

敏感数据防护系统 技术白皮书

(CDPS V2.0)



广州江南科友科技股份有限公司

1	系统简介.....	3
2	敏感数据防护系统设计思想.....	4
2.1	目标.....	4
2.2	原理.....	4
2.3	系统逻辑拓扑图.....	5
2.4	系统特点.....	6
2.4.1	设置严密.....	6
2.4.2	安全可靠.....	6
2.4.3	适应面广.....	6
2.4.4	使用方便.....	7
2.4.5	适用宽泛.....	7
2.4.6	管理简单.....	7
3	敏感数据防护系统功能介绍.....	8
3.1	服务端程序.....	8
3.2	客户端程序.....	9
4	敏感数据防护系统策略.....	10
4.1	概念.....	10
4.2	涉密策略.....	10
4.3	控制策略.....	11
4.4	明文邮箱策略.....	18
4.5	角色.....	20
4.6	策略组.....	20
5	敏感数据防护系统技术参数.....	22
5.1	网络环境要求.....	22
5.2	客户端延时.....	22

1 系统简介

江南科友敏感数据防护系统（Classified Data Protection System）结合了多年的数据安全经验，为金融、公共事业、互联网、运行商等设计开发的敏感数据防护系统，通过对计算机文件的加密保护实现重要文件不被泄密。

随着计算机应用的普及，各行业数据安全问题越来越突出，数据安全是包括两方面内容的：

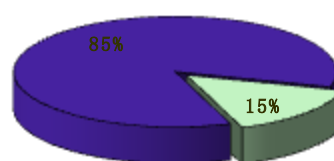
- 数据存储的可靠性问题
- 数据内容的私密性问题

可靠性是指一旦发生灾难性的事件，数据的所有者是否还能够将数据的内容重现回来。这涉及到计算机数据备份、存储介质的电磁性能、机械性能、化学性能等等方面。私密性是指数据的所有者是否能够保证数据的内容不会被传播到不可信任的范围中去。江南科友敏感数据防护系统就是解决数据保密问题。

数据的保密，又存在两个不同层次的信任模型：外部安全模型和内部安全模型。前者认为，所有对数据的威胁皆且仅来自外部，所有内部用户都是可以信任的。而后者认为，威胁不仅可以来自外部，而且可以来自内部；无论是内部用户还是外部用户，都是不可信任的。

显然，内部安全模型是更符合社会现实。

由于内部人员熟悉文件的存放，还可以接触到密级高、范围广的文件，所以一旦发生内部人员故意泄密事件，其危害程度是大大超过外部人员的盗取（例如黑客攻击行为）。可见，数据私密性的保护要内外兼修，甚至要防内重于防外。



■ 来自网络内部的威胁
□ 来自网络外部的威胁

2 敏感数据防护系统设计思想

2.1 目标

江南科友敏感数据防护系统(Classified Data Protection System, 以下简称“CDPS”)总的目标是:统一安全性和方便性的矛盾,即在保障数据严密的安全性的前提下,充分保留数据使用的方便性。

具体地可以细化为以下几条:

- 特定的文件(并非所有的文件)在生成(或保存)之时,就应该被加密,且加密要由计算机自动地进行,不能依靠人工执行;
- 文件的加密和解密,不能依赖人工设定的密码或口令;
- 被加密的文件在被涉密计算机打开之时,就应该被解密,且解密要由计算机自动地进行,无需人工操作,文件的使用者也无需知道“密码”;
- 被加密的文件在被非涉密计算机私自打开之时,应该报错、显示乱码或者其他方式以阻止文件内容被传播;
- 文件如果要被外部人员(或非涉密计算机)所读取,应该由专人来审查并解除其保密状态。

这些目标,可以归纳为十六个字:“敏感数据,强制加密;于内无碍,对外受控”。

2.2 原理

文件泄密有两个步骤:① 文件本身被非法地流传到可信任范围之外;② 流传出去的文件被不可信任的人读懂。以前众多的保密系统都是侧重于在第一步进行防范。如果将保密的希望寄托于文件不会被传出去,那么正如前文所述,从现在的眼光来看已经实属不易,从发展的眼光来看更将防不胜防。

CDPS 着眼于第二步的防范。我们认为,造成计算机数据泄密的根本原因是文件格式的通用性,即电子文档在不可信任的计算机上显示的内容和可信任的计算机上一样。

CDPS 需要在每一个涉密计算机上安装客户端程序。这个客户端程序会从服务器得到密钥(类似于人工设定的密码),而这个密钥不会也无需被涉及计算机的使用人员所掌握。

广州江南科友科技股份有限公司 地址(Add): 广州市萝岗区科学城科学大道 162 号创意大厦 B3 区主楼 2 层

邮编(P.C): 510663 电话(Tel): (86 20)28068388 传真(Fax): (86 20)28068389 服务热线: 4008001234

2.4 系统特点

CDPS 软件采用了一些独特的技术和思路，形成了很多自己的特色，从而使其成为一款优秀的计算机数据保密系统。这些特色可以归纳为六点。

2.4.1 设置严密

- 指定类型文件打开、移动、拷贝等操作过程中被自动加密；
- 客户端安装部署完成后，指定类型文件强制扫描加密；
- 客户端可设置为，使用者不可见、不可卸载、不可停止；
- 只有在服务端授权后的客户端才能本地解密文件；
- 加解密文件时自动向服务端写日志；
- 禁止任何非法程序访问密文；
- 非法用户端试图访问服务器时自动拒绝、报警；
- 服务端操作需要合法登录。

2.4.2 安全可靠

- 服务端提供与硬件相关的全球唯一密钥，不可复制；
- 密钥不在硬盘上出现；
- 对文件加密采用标准和全文加密技术；
- 密文中不带密钥，从密文中得不到文件破解的任何信息；
- 程序提供多种加密算法，对文件加密时，随机选取加密算法；
- 提供用户增强自定义密钥功能。

2.4.3 适应面广

- 支持对所有 Windows 文件加解密；
- 用户可自定义加密程序和文件类型；
- 可设置部门之间的加密，也可以设置部门之间密文共享，并且可设置密级权限，使得部门内部控制、交流、管理密文，更加协调方便；
- 免去增加应用程序需要开发功能的烦恼；

- 免去由于应用程序升级带来的软件升级烦恼。

2.4.4 使用方便

- 客户端对使用者完全透明；
- 对文件操作过程中自动加密，合法打开文件自动解密。加密时不需要指定加密文件，解密时不需要输入密码；
- 密文在加密环境许可的范围内不需要做任何处理，交流无阻。
- 提供移动办公的商务授权策略管理；
- 所有管理都设在服务端，不需要到每个客户端去操作；
- 图形化界面，配合文本和视频教程，通俗易懂、方便易用。

2.4.5 适用宽泛

- 仅与操作系统相关，而与应用软件无关；
- 用户可以方便地将任何类型的文件自定义为“敏感数据”。

2.4.6 管理简单

- 客户端加密策略、客户端加入、离线授权、脱机使用，等设置都在服务端进行；
- 只要修改涉密策略，更新在线用户立即生效；
- 提供备用服务器，主服务器发生故障时自动访问备用服务器；
- 审批解密采用网络通讯在线进行；
- 海量日志管理功能。

3 敏感数据防护系统功能介绍

3.1 服务端程序

服务端程序运行于 CDPS 服务器上，用于管理各种策略。服务器在整个系统中起到的主要作用如下：

- 进行软件注册；
- 管理系统密钥，并向合法的计算机提供这个密钥（密钥是不可见的）；
- 管理（新建、删除、制定、命名、分发）各种策略；
- 对合法的计算机（包括涉密终端、解密程序）进行登记管理；
- 对涉密终端的密文密级、用户组权限授权设置；
- 对便携式涉密终端进行离线授权；
- 设置各种系统参数；
- 记录解密日志、打印日志、系统日志；
- 处理客户端请求。

在 CDPS 服务器上，从 Windows 中的“开始”菜单或者用其他快捷方式可以启动 CDPS 服务端程序。CDPS 服务端程序启动之后，首先显示当前状态，其界面如图所示：



3.2 客户端程序

客户端是运行于各个涉密终端上,用于计算机之间对指定数据自动加密和解密的程序。

客户端程序对使用者来说是完全透明的,会随 Windows 操作系统一起启动,运行的一些参数都是由服务器通过分发策略的方式来指定的。

客户端在生成以下文件的时候,所得到的文件会被自动加密:

- 用其涉密程序生成的任何后缀(例外后缀除外)文件;
- 用其涉密程序生成的指定的后缀文件;

在涉密终端上的以下操作得到的文件,不会被CDPS自动加密,文件将是明态的:

- 用非涉密程序生成一个非涉密后缀的文件;
- 用涉密程序生成一个以“涉密程序”的“例外后缀”为后缀的文件。

4 敏感数据防护系统策略

4.1 概念

CDPS 系统可以对每一台涉密终端实现不同的管理。这些都是通过策略来实现的。所谓的“策略”，就是由系统管理员针对每一个涉密终端做出的个性化设置，这些设置回答了以下三类七个问题：

关于文件加解密

1. 由哪些应用程序生成的文件需要自动加密？
2. 哪些类型（即文件后缀名是什么）的文件需要自动加密？
3. 哪些应用程序能够打开密文文件？

关于控制访问

4. 涉密终端与服务器连接状态的检查周期是多长时间？
5. 对于涉密的打印行为，是否允许？
6. 对于涉密的“复制-粘贴”行为，是否允许？

关于明文邮件

7. 向哪些电子邮件账户发送密文附件，对方可以直接收到明文？

由于对用户不同部门而言，所谓的“敏感数据”也可能是不同的。例如对于技术部而言，各种 CAD 绘制的图形文件就是敏感数据；而对财务部而言，各种报表可能才是需要保护的。

CDPS 系统的特点之一就是允许用户的系统管理员自行对每一个涉密终端定义“敏感数据”。这便是通过文件策略来实现的。

每一个文件策略都包括两个名单：涉密应用（或称“涉密程序”）和涉密后缀。

4.2 涉密策略

涉密策略是用于定义客户端涉密范围的策略。它是 CDPS 加密系统中最重要策略。它指定了客户端哪些程序和类型是需要加密的，其它程序是不加密的。

涉密程序是 CDPS 系统非常重要的一项定义。如 MS Word 需要加密，则其程序

广州江南科友科技股份有限公司 地址(Add)：广州市萝岗区科学城科学大道 162 号创意大厦 B3 区主楼 2 层

邮编(P.C)：510663 电话(Tel)：(86 20)28068388 传真(Fax)：(86 20)28068389 服务热线：4008001234

Winword.exe 就是涉密程序。根据要求，可将涉密程序定义为产生的所有文件加密或者是指定的类型加密。

通过涉密策略的灵活定义，可满足不同用户不同加密需求以及集成要求。

为了使涉密策略定义更加精准，江南科友科技股份有限公司提供了现成的若干涉密策略定义，此类策略类型为“厂商定义”如图所示。



“厂商定义”策略只有江南科友 CDPS 技术人员才能修改，一般用户无法修改。用户只能修改自定义策略。

江南科友科技股份有限公司将根据实践不断完善“厂商定义”策略，并在定期汇报给用户。需要升级和更新的用户，联系江南科友技术人员获取相关策略即可进行策略升级。

4.3 控制策略

控制策略是用来控制客户端操作的一组策略。包括“加密控制”、“连接控制”、“涉密打印”、“操作控制”、“安全控制”、“设备控制”、“申请控制”等多种控制方式。控制策略编辑界面（如图所示）：



加密控制：CDPS 提供三种加密方式，其含义如下：

强制加解密：涉密终端将根据文件策略自动加解密文件。

仅控制密文：涉密程序可以打开密文，并且操作该文件后仍为密文。如果操作其他或者相同类型的明文时，文件不会被加密仍是明文。如涉密程序为 word，如果 word 打开了一个密文，则即使另外打开一个明文，明文保存后仍然是明文，密文保存后仍然是密文。当然，此时无法从 word 密文中拷贝内容到明文中。同时，密文在拷贝或通过邮件发送出去时仍然为密文。

能打开不加密：涉密终端可以用涉密程序打开加密过的文件，但涉密程序不会将生成的文件自动加密。也就是说打开密文后，另存的新文件是明文。此策略必须同时定义相应的涉密程序，否则也无法打开密文。由于此策略的特殊性，一般只用于领导，选择时请注意不要误选。

连接控制：连线方式共有四种其含义如下：

仅启动时访问服务器：客户端只要启动时访问一次服务端取策略，然后不依赖于服务端便可运行。这种策略是最常见的一种策略，一般用于台式机的控制。

定时连接：让客户端定时访问一次服务端，以验证其仍然在线。一般用于笔记本电脑的连线控制。防止其不断电拿走机器，在外面仍然可以打开密文。

断线关机：同定时访问，但如果不能连接服务端，CDPS 客户端会自动将涉密终端关机。

脱机使用：就是允许涉密终端在未连接到服务器时仍然可以打开密文。一般用于网络

广州江南科友科技股份有限公司 地址(Add)：广州市萝岗区科学城科学大道162号创意大厦B3区主楼2层

邮编(P.C)：510663 电话(Tel)：(86 20)28068388 传真(Fax)：(86 20)28068389 服务热线：4008001234

状况极差的情况。“时间控制”选项用于控制可最长脱机使用的时间。

操作控制项目：操作控制项目的含义如下：

禁止将涉密内容拷贝到非涉密程序：就是不能将涉密程序中的内容拷贝到非涉密程序中去。但不影响涉密程序与涉密程序之间的拷贝，也不会影响非涉密程序将内容拷贝到涉密程序中。

禁止键盘和程序截屏：禁止 PrtSc 键或其它程序拷贝屏幕。仅当有涉密程序打开时有效。

禁止非涉密程序 OLE 插入涉密内容：禁止非涉密程序以 OLE 的方式链接或者嵌入涉密内容。

禁止删除密文：所有已经加密过的文件不能被删除。此选项在正常使用时不要勾选，它会影响到一些涉密程序的正常使用。仅当某员工要离职，且有可能破坏其文件时使用。

设备控制：设备控制选项的含义如下：

禁止 USB 存储设备使用：禁止插入 U 盘或移动硬盘。但不会影响 USB 打印机或鼠标等非存储 USB 设备的使用。

禁止光驱设备：禁止光驱的播放和刻录。

打印控制：打印控制选项的含义如下：

禁止涉密打印：禁止涉密程序打印文件，不管是不是打印密文。

打印时截屏：涉密程序打印文件时，截屏保存当前文件内容。

备份打印文件：自动将打印的文件备份到服务器。目前只针对 doc/xls 文件。

安全控制：安全控制选项的含义如下：

禁止进入安全模式：系统不能进入安全模式，以防止用户在安全模式下破坏客户端程序。注意：禁止进入安全模式仅对系统盘为 NTFS 格式有效。并要将注册表中 CDPSFilter 服务项的 start 值设置为 0。

禁止离线时使用涉密程序：当客户端未启动时，涉密程序无法启动。用于防止个别员工为躲避加密，拔掉网线不让客户端启动而干私活。

申请控制：申请控制设置界面（如图所示）页选项含义如下：

自动加密申请解密后的文件：这是一项减小泄密风险的设置。解密后的文件在一定时间内或者是重启客户端后必须再次被加密，以保证文件的安全。

扩展控制：扩展控制是用来补充控制客户端操作的一组策略。包括“备份控制”和“其

他”两种控制方式。控制策略编辑界面（如图所示）。



客户端的自动备份发生在对涉密后缀文件进行重写时。非涉密后缀类的文件的重写不会自动备份。因此，自动备份的效果应跟涉密策略一起设置。

备份控制：备份控制选框中有三种备份方式。其含义如下：

不自动备份：客户端不自动备份。该类备份策略也不需要进行任何其它设置。

备份到本地：客户端产生的备份放在本机某个目录。还需要对本地备份页的相关选项进行设置。

备份到网络：客户端产生的备份放在指定的备份服务端。还需要对“网络备份”页进行相应的设置。

备份方式：可将备份文件备份成明文，也可以备份成密文。当设置成本地备份时，请不要将备份方式设置成备份成明文。

当前目录保存备份：自动备份时，将最新的备份文件保存一份在密文所在的目录。此备份文件的后缀为*.CDPSbak，且为隐藏文件。

本地备份：本地备份的设置界面如图所示。仅当备份策略为“备份到本地”时才需要设置。



备份目录：备份文件备份的目录，注意，所写盘符必须要客户端机器上存在，否则将不能自动备份。

备份文件管理：“不分目录，同名覆盖”表示所有备份文件都备份到备份目录下，相同名称的文件将会自动覆盖掉。“按日期分目录”是指每天建立一个新目录，每天备份的文件保存在该目录下，同名文件仍然会覆盖。“保持文件原路径”是指备份时将文件原路径直接转换保存到备份目录，不会覆盖。

备份文件个数：指保存备份文件的数量。最少为 2 个。备份文件会以“n_原文件名”的形式命名，其中 n 越小表示是越新的备份。当有新备份时，会将新备份文件命名为“1_原文件名”，其它老文件自动后移。

网络备份：网络备份设置界面如图所示。

仅当备份策略为“备份到网络”时才需要设置网络备份页选项。

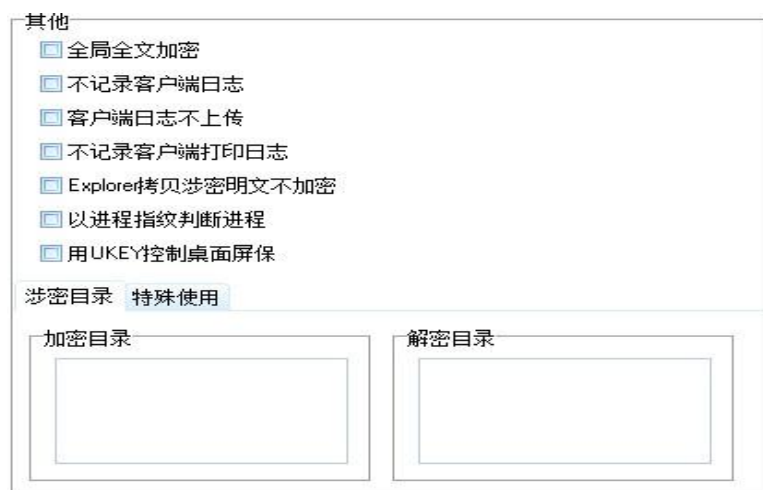
备份到网络必须在网络上安装备份服务器。CDPS 备份服务端程序在 Disc B 盘的 BackSev 目录下，直接拷贝到文件备份服务端运行 DDC_S.exe 安装即可。



将文件服务端所在机器 IP 及备份端口号填写到相关输入框内，若服务端已经运行，则可点击“测试连接”按钮测试是否连接通畅。

注意：备份到网络将对网络传送造成一定的负担，特别是一些大文件的自动备份，将会影响本机的使用效率，造成机器“假死”，因此，建议经常进行大文件编辑的用户不使用网络备份。同时，若用户数量较多时，建议设置多台网络备份服务器，以分散网络备份带来的网络数据传输压力。

其他控制：其他控制选框（如图所示）其含义如下：



全局全文加密：对所有加密采用全文加密模式。

不记录客户端日志：设置客户端运行时，是否记录密文的产生、删除、重命名等信息。

客户端日志不上传：设置客户端记录的日志是否上传到加密服务器。

不记录客户端打印日志：设置涉密文件打印是否有日志记录。

Explorer 拷贝涉密明文不加密：在拷贝涉密类型的明文时，不对文件进行加密。

以进程指纹判断进程：根据进程特点识别进程。

用 UKEY 控制桌面屏保：通过 UKEY 控制客户端机器，当无 UKEY 时，客户端处于保密状态。

涉密目录：涉密目录分为加密目录和解密目录，其含义如下：

加密目录：任何明文文件被置于此设置的目录后，会被主动加密为密文文件。可以将鼠标移动到加密目录选框内，然后点击右键添加加密目录。（添加格式为*\test*）

解密目录：任何明文文件被置于此设置的目录后，会被主动将加密文件给解密。可以将鼠标移动到加密目录选框内，然后点击右键添加加密目录（添加方格式和加密目录一样）。

特殊使用：特殊使用选框包括非法进程、去表示进程和 PLM 服务器，其含义如下：

非法进程：用于禁止客户端某些非法进程的运行。具体进程由编辑框定义，多个进程用半解分号(;)分隔。

去权限进程：此类进程在上传密文时，自动将群组控制权限去掉，以方便不同部门人员阅读密文。

PLM 服务器：添加 PLM 服务器的 IP 地址。

非法进程、其表示进程和 PLM 服务器添加方式都是将鼠标移动到加密目录选框内，然后点击右键添加进程或者 IP。

注：如果勾选了“功能设置”→“系统设置”→“系统控制”中的“启用密文权限控制”后，将会自动显示出“密文权限控制”的设置。

其他

☐ 全局全文加密

☐ 不记录客户端日志

☐ 客户端日志不上传

☐ 不记录客户端打印日志

☐ Explorer拷贝涉密明文不加密

☐ 以进程指纹判断进程

☐ 用UKEY控制桌面屏保

密文权限控制

缺省密级:

缺省群组:

涉密目录 特殊使用

加密目录

解密目录

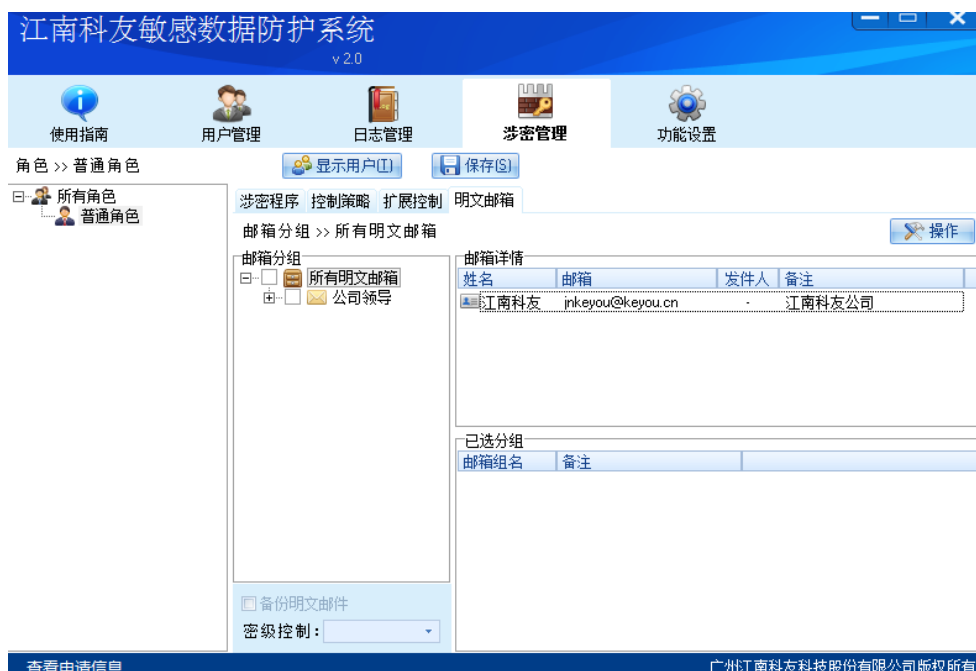
“缺省密级”：缺省密级是设置该角色所生成密文密级的等级，默认为“秘密”、“机密”和“绝密”三种，其中“绝密”为最高密文密级。

“缺省群组”：缺省群组是未新用户设置了默认群组，如果没有使用群组功能在此可以不比设置；默认群组为“技术部”、“财务部”和“采购部”。

4.4 明文邮箱策略

明文邮箱策略是为了方便用户对外交流的一组策略。明文邮箱策略中定义了的邮件，当用户通过CDPS客户端提供的明文邮箱功能发送密文附件的邮件时，密文附件将自动解密。

明文邮箱策略设置界面如图所示：

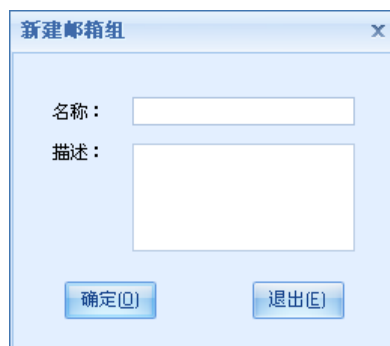


明文邮箱策略的制订包括明文邮件组的制订及明文邮箱的定义两部分。

明文邮箱策略组左边进行。选中相应策略组，点击右键将弹出策略组编辑菜单，如图所示。



点击“新增分组”菜单，将在当前选中策略组下新建一个策略组，并弹出新建策略组编辑窗口，如图所示。



4.5 角色

角色是用于管理不同类别加密要求的策略组。角色显示在涉密策略的左侧(如图所示)。

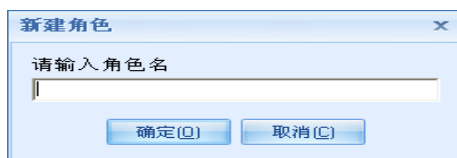
点击角色里面相应的组名，右侧显示该组所拥有的策略。

只有在“所有角色”显示状态下，才可以新建、编辑、删除和克隆角色。当然，操作用户还必须有相应的权限才行。

点击策略组相关策略，右键操作菜单如图所示：



新增/修改角色：点击“新增”菜单，弹出（如图）所示编辑框。选中一个角色，点击“修改”，也可以得到此编辑界面。

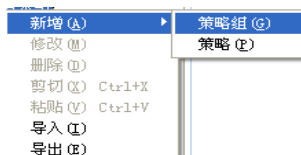


克隆角色：此功能可用于快速新建一个角色，使得它与某个角色拥有相同的策略。

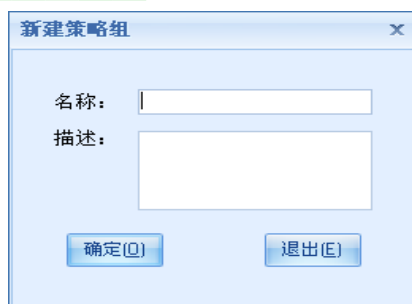
4.6 策略组

策略组是用来集中管理某一组涉密策略的。在“涉密管理”界面的“涉密程序”菜单页下方点击某个策略组时，右侧可显示相应的涉密策略。点击“所有策略”时，右侧显示所有定义了的涉密策略。

在涉密程序页面下方单击右键，弹出右键菜单：



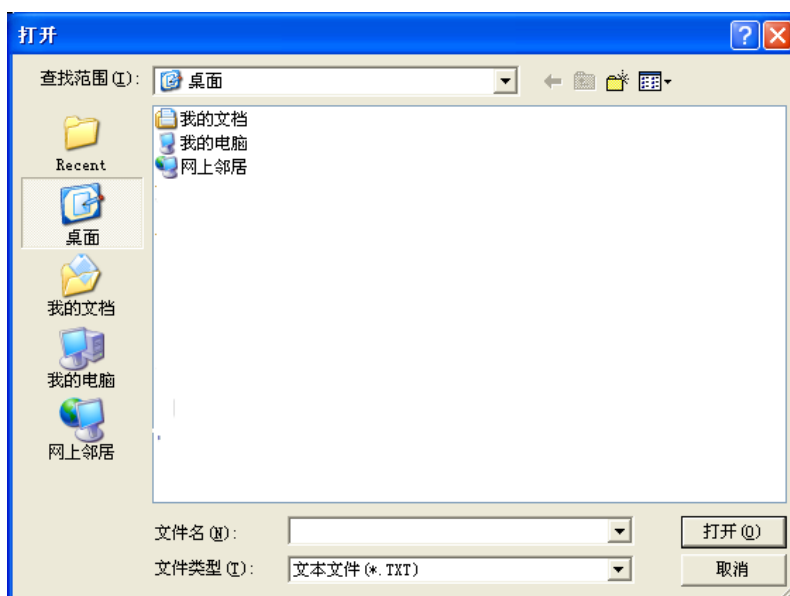
新建：点击“新增”菜单，弹出所示编辑框。选中一个策略组，点击“修改策略组”，也可以得到此编辑界面（注：厂商策略组不可编辑）。



删除策略组：删除策略组并不会影响涉密策略，但会影响已经分发此策略组用户的策略。

剪切/粘贴策略组：用于快速新建一个拥有相同涉密策略的策略组。

导入/导出策略组：用户可以快速将已经设置好的策略导入到服务端，也可以将自定义的策略或者策略组导出做备份，导出操作入图所示。



5 敏感数据防护系统技术参数

5.1 网络环境要求

CDPS 系统对网络环境要求也非常简单，只要客户端（控制端）与服务器之间的 TCP/IP 协议通畅就可以了。

5.2 客户端延时

客户端在对文件进行自动加解密的时候，会耗费 CPU 资源，也就会造成延时。这是用户为了数据安全所需要花费的唯一代价。具体延时的长短，依据计算机硬件性能、应用软件的大小而定。以下是一组测试数据，仅供参考。

CPU: Intel Centrino 1.3GHz		内存: 512M DDR	
操作系统: MS Windows XP Pro SP2		杀毒软件: Symantec AntiVirus 企业版 8.0	
应用软件: UG NX2		数据文件大小: 31.5M	
操作	在操作系统中双击数据文件	点击应用软件快捷方式	应用软件启动后打开数据文件
计时	启动应用软件并打开数据文件	启动应用软件	打开数据文件
安装 CDPS 之前	约 35 秒	约 29 秒	约 6 秒
安装 CDPS 之后	约 41 秒	约 34 秒	约 6 秒