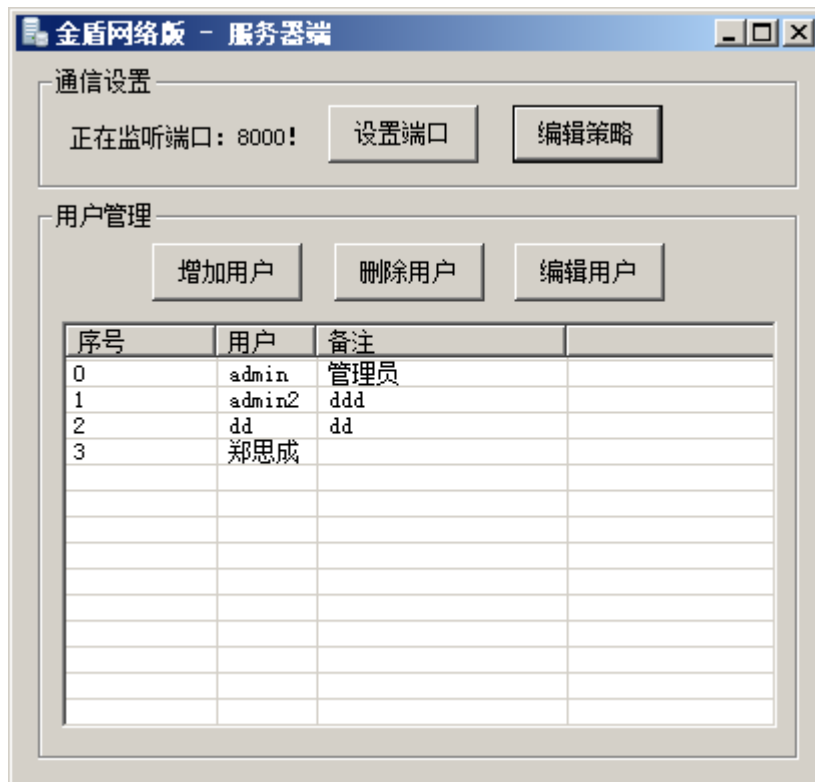


多缓冲管理

4. 内网透明加解密

4.1 安装部署（服务器端）

在服务器上安装“南方金盾网络版 - 服务器端.exe”。安装后软件界面如下：



服务器端可进行用户和策略的集中管理，以及端口号的设置。

4.2 安装部署（客户端）

在客户机上安装“南方金盾网络版 - 客户端.exe”。安装后软件界面如下：

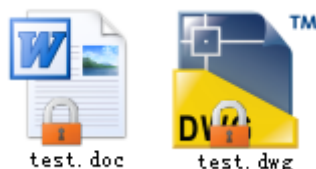


设置服务器的 IP 地址和端口号，输入用户名和密码即可登录并启动客户端。

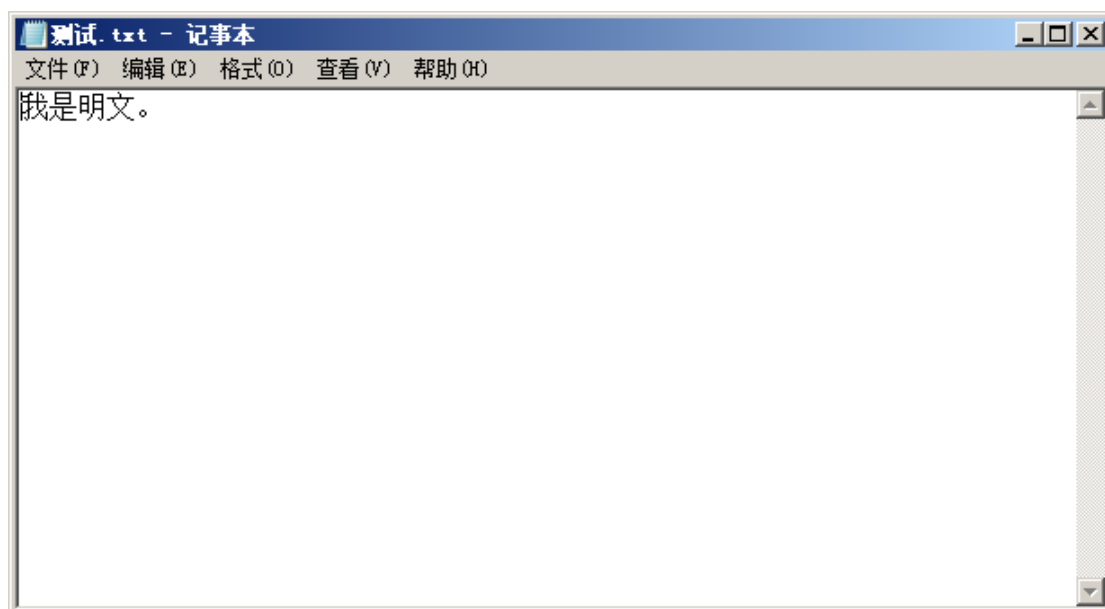
4.3 功能说明

软件部署完以后即可像之前一样正常的打开保存电子文档，加解密过程都自动完成。

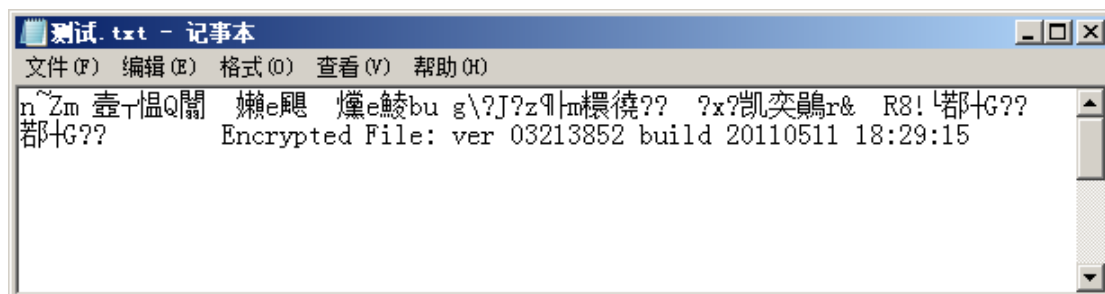
可启用外壳扩张（加密文件的图标上会显示一把小锁）。



启用了外壳扩张之后的加密文件的效果

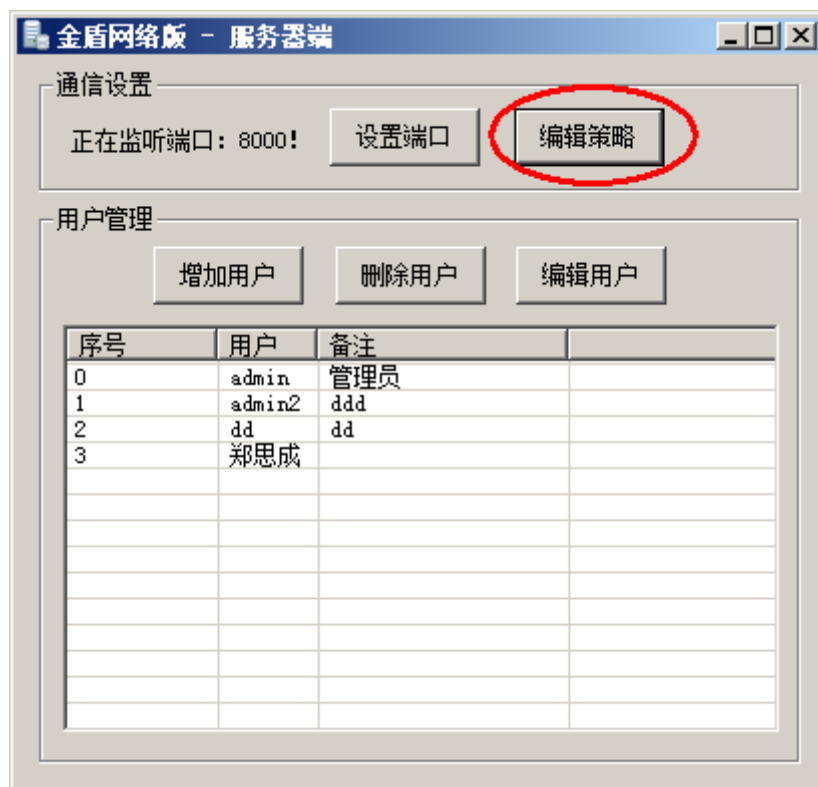


启动客户端后打开加密文件看到的内容



停止客户端后打开加密文件看到的内容

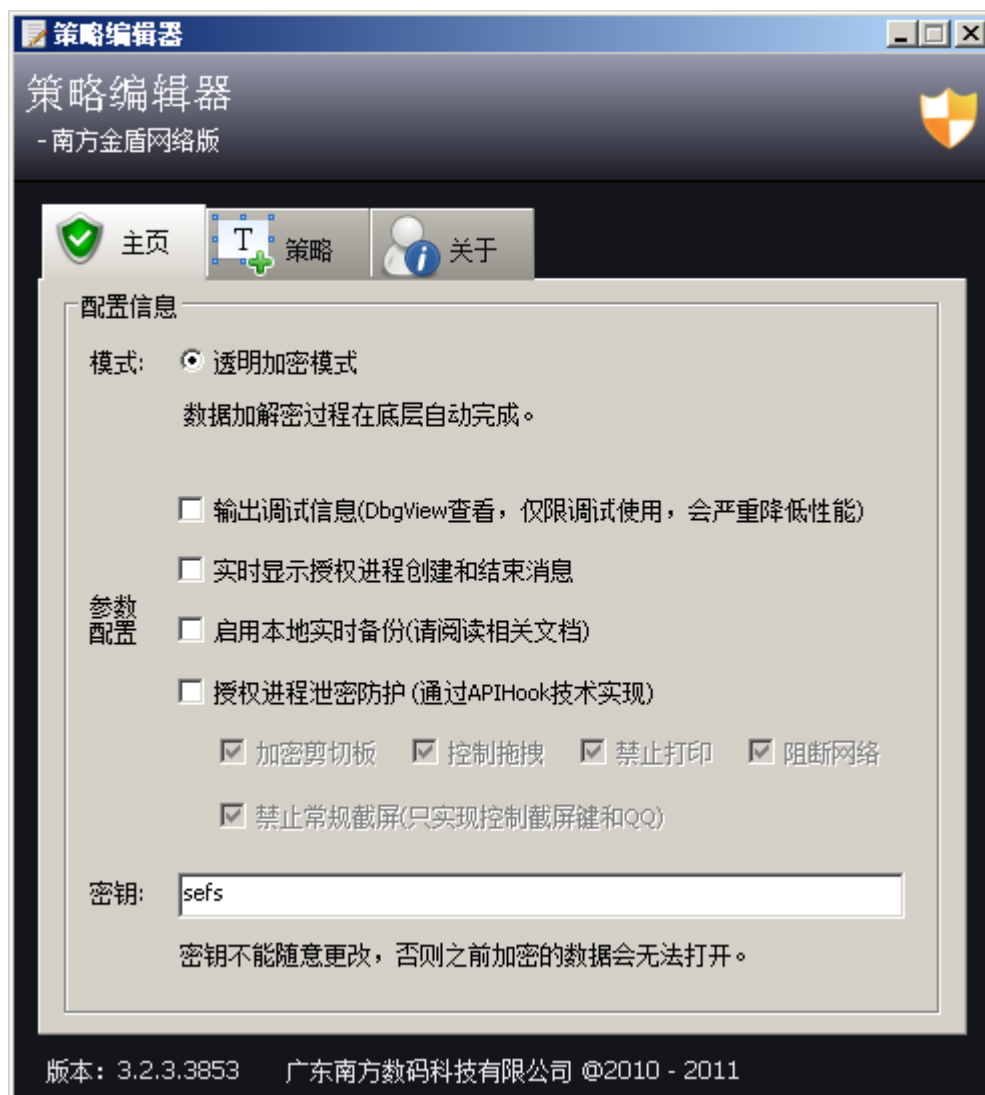
5 策略编辑器



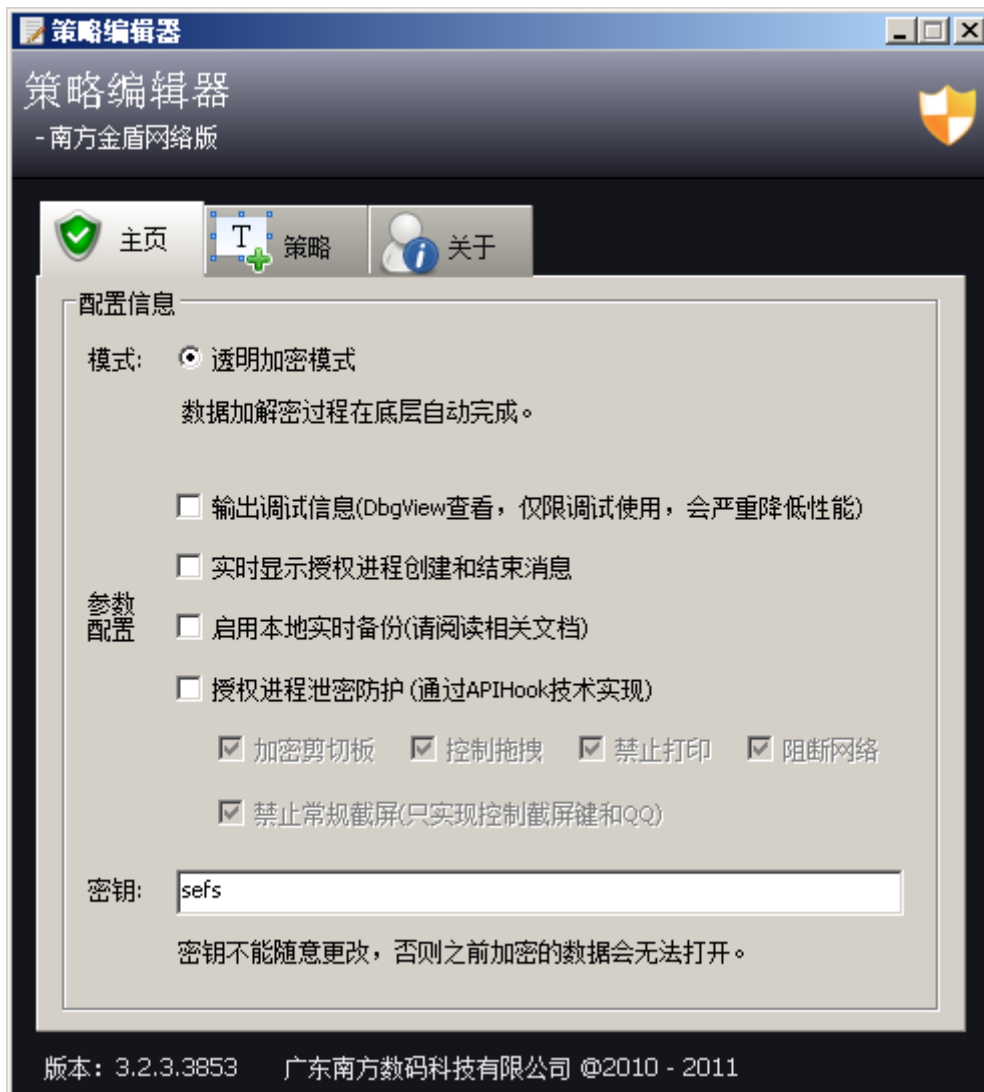
单击服务器端的“编辑策略”按钮打开策略编辑器。

服务器端进行的策略编辑对所有登录用户均有效。

如果客户已经登录，则下次启动客户端的时候新的设置才会有效。



5.1 全局设置

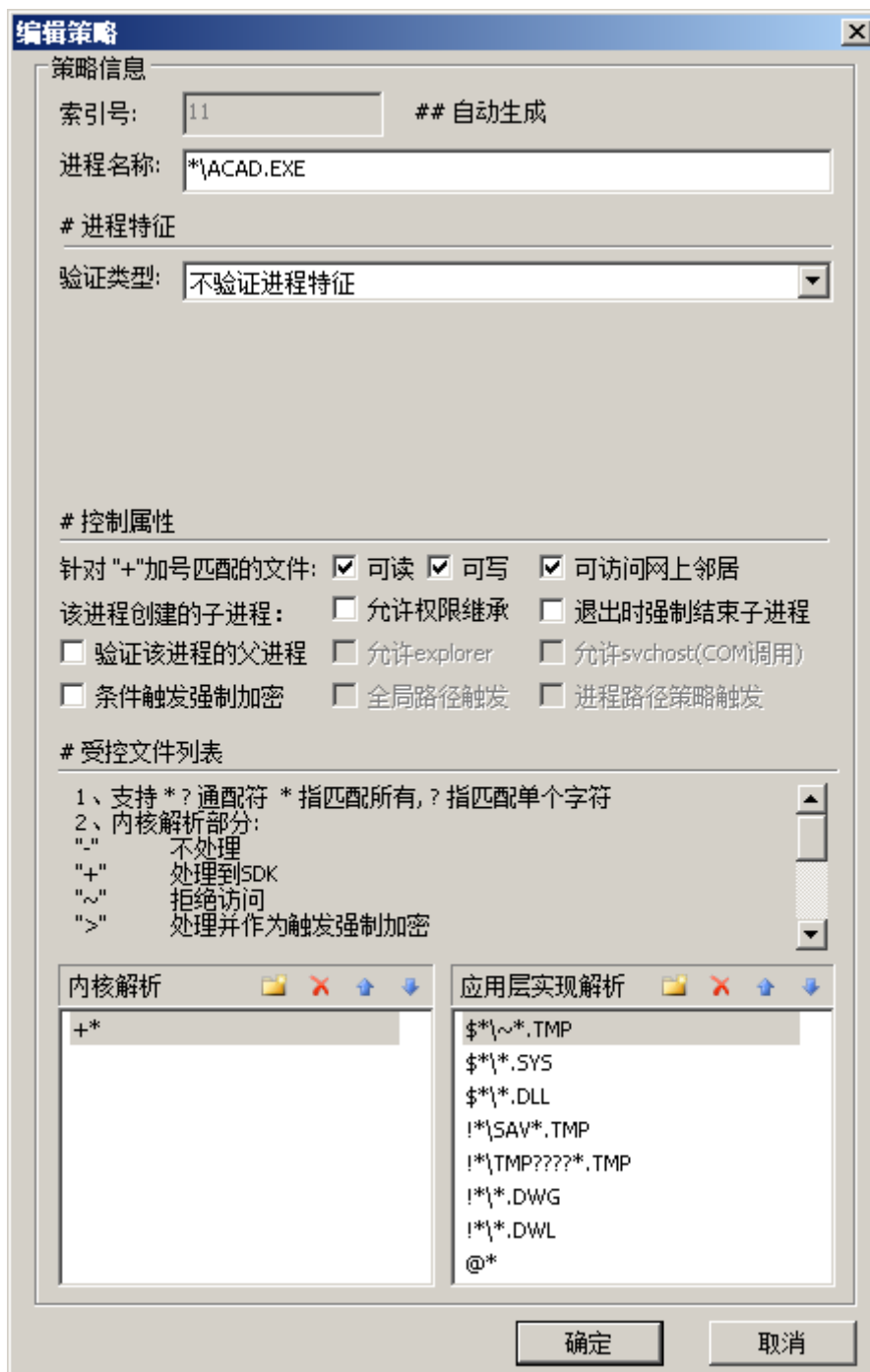


可开启授权进程的泄密防护, 设置密钥等。

5.2 进程策略编辑



策略编辑器主界面



针对某个授权进程进行更为详细的设置。

例如：

可设置某个进程（例如 AutoCAD）无法打开 dwg 文件；

可设置某个进程（例如 AutoCAD）能打开 dwg 文件，但无法修改；

可设置某个进程（例如 AutoCAD）能打开和修改 dwg 文件，但无法保存到网络存储器；

以下是更为详细的策略编辑说明：

1、支持 * ? 通配符 * 指匹配所有, ? 指匹配单个字符

2、内核解析部分：

"_" 不处理

"+" 处理到 SDK

"~" 拒绝访问

">" 处理并作为触发强制加密

3、加密实现解析：

!" 需要加密, 比如 txt doc 等

"&" 加密并且备份, 通常是授权进程的常见后缀 *.doc

"@" 写操作欺骗

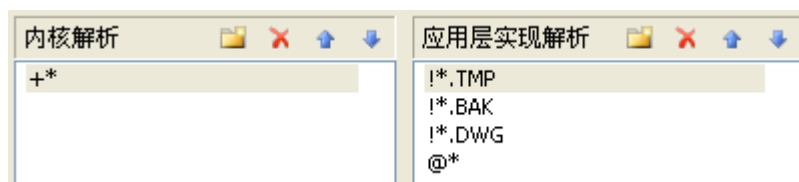
"#" 将文件镜像到指定文件

"\$" 写 PE 文件检查

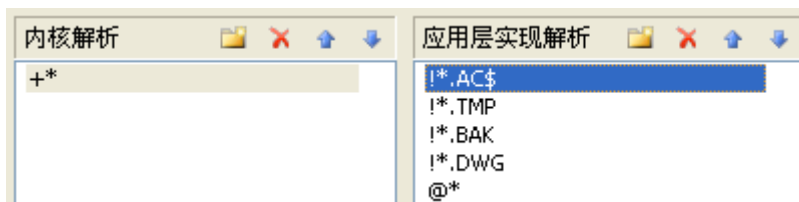
"%" 只有开始写才会加密

5.3 AutoCAD 进程策略示例

示例一（DWG 可正常读写，但是无法导出 DXF）：

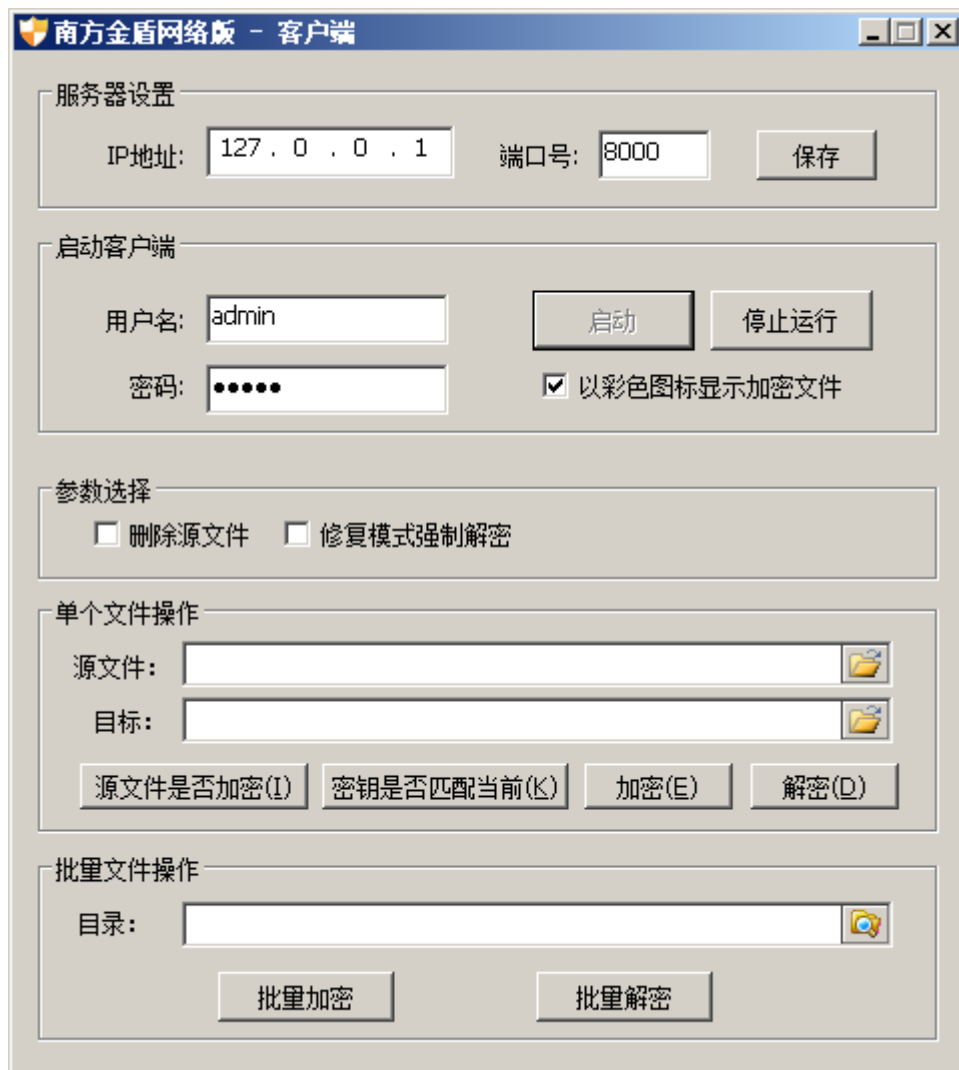


示例一（DWG 可正常读写，可导出 DXF，但仍自动加密）：



6. 手动加解密

当用管理员的身份登录成功后，会自动展开管理员工具以手动进行文件的加解密操作。



用管理员的账号登录之后的客户端



非管理员登录后的客户端

可检测源文件是否是加密了的文件。

可批量进行文件的加密与解密。