
# Curtain™ e-locker(易锁) 5.0

## 安装说明书

发布日期: 2018 年 1 月 1 日

若对产品或本说明书有任何疑问或查询，欢迎联络我们的代理商或服务提供商。

若需要其他协助，请发电子邮件至：info@coworkshop.com 。

本说明书的内容如有更改，恕不另行通知。关于使用 Curtain e-locker(易锁)的一切条文及细侧，请参阅软件授权协议（Curtain e-locker Software License Agreement）。



本说明书内所提到的其他产品或商标，均属于相关公司所拥有。

# 目录

# 1 - 前言

## 1.1 - 资料外泄的威胁

在每天的工作中，有些敏感资料又必需要给员工去用(如:业务会接触到客户资料;工程师会接触到图档等)，但公司又很困难去控制员工如何使用这些敏感资料。当员工有权去使用这些资料时(如:读取、修改等)，就如同可以拥有它，员工可以很容易通过不同渠道将资料带走(如:打印、移动硬盘、Internet、电邮、甚至截屏等)。对公司来说，可以全面控制敏感资料的使用，是十分困难的。

## 1.2 - Curtain e-locker(易锁)的设计目的

Curtain e-locker(易锁)是一套完善的防止资料外泄解决方案，它可以有效防止不授权员工用任何渠道将资料带走。实施Curtain e-locker后，公司可以容许授权员工正常使用敏感资料，同时，公司可以完全防止员工在使用资料时将资料带走。

## 1.3 - 后台系统(如:Windows文件服务器)亦有权限控制，为什么需要Curtain e-locker?

是的，后台系统也有权限控制，但是，后台系统只可以控制"读取"、"修改"、"删除"等权限。如果管理员容许用户访问服务器资料(如:共享文件夹)，后台系统就不能阻止用户将文档保存至本地磁盘、USB硬盘或透过电邮将文档外发，这方面正正就是Curtain e-locker的功用，因此，Curtain e-locker并不是取代后台系统，而是与后台系统紧密合作。当一个用户授权使用服务器上的资源时，管理员可以使用Curtain e-locker来防止资料外泄。

举例: 下图是Windows文件夹的权限设定，图中可见，它并没有"打印"或"保存"等控制。

## 1.4 - 我们公司已经禁止使用USB接口和互联网，为什么还需要Curtain e-locker?

是的，禁止使用USB接口和互联网是可以减低资料外泄的风险。但是，还有很多渠道可以将资料带走。例如:

- 打印
- 截屏、截屏软件
- 复制粘贴
- 电邮
- Wi-Fi、蓝芽 (用手机作为热点)
- Skype, Whatsapp, QQ, Wechat
- 更多...

有些公司尝试把所有接口或渠道堵住，但是对管理员来说，这是十分困难去实施和维护形形色色不同的控制。而且，在现今信息发达的社会，不容许员工在工作时使用电邮、Skype、USB等工具是十分不方便的。Curtain e-locker既不影响正常操作，亦可以确保资料的安全，Curtain e-locker在方便性和资料保安之间取得很好的平衡。

## 1.5 - 关于Curtain e-locker

### 1.5.1 - Curtain e-locker的基本控制

Curtain e-locker可以控制:

- 保存到任何地方
- 发送
- 打印
- 截屏
- 复制内容到任何位置
- 复制文件到任何位置

Curtain e-locker只控制受保护区内的文档，员工可以如常使用受保护区内的文档，只是一切非授权的功能都会被Curtain e-locker堵住。比如:如果用户不容许存储受控文档到别的地方或打印受控文档，这些功能都会被Curtain堵住，但用户依然可以使用电邮、USB移动硬盘或互联网，只是受保护区内的文档受到Curtain的控制。

系统管理员可以针对不同用户或电脑来设定不同的安全策略群组，请参考相关文件。

### 1.5.2 - Curtain e-locker的基本结构

员工在日常工作中，很多时需要接触到一些机密资料(如:销售人员会接触到客户资料、工程师需要接触图档等等)。当他们授权访问Windows文件服务器上的共享文件夹时，公司是十分困难防止他们将这些机密资料带走。

实施Curtain e-locker后，管理员可以设定那些服务器上的共享文件夹需要Curtain的保护。如果员工需要使用这些受保护资料，他们的计算机必需要安装了Curtain客户端，在安装Curtain客户端时，系统会自动在员工计算机上建立一个安全文件夹(称为本地受保护区)。

管理员于Curtain管理端上建立及设定不同的安全策略群组，设定后指派用户计算机到不同的群组当中。Curtain e-locker有一个独有的设计，称为受保护区(受保护区是由服务器上的受保护资料和客户端上的本地受保护区组成的)，员工可以在受保护区内如常使用机密资料(如:读取、修改等)，但是在没有授权情况下就不能将资料带到受保护区之外。同时，员工依然可以使用互联网、电邮等设备。


### 1.5.3 - Curtain e-locker的基本组件

Curtain e-locker有三个基本的组件:

- Curtain客户端
- Curtain管理员(我们亦会把安装了Curtain管理员的计算机称呼为Curtain安全策略服务器)
- Curtain服务器插件

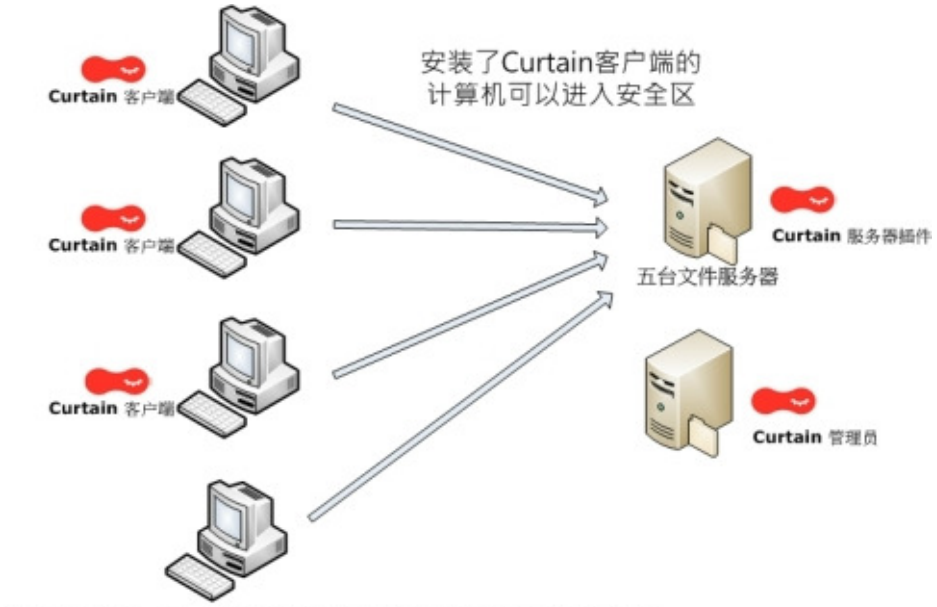
Curtain客户端:
当用户使用服务器上的受保护资料时(如:文件服务器上的受保护共享文件夹、受保护网站等)，用户的计算机必需要已经安装了Curtain客户端。在安装Curtain客户端时，系统会自动建立一个安全的文件夹(那就是Curtain本地受保护区)。

Curtain管理员:
系统管理员可以用Curtain管理员来集中地为所有Curtain客户端设定安全策略。同时，Curtain管理端會储存用户审计日志以供授权人员查阅。一般而言，一家公司只需要安装一台Curtain管理员。

Curtain服务器插件:
Curtain服务器插件需要安装在所有需要Curtain e-locker保护的服务器上。Curtain服务器插件会定时与Curtain管理员沟通，用最新的安全策略来保护服务器上的资料。

举例:这家公司想用Curtain e-locker来保护它们五台服务器上的共享文件夹，那么他们需要于这五台服务器上都安装Curtain服务器插件。

以下是Curtain e-locker基本的架构:

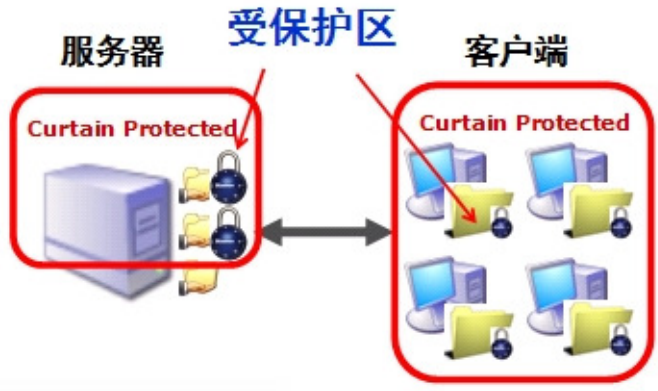



备注:
- Curtain管理员可以安装在一台独立的服务器上或是安装在其中一台文件服务器上。
- 系统管理员可以通过"例外"这个功能来容许没有安装Curtain客户端的电脑访问受保护的服务器资源。

### 1.5.4 - Curtain受保护区的概念

受保护区是由(1)服务器上的受保护资料和(2)客户端上的本地受保护区组成的。服务器上的受保护资料可以是文件服务器上的共享文件夹、SharePoint、ERP、自行开发的系统等。而在用户计算机上，本地受保护区会在安装Curtain客户端时自动生成，文件夹名称是"ProtDir"，它会被建立于所有本地的硬盘上。

受保护区:



客户端上的本地受保护区:


以上例子，本地硬盘上有两个分区(C和D)，所以"ProtDir"会建立于C和D这两个分区之下。而且，本地受保护区是个人化的，即使在同一台计算机上，用户也不能访问另一位用户的本地受保护区。

备注:
- 于安全策略群组，有一个"隐藏本地受保护区"的设定，管理员可以通过启动这功能，来达到强制用户直接使用文件服务器上受控文档的效果。
- 软件有一个"本地加密磁盘"的功能，管理员可以通过这功能来加密本地受保护区，来提升资料安全性。
- 如有需要，管理员可以添加 "附加本地受保护区"。

# 2 - 安装前的准备

## 2.1 - Curtain e-locker的实施计划

安装前的准备:

- 那些服务器上的资料需要受Curtain e-locker保护(如:文件服务器上的共享文件夹、SharePoint、ERP、自行开发的系统等)?
- 那些用户需要使用这些受保护的资料?
- 公司想如何控制用户使用这些受保护的资料(如:禁止保存到受保护区以外)?
- 那台服务器会安装Curtain管理员?
- 是否想将Curtain e-locker与Active Directory整合(以便使用AD用户/用户群组来配置安全策略)?
- 是否想将用户电脑上的本地受保护区加密?

实施次序:

1. 安装Curtain管理员
2. 在所有需要Curtain e-locker保护的服务器上安装Curtain服务器插件
3. 在用户的计算机上安装Curtain客户端
4. 激活Curtain e-locker
5. 于Curtain管理员上建立及设定安全策略群组
6. 从Active Directory导入用户资料(如果需要按AD用户/用户群组来配置安全策略)
7. 指派电脑/用户到不同的安全策略群组
8. 设定服务器上的受保护区(那些服务器上的资料需要保护)
9. 完成

备注: 不应该将Curtain服务器插件和Curtain客户端安装在同一台计算机上。

## 2.2 - 系统软硬件的要求

### 2.2.1 - Curtain服务器插件和Curtain管理员对系统软硬件的要求

Curtain服务器插件和Curtain管理员对系统软硬件的要求:

- Intel Pentium或更好的处理器
- Windows XP、服务器2003、2008、2012、2012R2、2016、Vista、Win 7、Win 8、Win 8.1或Win 10操作系统
- 128MB内存 (建议256MB内存)
- 200MB硬盘空间 (NTFS格式)
- TCP/IP网络协定
- TCP端口8443（默认开放）
- TCP端口24821与24822必需开放（注意：如果网络存在防火墙，请确认这两个端口未被遮罩）
- 对于64位元操作系统，MSXML 4或6是必需的 (在微软官方网站上可以下载到)

### 2.2.2 - Curtain客户端对系统软硬件的要求

Curtain客户端对系统软硬件的要求:

- Intel Pentium或更好的处理器
- Windows XP、服务器2003、2008、2012、2012R2、2016、Vista、Win 7、Win 8、Win 8.1或Win 10操作系统
- 128MB内存 (建议256MB内存)
- 200MB硬盘空间 (NTFS格式)
- TCP/IP网络协定
- TCP端口24821与24822必需开放（注意：如果网络存在防火墙，请确认这两个端口未被遮罩）
- 对于64位元操作系统，MSXML 4或6是必需的 (在微软官方网站上可以下载到)

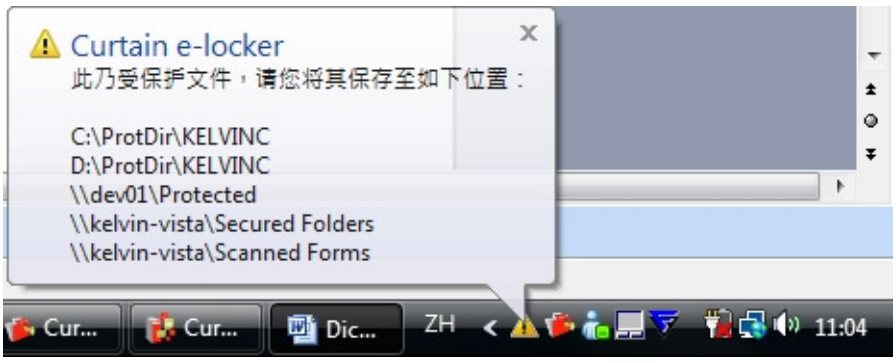
## 2.3 - Curtain的基本权限控制

Curtain的基本权限控制可以针对个别安全策略群组和应用软件来设置的，以下是默认的权限控制。


"强制保存到受保护区内" - 此选项被选取时，用户不能于应用软件中(如:Word)将受控文档保存到受保护区之外。
"禁止复制出去" - 此选项被选取时，用户不能于Curtain客户端中将受控文档复制到受保护区之外。
"禁止打印" - 此选项被选取时，于应用软件中所有有关打印的功能都会被禁止。
"附加水印" - 此选项被选取时，打印出来的文件上会加上水印 (详细资料请参考相关文档)。
"记录打印内容" - 此选项被选取时，系统会为打印出来的文件拍快照，快照会储存在Curtain管理员的审计日志内(详细资料请参考相关文档)。
"禁止截屏" - 此选项被选取时，当用户使用截屏键或截屏软件时，显示敏感资料的窗口都会变成灰色。
"禁止剪贴板" - 此选项被选取时，将文档内容复制粘贴到受保护区之外都会被禁止(如:复制粘贴内容到Email)。
"禁止传送(如:电邮、互联网等)" - 此选项被选取时，于应用软件中所有有关发送的功能都会被禁止。

设置Curtain权限控制的例子

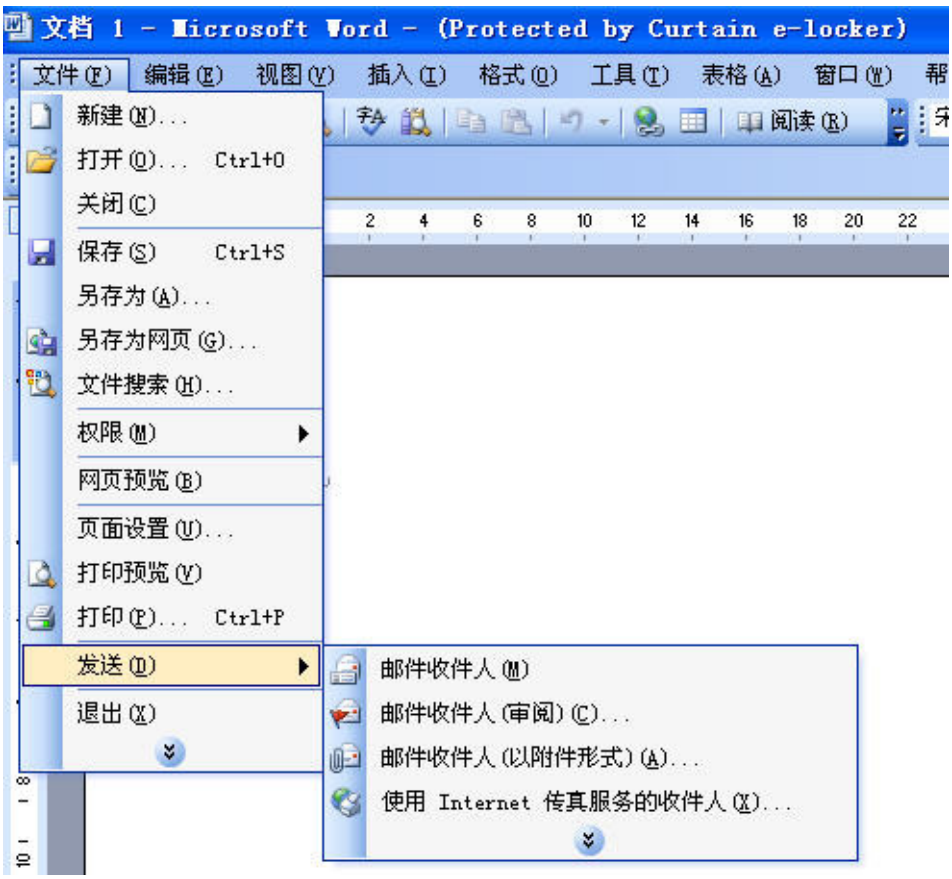
情况1 - 针对MS Word，启动"强制保存到受保护区内":
- 当用户尝试于MS Word内通过选择"文件>另存"将受控文档保存到受保护区之外时，Curtain e-locker会禁止有关操作并提示用户。




情况2 - 针对MS Word，停用"禁止复制出去":
- 于Curtain客户端，点选一个Word文档，按鼠标右键，你可以于子菜单中看见"复制到"选项。你可以使用此功能将文档复制到受保护区之外。

文档被复制到受保护区之外后:
- Curtain e-locker再不会控制此文档。
- Curtain e-locker会将此"移出复制"操作记录在审计日志中。


情况3 - 针对MS Word，启动"禁止传送(如:电邮、互联网等)":
- 当用户尝试于MS Word内通过选择"文件> 发送"将受控文档以电邮方式传送到受保护区之外时，Curtain e-locker会禁止有关操作并提示用户。



## 2.4 - 给Curtain e-locker开放端口

### 2.4.1 - 给Curtain管理员和服务器插件开放端口24821和24822

如果启用了Windows防火墙，请给Curtain管理员和服务器插件开放端口24821和24822。

于Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10操作系统下，添加以下规则：

- 24821的TCP的入站规则
- 24821的UDP的入站规则
- 24822的TCP的出站规则
- 24822的UDP的出站规则

于Windows 2003和XP，把以下端口设定为例外：

- TCP的24821
- UDP的24821
- TCP的24822
- UDP的24822

于Windows 2008/2012/Vista/Win 7/Win 8/Win10操作系统下，添加规则的步骤：

举例设置24821的TCP的入站规则
1. 右键选择【计算机】>【管理】，弹出"服务器管理器"界面，选择"配置>高级安全 Windows 防火墙>入站规则"，右键选择"入站规则"，选择"新规则"。

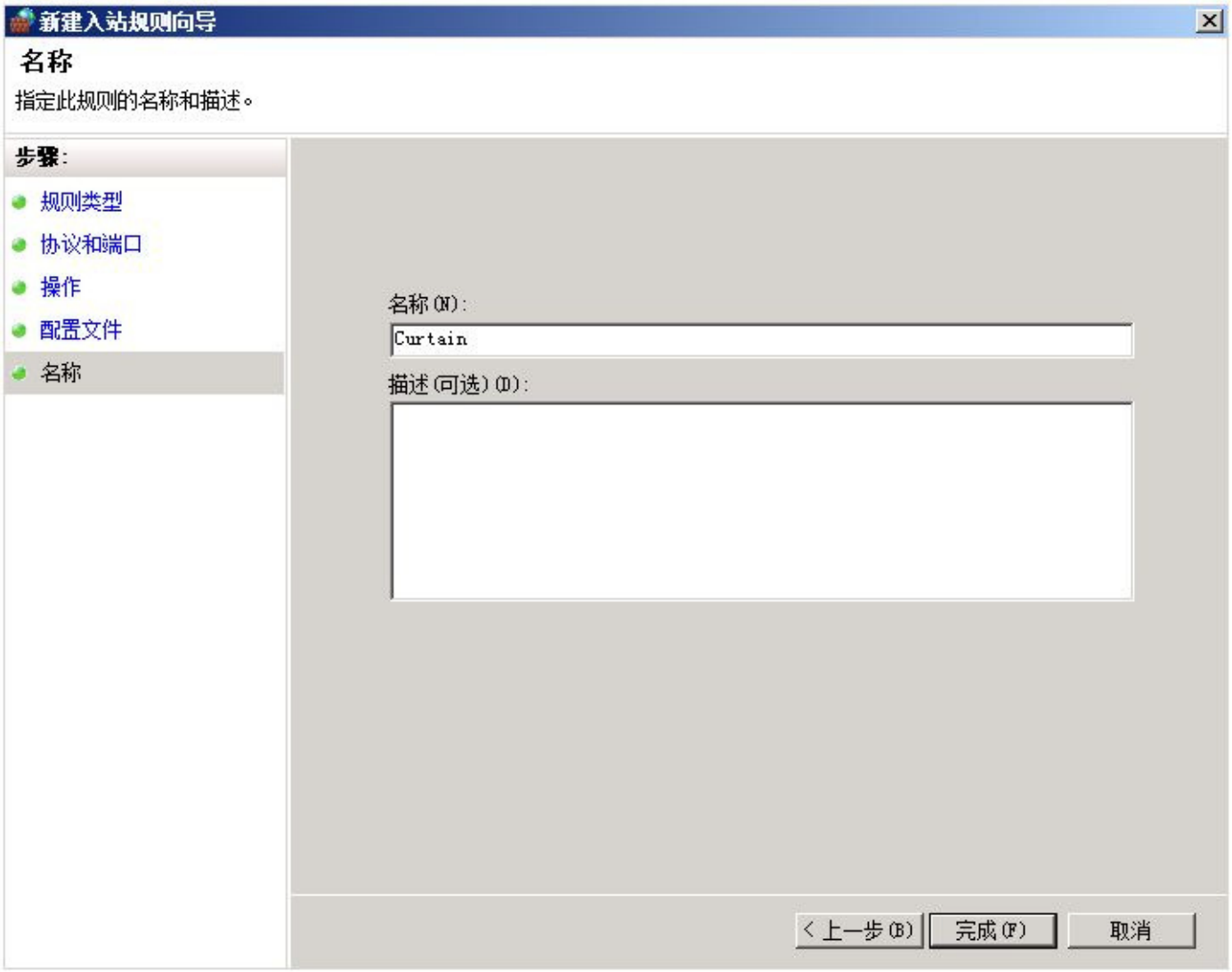
2. 弹出"新建入站规则向导"，如下图所示，选择"端口"，点击【下一步】。

3. 在"特定本地端口" 内输入"24821"，点击【下一步】。

4. 选择"允许连接"，点击【下一步】。

5. 如图所示默认勾选上"域"，"专用"，"公用"，点击【下一步】。

6. 在名称内输入"Curtain"，点击【完成】。



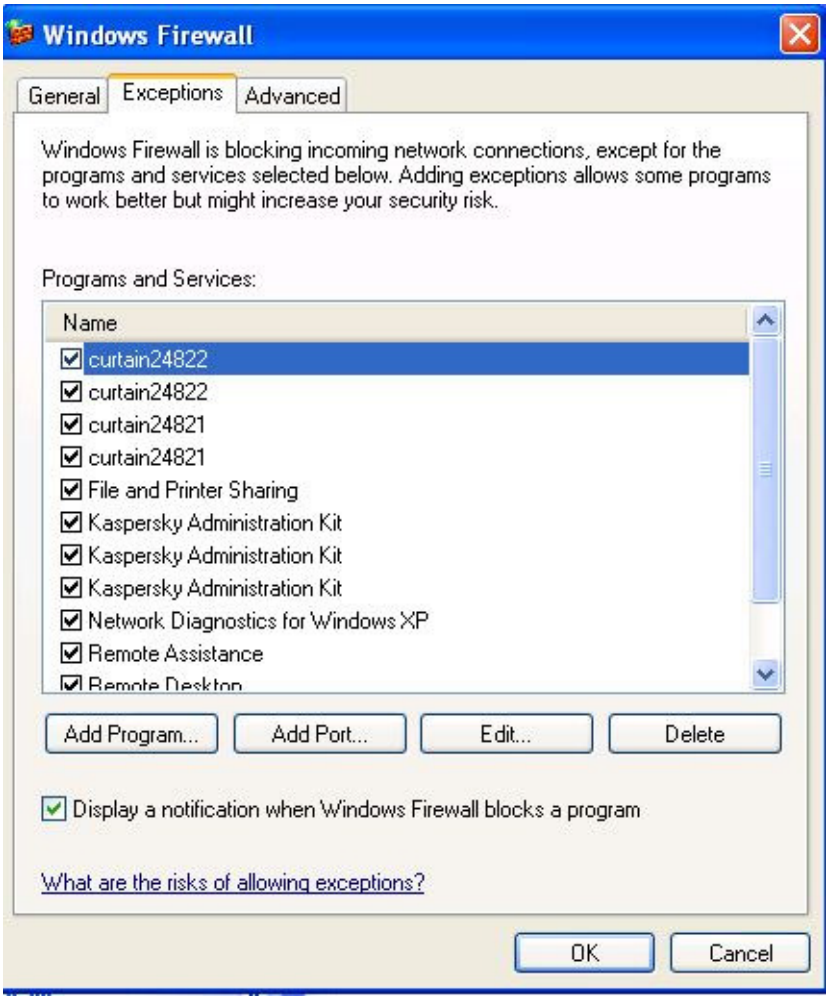
7. 查看右方入站规则的列表，在列表中会多出一项 “Curtain” ，如下图所示，添加例外端口操作成功。


同理，按上面步骤设置 24821的UDP的入站规则， 24822的TCP的出站规则， 24822的UDP的出站规则即可。

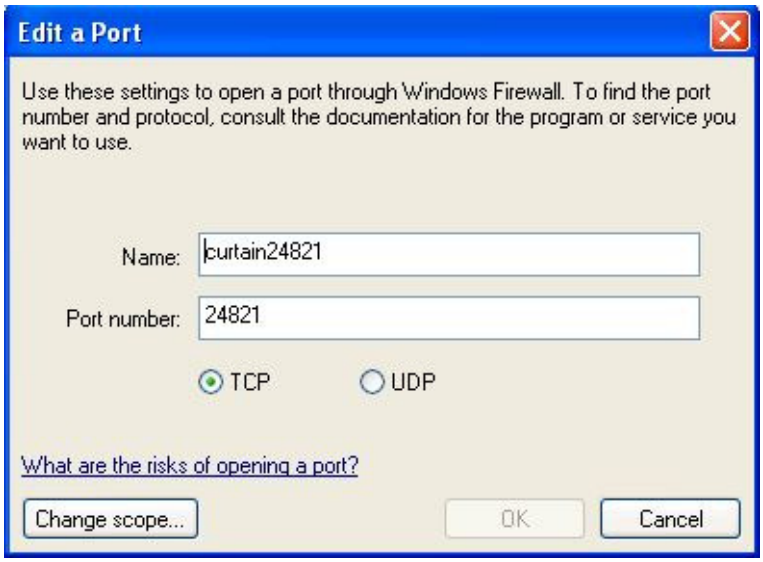
备注：
- 设置出站规则时，右键选择"出站规则"，选择"新规则"。

于Windows 2003和XP，设置例外端口的步骤

1. 进入"控制面板>Windows Firewall>Exceptions"，按"Add Port..."



2. 给此例外输入名称、端口为TCP的24821，并按OK确定。




同理，按上面步骤设置UDP的24821，TCP的24822 ，UDP的24822即可。

### 2.4.2 - 给Curtain客户端开放端口24821和24822

如果启用了Windows防火墙，请给Curtain客户端开放端口24821和24822。

于Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10操作系统下，添加以下规则：

1. 24822的TCP的入站规则
2. 24822的UDP的入站规则
3. 24821的TCP的出站规则
4. 24821的UDP的出站规则

于Windows 2003和XP，把以下端口设定为例外：

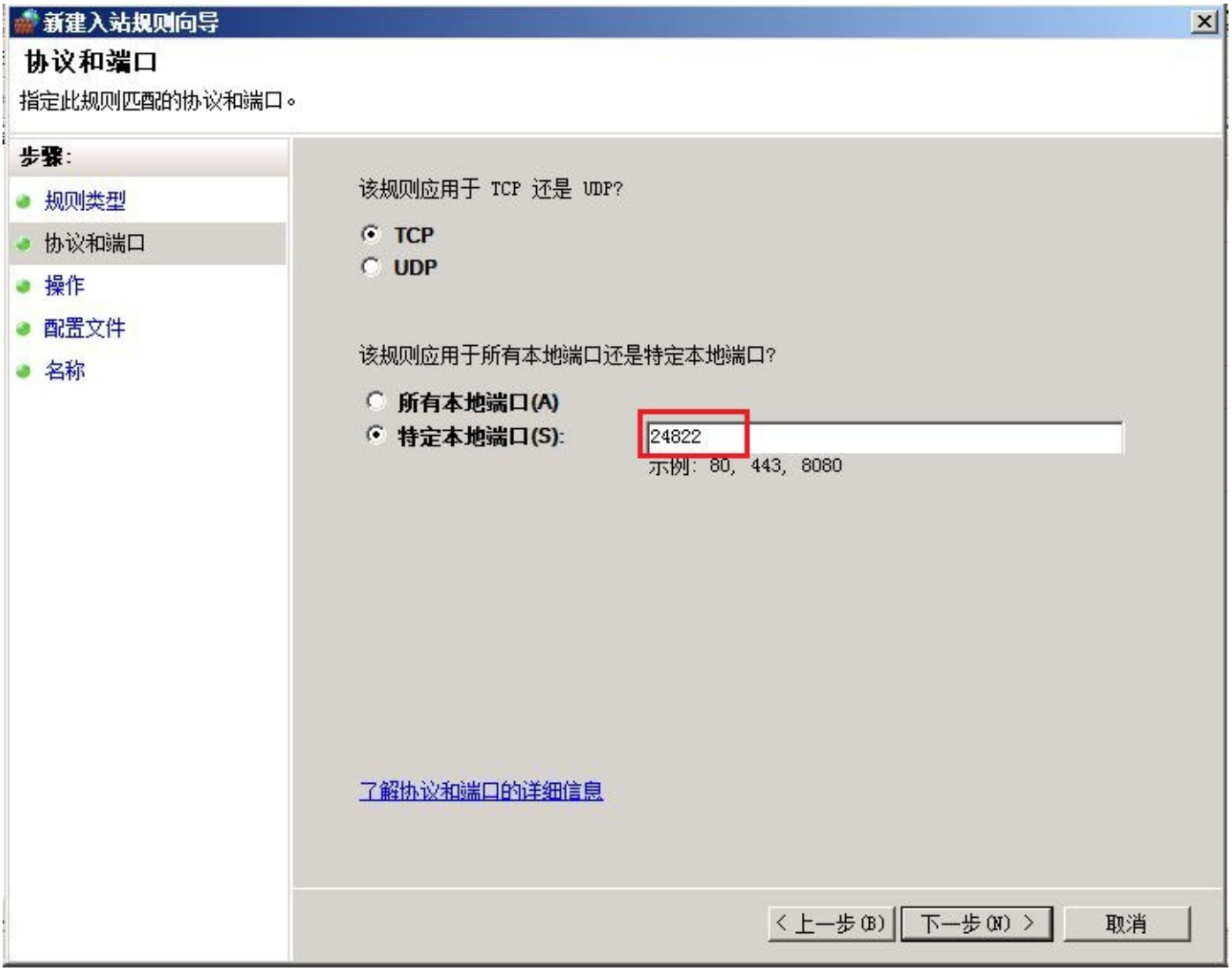
1. TCP的24822
2. UDP的24822
3. TCP的24821
4. UDP的24821

于Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10操作系统下，添加规则的步骤：

举例设置24822的TCP的入站规则
1. 右键选择【计算机】>【管理】，弹出"服务器管理器"界面，选择"配置>高级安全 Windows 防火墙>入站规则"，右键选择"入站规则"，选择"新规则"。

2. 弹出"新建入站规则向导"，如下图所示，选择"端口"，点击【下一步】。

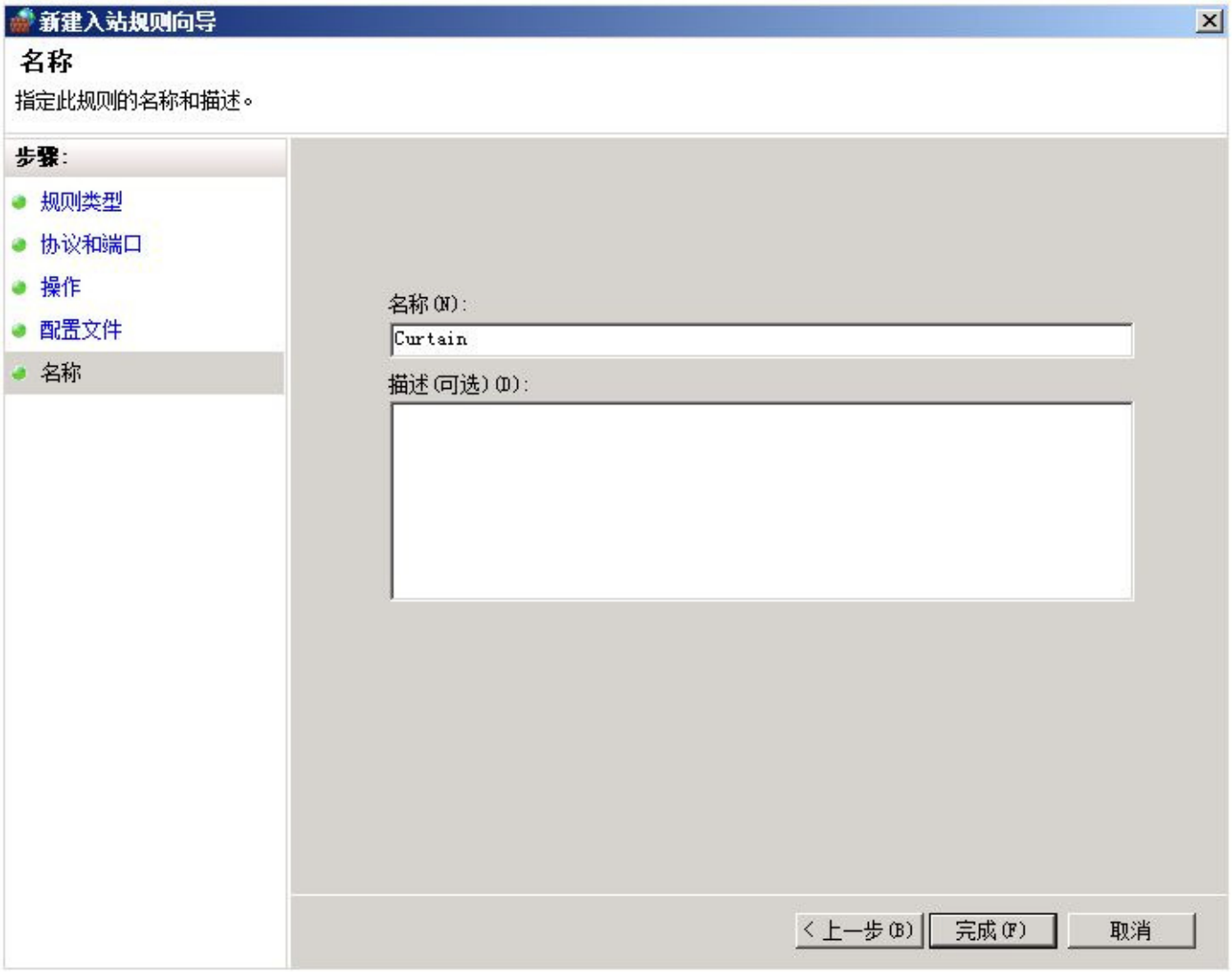
3. 在"特定本地端口" 内输入"24822"，点击【下一步】。



4. 选择"允许连接"，点击【下一步】。

5. 如图所示默认勾选上"域"，"专用"，"公用"，点击【下一步】。

6. 在名称内输入"Curtain"，点击【完成】。



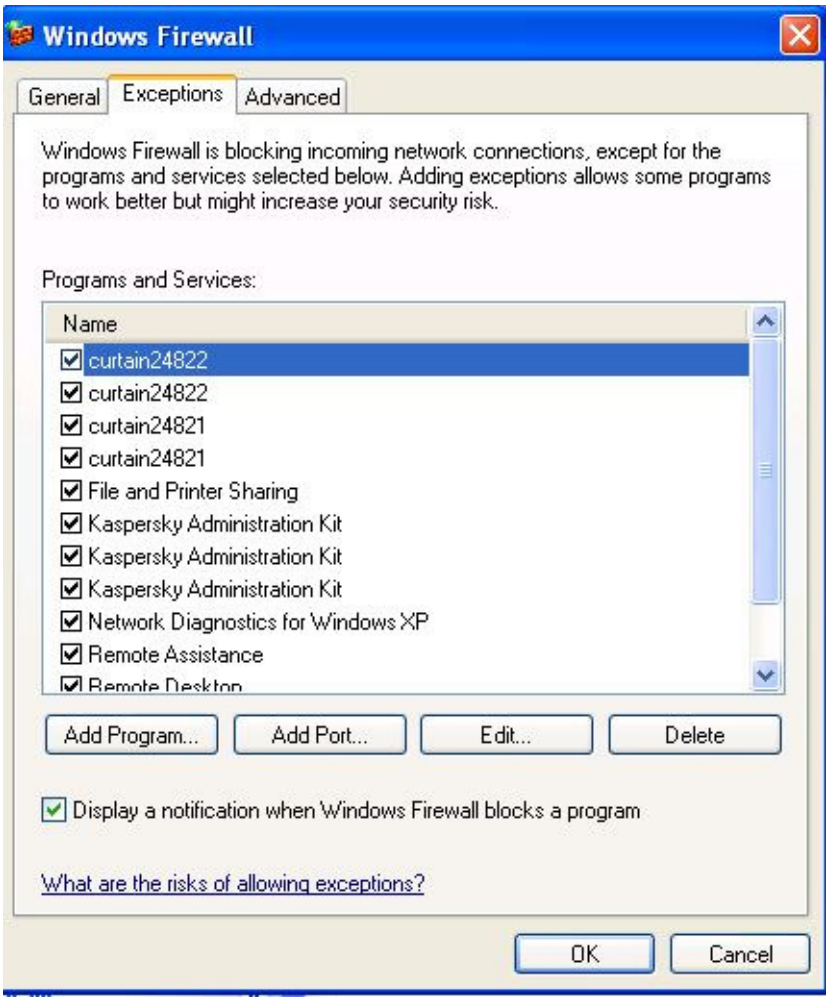

7. 查看右方入站规则的列表，在列表中会多出一项"Curtain"，如下图所示，添加例外端口操作成功。


同理，按上面步骤设置 24822的UDP的入站规则， 24821的TCP的出站规则， 24821的UDP的出站规则即可。

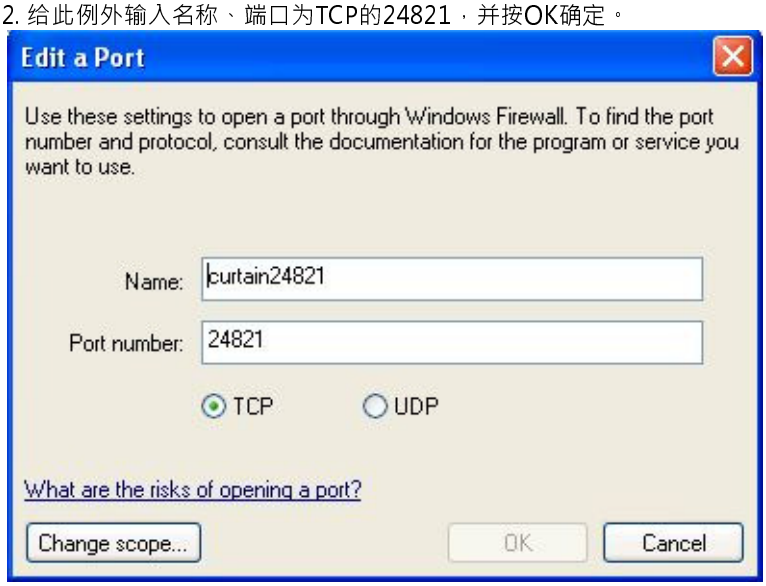
备注：
- 设置出站规则时，右键选择"出站规则"，选择"新规则"。
- 请注意，在Curtain客户端上入站规则是开放端口24822，而在Curtain管理员和服务器插件上入站规则是开放端口24821，很容易混乱。

## 于Windows 2003和XP，设置例外端口的步骤

1. 进入"控制面板>Windows Firewall>Exceptions"，按"Add Port..."



2. 给此例外输入名称、端口为TCP的24821，并按OK确定。




同理，按上面步骤设置UDP的24821，TCP的24822 ，UDP的24822即可。

### 2.4.3 - 于Curtain服务器插件上检查Tomcat 8005端口是否已被占用

在安装Curtain服务器插件过程中，会同时安装Tomcat，为了避免Tomcat端口8005冲突，请在安装Curtain服务器插件之前先检查端口是否已被占用。如果端口8005已被占用，请在安装Curtain服务器插件后不要重启电脑，先为Curtain服务器插件更改Tomcat端口（更改端口步驟，請參考FAQ 00193）。

查看Tomcat端口8005的步骤：

1. 在Command Prompt下，输入netstat -ano|findstr “8005” ，然后按 “输入” 。

2. 如果该端口没有被占用，查找为空（如下图）。


3. 如果端口已被占用，就会列出占用程序的信息。


4. 使用PID来查询程式信息，于Command Prompt，输入tasklist|findstr “3856” ，然后按回车键（上图例子PID为3956）。

5. 手动修改server.xml文档（请参考FAQ 00193）。

### 2.4.4 - 为Curtain服务器插件更改Tomcat 8005端口

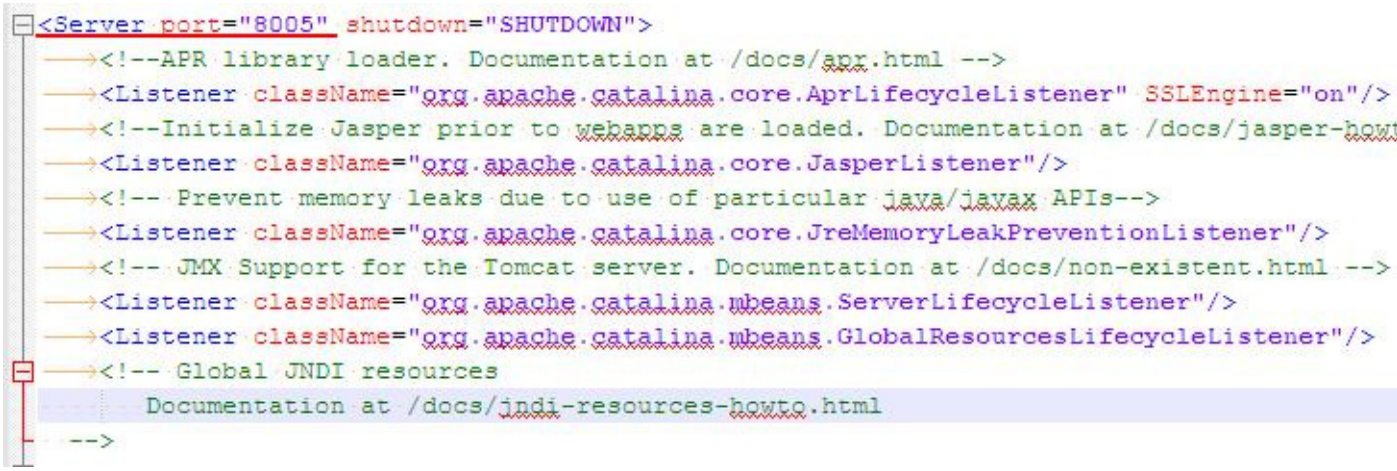
如果Tomcat端口8005已被其他程式占用，请在安装Curtain服务器插件后不要重启电脑，先为Curtain服务器插件更改Tomcat端口。

为Curtain服务器插件更改Tomcat端口的步骤：
1. 于计算机管理，将“Curtain web service”服务停止。

2. 到文件夹 C:\Program Files\CoworkShop\Curtain 3\Runtime\tomcat6.0.26\conf\。

3. 用Notepad打开server.xml文件（或其他编辑工具）。

4. 找到port 8005（如图所示位置），并将“8005”改为其他空闲的端口，然后保存。




5. 于计算机管理，将“Curtain web service”服务启动（安装Curtain服务器插件后需要重启电脑）。

6. 完成。

# 3 - 安装

## 3.1 - 安装Curtain管理员

当决定好在那一台服务器上安装Curtain管理员后，请按以下步骤进作安装。

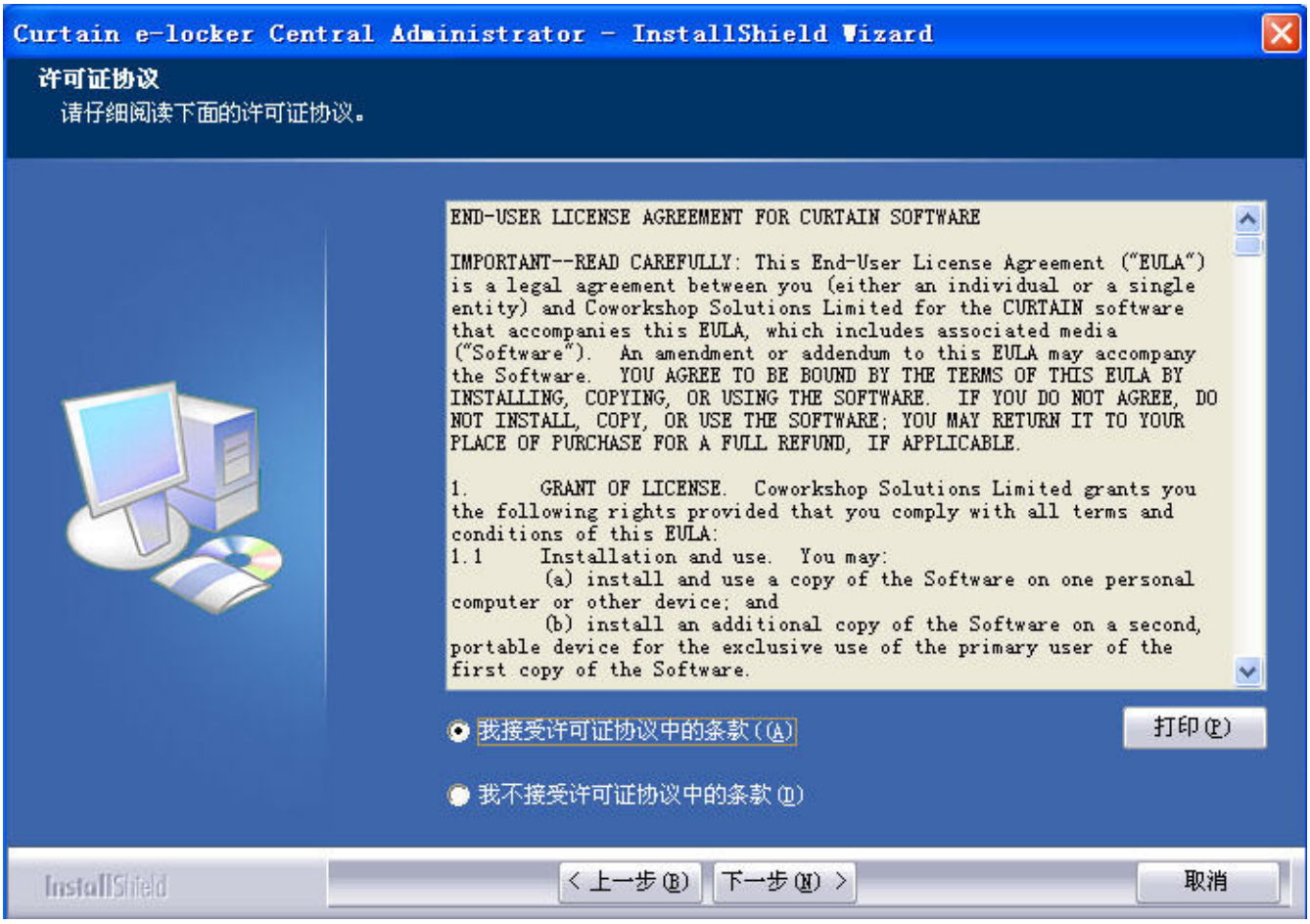
安装Curtain管理员的步骤:
1. 复制适合的Curtain服务器安装包(如: CurtainAdmin_Win32(327304).zip 或 CurtainAdmin_X64(327304).zip )到服务器的硬盘上。

2. 解压安装包。

3. 执行Curtain服务器安装程序。请确保以Windows管理员身份登入。
接着，请选择安装程序的语言。


4. 选择安装程序的语言，并按确定。

5. 阅读软件使用证协议。如同意协议内容，选择"我接受软件使用证协议"，并按下一步继续安装。



接着，请选择模块进行安装。


6. 有以下两个情况:
(a) 如果只是在这台服务器上安装Curtain管理员，
- 只需要点选"Curtain管理员"

(b) 如果需要保护这台服务器上的资料(如:文件服器上的受保护共享文件夹、受保护网站等)，
- 点选"Curtain管理员"以安装Curtain管理员，和
- 点选"Curtain服务器插件"以安装Curtain服务器插件。
并按下一步继续安装。

7. 选择安装程序的文件夹，并按下一步继续安装。

8. 按安装按钮，开始安装程序。

9. 如果在此台服务器上安装了Curtain服务器插件，在完成安装后，请重启电脑。

## 3.2 - 安装Curtain服务器插件

如果需要保护一台服务器上的资料(如:文件服务器上的受保护共享文件夹、受保护网站等)，你需要在该服务器上安装Curtain服务器插件。请按以下步骤进作安装。

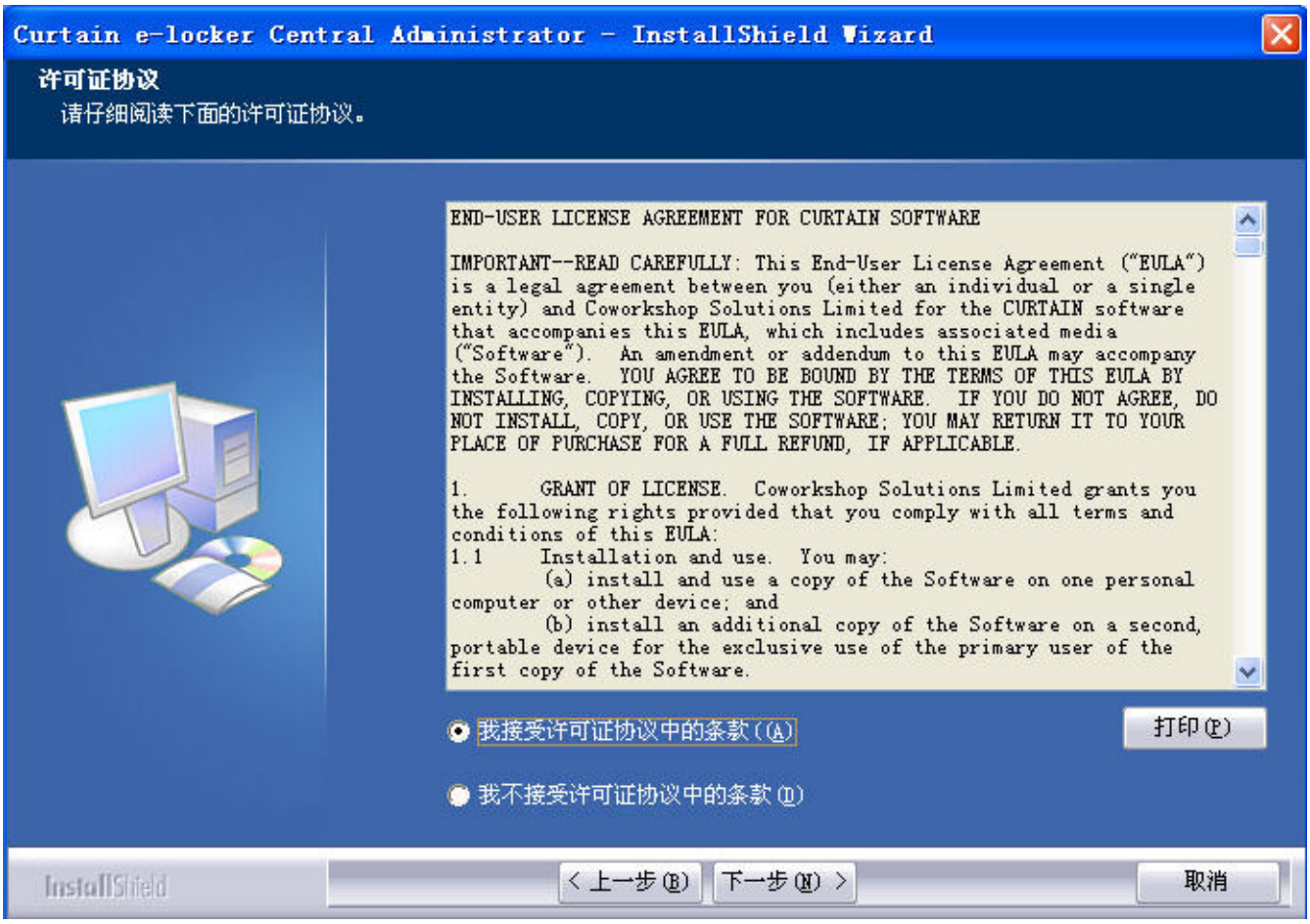
安装Curtain服务器插件的步骤:
1. 复制适合的Curtain服务器安装包(如: CurtainAdmin_Win32(327304).zip 或 CurtainAdmin_X64(327304).zip)到服务器的硬盘上。

2. 解压安装包。

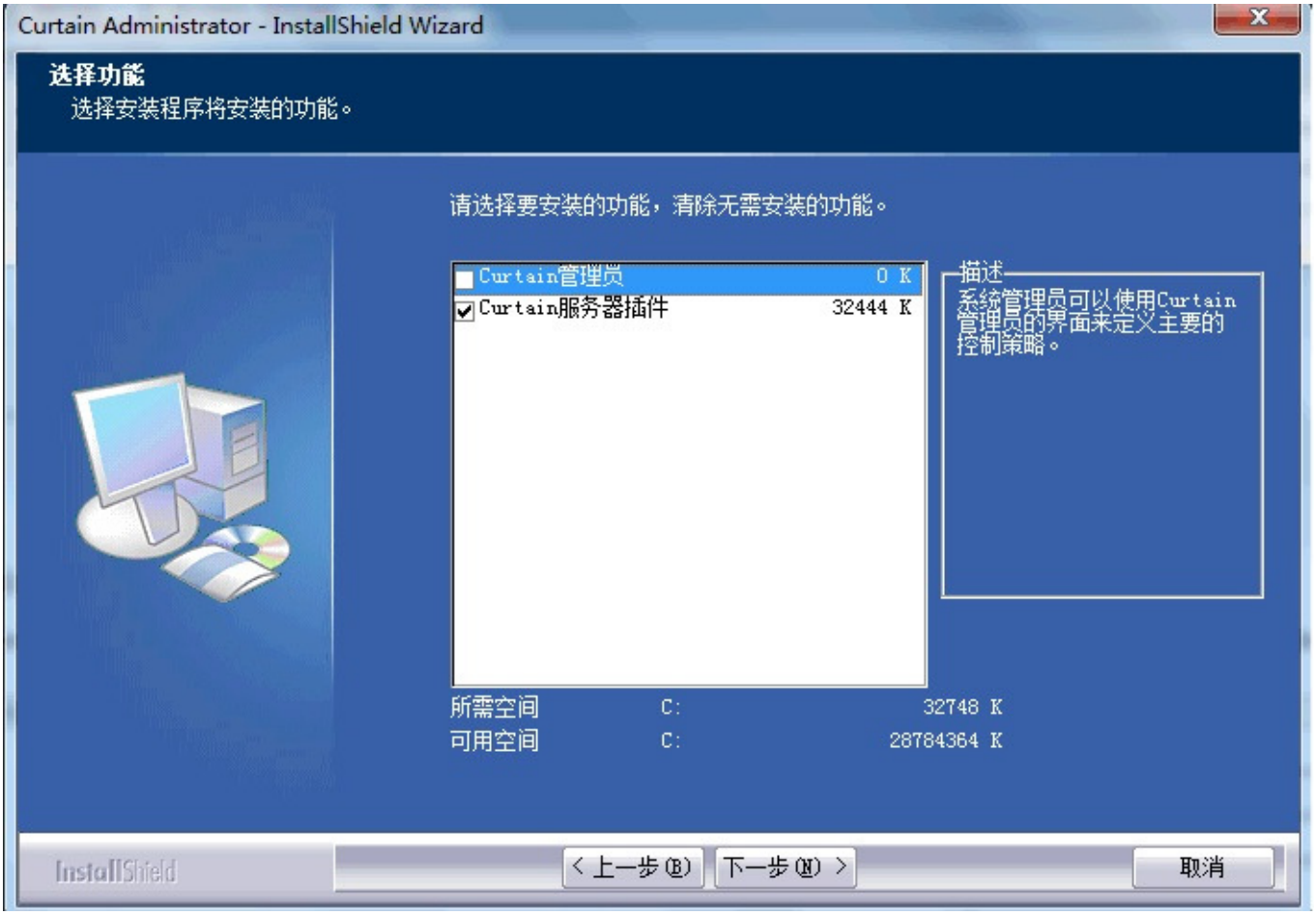
3. 执行Curtain服务器安装程序。请确保以Windows管理员身份登入。
接着，请选择安装程序的语言。


4. 选择安装程序的语言，并按确定。

5. 阅读软件使用证协议。如同意协议内容，选择"我接受软件使用证协议"，并按下一步继续安装。



接着，请选择模块进行安装。




6. 只需要点选"Curtain服务器插件"，并按下一步继续安装。

7. 选择安装程序的文件夹，并按下一步继续安装。

8. 按安装按钮，开始安装程序。

9. 在完成安装后，请重启电脑。

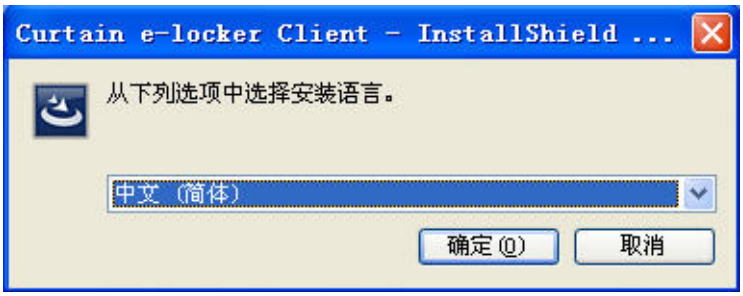
## 3.3 - 安装Curtain客户端

如果用户需要使用服务器上的受保护资料时(如:文件服务器上的受保护共享文件夹、受保护网站等)，用户的计算机必需要安装Curtain客户端。请按以下步骤进作安装。

安装Curtain客户端的步骤:
1. 复制适合的Curtain客户端安装包(如: CurtainClient_Win32(327304).zip 或 CurtainClient_X64(327304).zip)到用户计算机的硬盘上。

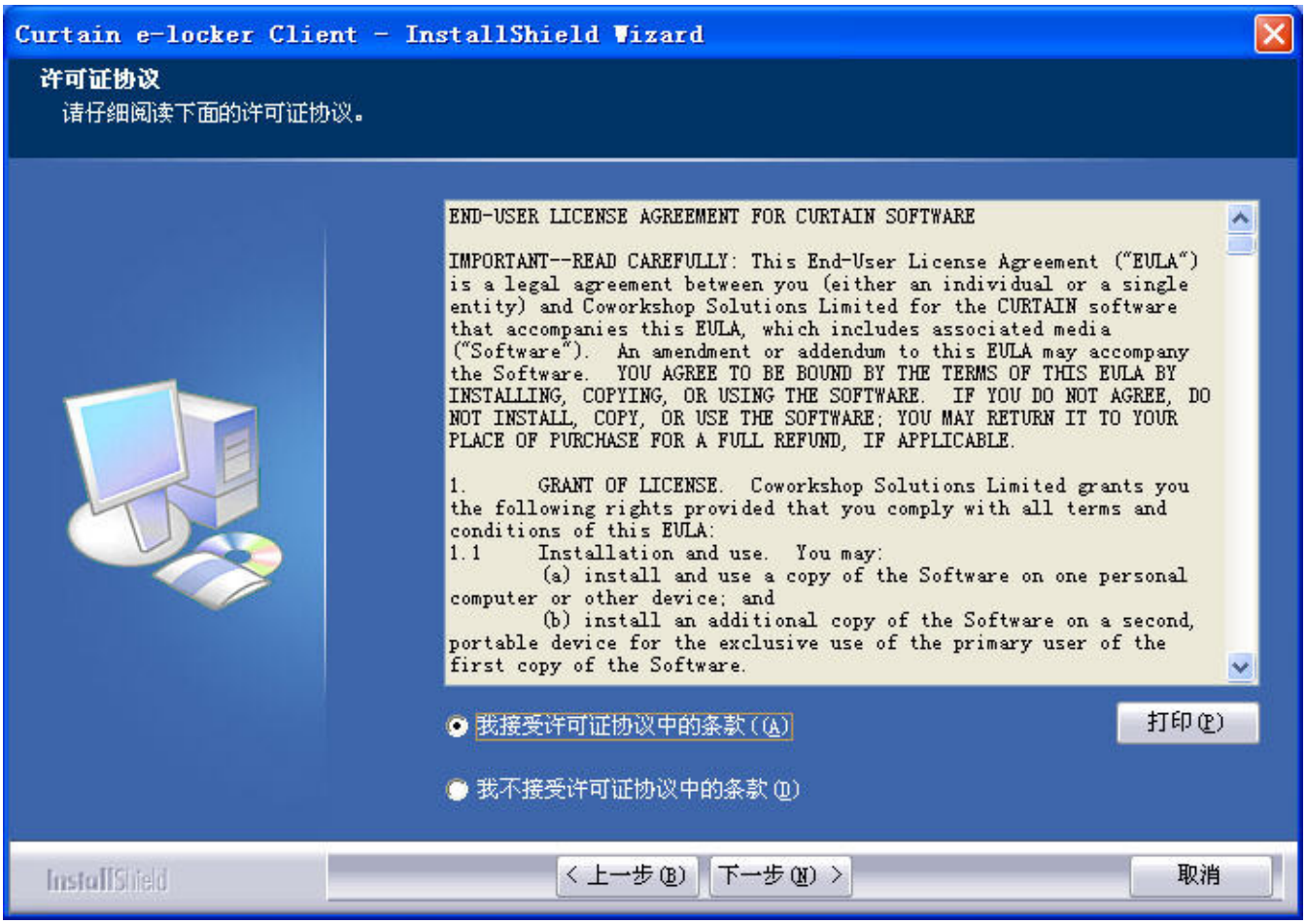
2. 解压安装包。

3. 执行Curtain客户端安装程序。请确保以Windows管理员身份登入。
接着，请选择安装程序的语言。

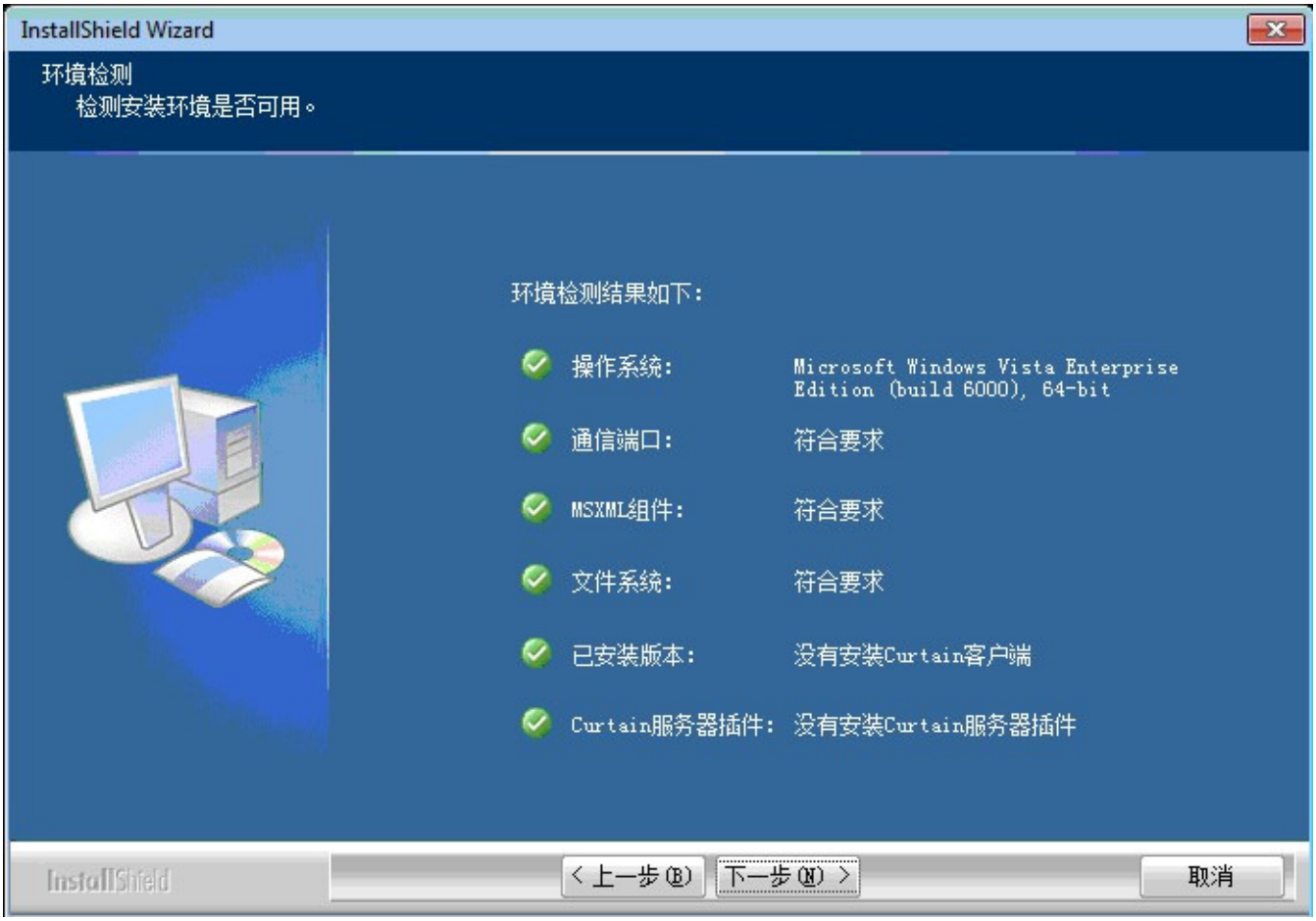



4. 选择安装程序的语言，并按确定。

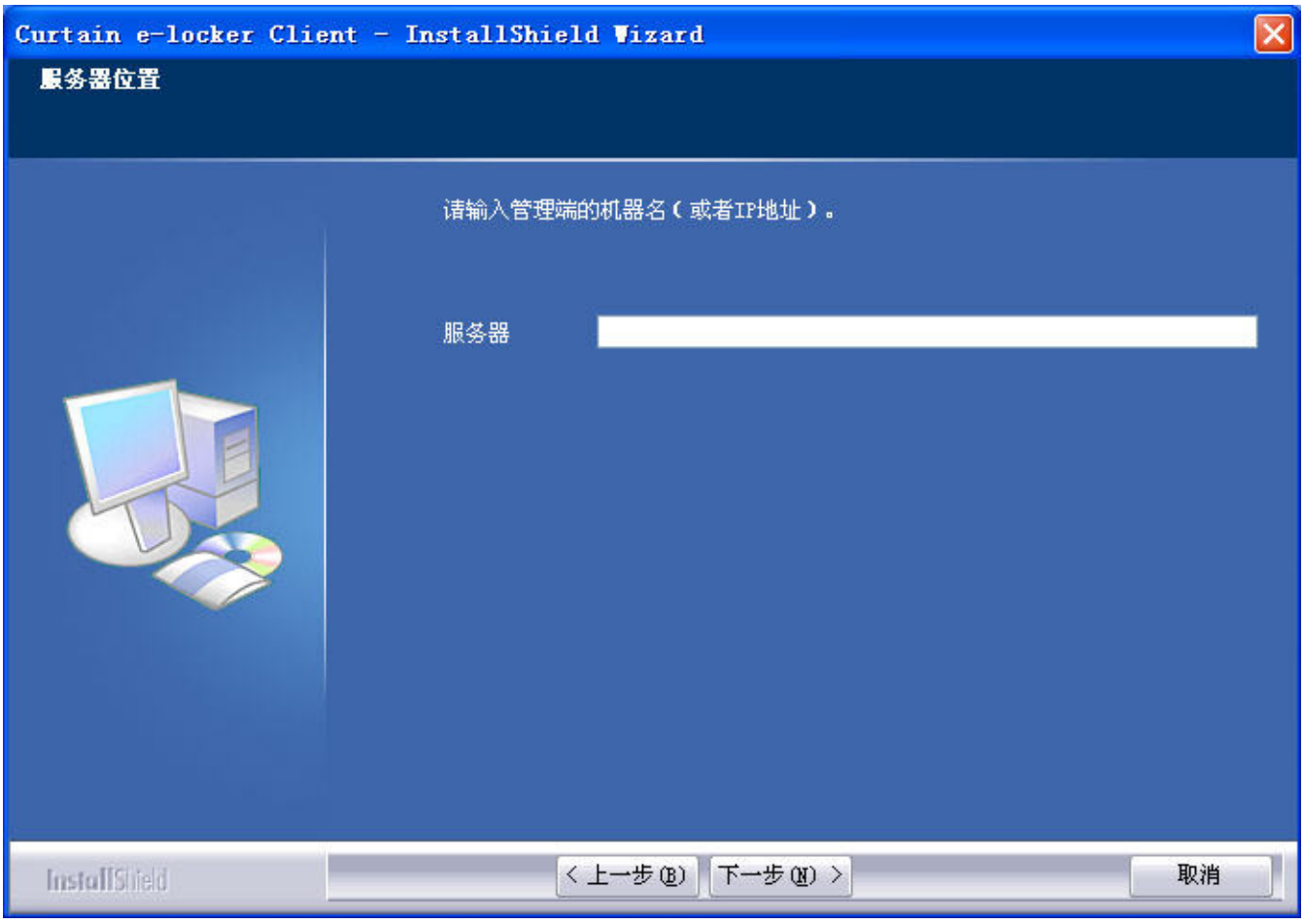
5. 阅读软件使用证协议。如同意协议内容，选择"我接受软件使用证协议"，并按下一步继续安装。



接着，安装程序会检测系统环境是否满足安装要求，请按下一步继续安装。



6. 输入Curtain管理员的IP地址或计算机名称(请确保输入正确。如不太肯定，请联络系统管理员)，并按下一步继续安装。




7. 选择安装程序的文件夹，并按下一步继续安装。

8. 按安装按钮，开始安装程序。

9. 完成安装后，请重启计算机。

备注：如果想通过Group Policy(群组原则)远程安装Curtain客户端，请参考FAQ 00201。

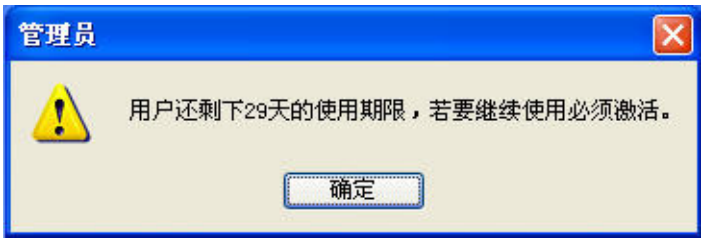
# 4 - 产品激活

## 4.1 - 产品激活

Curtain e-locker应用了产品激活技术来控制软件的使用证。如果没有进行产品激活，客户只可以使用Curtain e-locker三十天。期间，客户可以随意使用软件，以达至评估软件功能的目的。在三十天后，如果客户想延长测试期限，客户可以向我们或我们的代理商作出申请。

对于已经是Curtain e-locker的客户，客户应该于安装系统时进行产品激活。并且需要每年进行一次产品重新激活，以控制软件的使用证。我们会协助客户进行每年的重新激活而不收取任何费用(包括没有购买软件维护的客户)。关于产品激活的步骤，请参考相关文件。

当需要进行产品激活时，每当用户开启Curtain客户端或Curtain管理员时，系统会弹出提示信息。以下是相关提示信息。




于激活限期前三十天，系统会开始弹出提示信息。如果到激活限期时还未进行激活，用户将不能开启Curtain客户端和Curtain管理员，直至产品重新激活。

备注: 管理员只需要在Curtain管理员上进行产品激活，当Curtain管理员被成功激活后，所有Curtain客户端也会自动被激活。

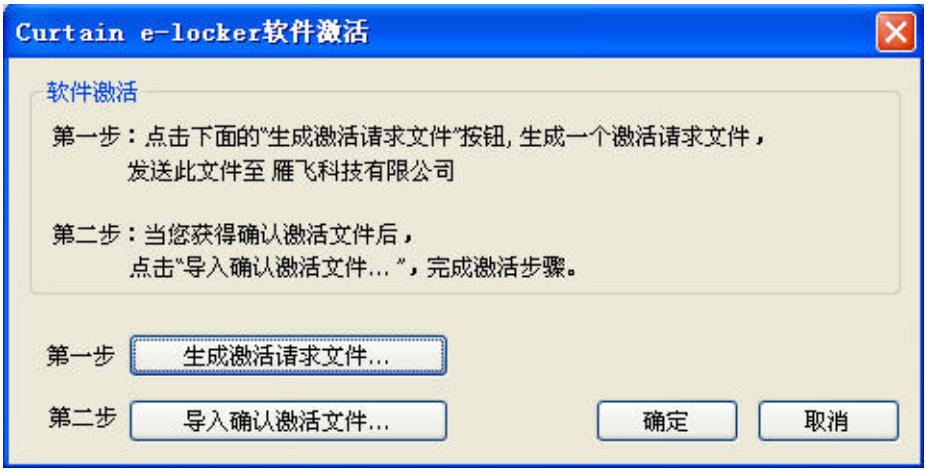
## 4.2 - 激活Curtain e-locker

当需要进行产品激活时，每当用户开启Curtain客户端或Curtain管理员时，系统会弹出提示信息。请按以下步骤进作产品激活。

激活Curtain e-locker的步骤:
1. 开启Curtain管理员。接着，系统会要求进行产品激活。

2. 按"是"开始产品激活(或按"否"跳过激活)。
如果你是初次进行产品激活，请输入25个位的产品钥匙。
如果这是每年的产品重新激活，请跳到步骤4继续。


3. 输入产品钥匙(请注意大小写)和公司资料，完成输入后按确定继续。
接着，系统会显示以下对话框。

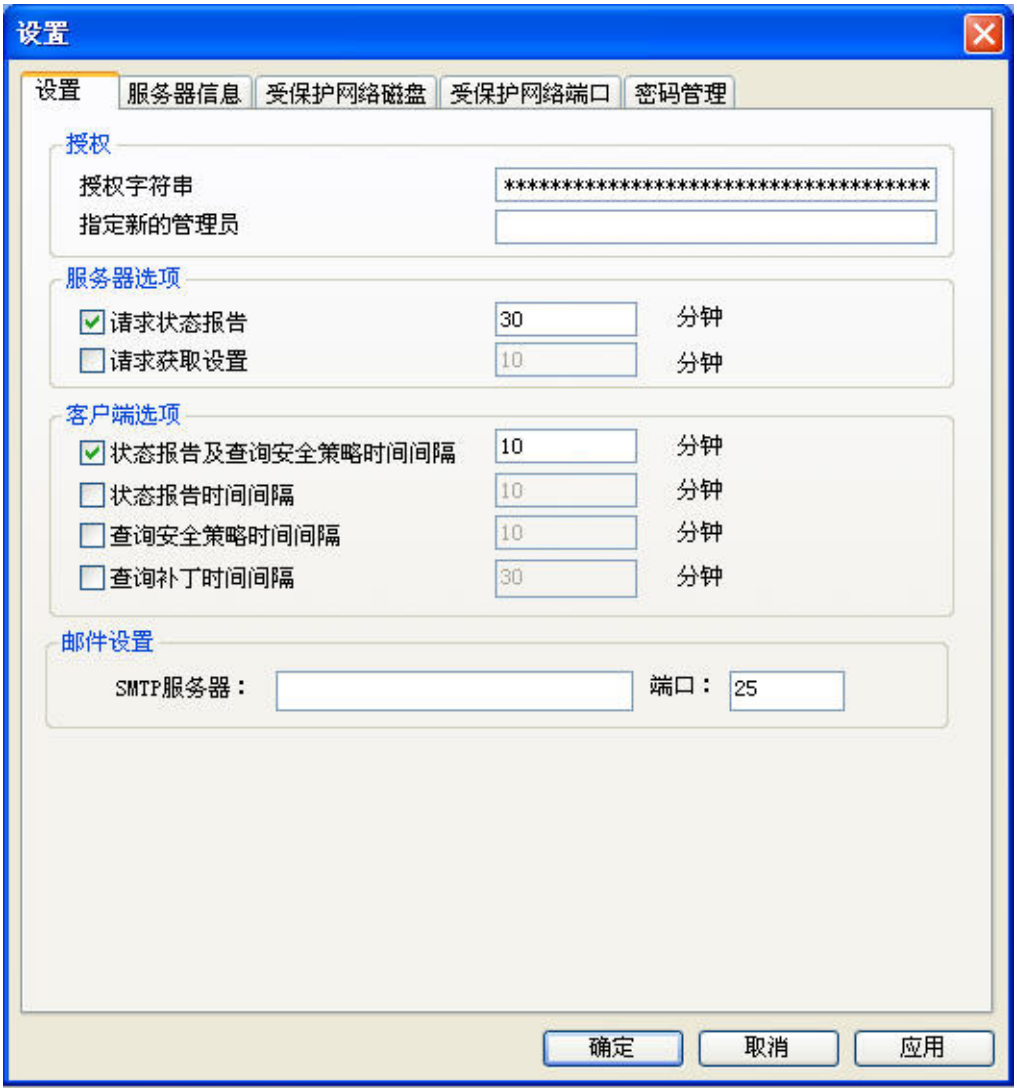



4. 按"生成激活请求文件"按钮将"要求激活文档"保存，并将该文档发送给我们(registration@coworkshop.com)。
我们收到要求激活文档后，我们会把以下文档发送回给你。
如果这是初次产品激活，你将会收到两个文档(确认码和授权字符串)
如果这是每年的产品重新激活，你将会收到一个文档(确认码)

5. 当收到确认码后，请按"导入确认激活文件"，并选择确认码文档。按确定按钮后，系统会显示以下信息。

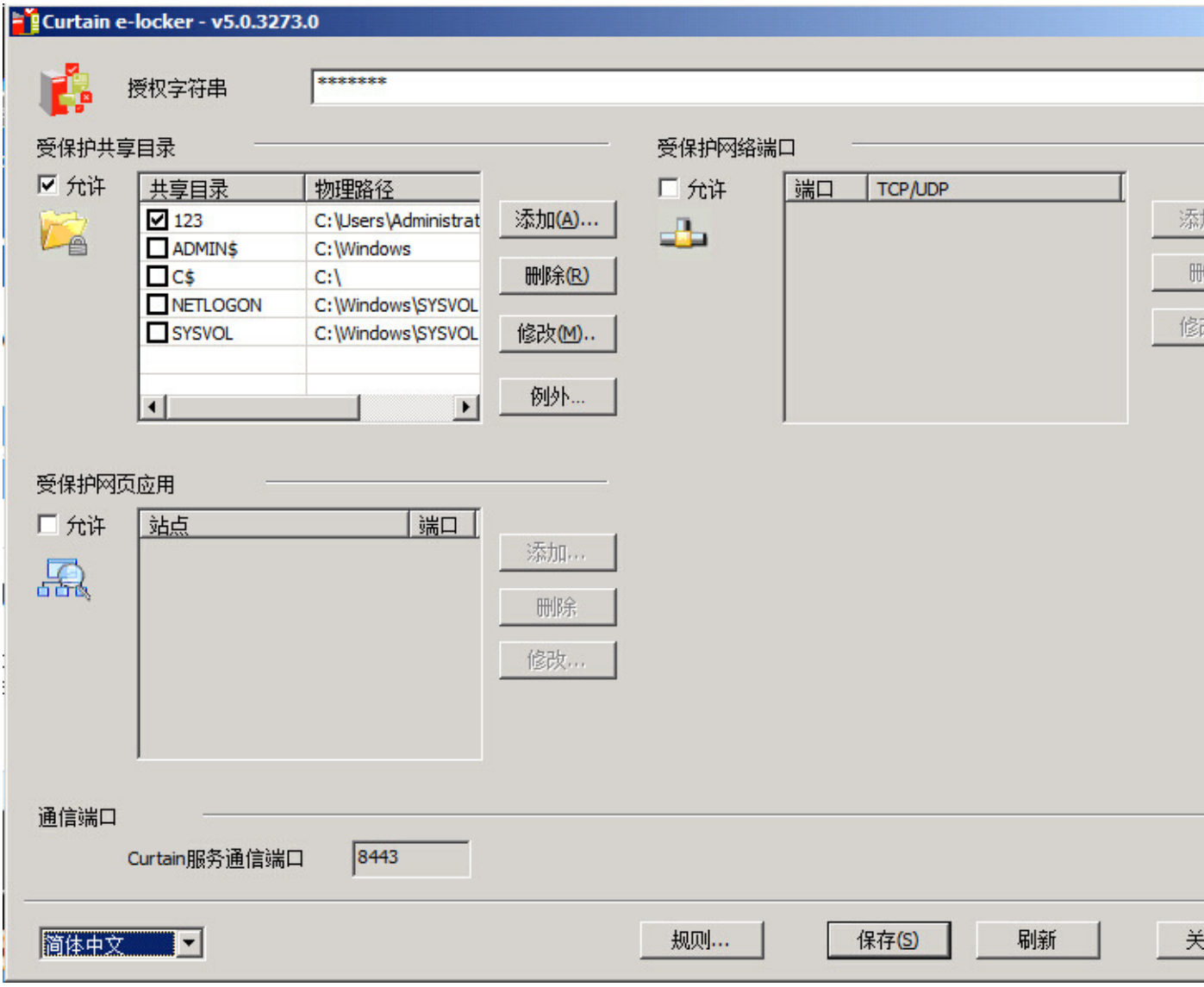

如果这是初次产品激活，请跳到下一个步骤继续。
如果这是每年的产品重新激活，你已经成功完成了重新激活。

6. 在Curtain管理员，于菜单上选择"文件>设置"。接着，系统会显示"设置"对话框。
请输入授权字符串，并按确定。




如果你为了保护服务器上的资料(如:共享文件夹等)，在服务器上只单独安装了Curtain服务器插件，请按步骤7至10把授权字符串输入到Curtain服务器插件上。

7. 启动"安全网络管理" (于"开始 > 程式 > Coworkshop Curtain e-locker"下)。




8. 输入授权字符串,并按"保存"。

9. 按"刷新"来应用新的设定。

10. 按"关闭"离开。

恭喜! 你已经成功完成了产品激活。

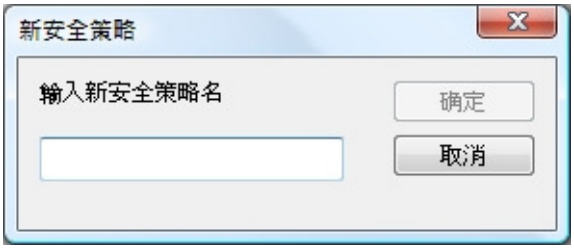
# 5 - 设置

## 5.1 - 新增安全策略群组

管理员可以建立多个安全策略群组来管理不同的电脑或用户，我们建议用Default Policy安全策略群组来保护大部份的电脑或用户，以下是安全策略群组例子以供参考。
- Default Policy: 用于一般用户，不容许列印和保存受保护文档到受保护区以外。
- Managers: 用于管理人员，容许列印和保存受保护文档到受保护区以外。
- Notebooks: 用于手提电脑: 对于手提电脑，不容许列印和保存受保护文档到受保护区以外，并且电脑必需每72小时连接Curtain管理端才能继续使用本地受保护区内的文档。

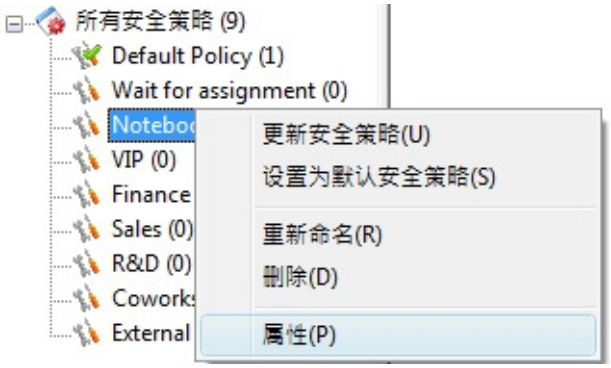
以下是新增安全策略群组的步骤:
1. 在Curtain管理员菜单，选择"文件>新建安全策略"。接着，系统会要求你输入新建的安全策略名称。

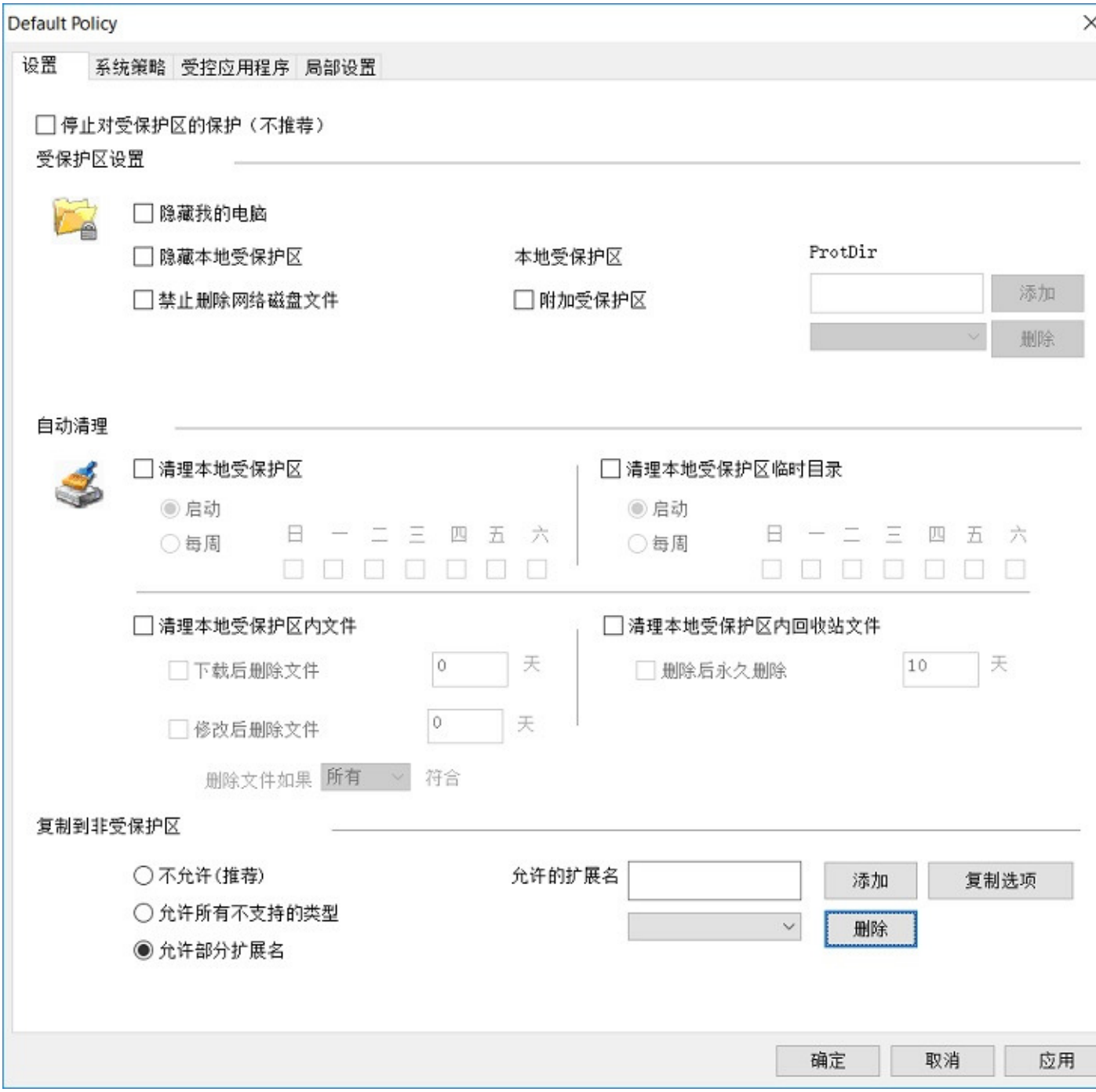

2. 输入新建的安全策略名称，并按确定。




## 5.2 - 修改安全策略群组的设定

修改安全策略群组设定的步骤:
1. 在Curtain管理员，点选一个安全策略，按鼠标右键，并选择"内容"。


所有安全策略 (9)
Default Policy (1)
Wait for assignment (0)
Notebo
VIP (0)
Finance
Sales (0)
R&D (0)
Cowork
External
更新安全策略(U)
设置为默认安全策略(S)
重新命名(R)
删除(D)
属性(P)


Default Policy
设置
系统策略
受控应用程序
局部设置
停止对受保护区的保护（不推荐）
受保护区设置
隐藏我的电脑
隐藏本地受保护区
禁止删除网络磁盘文件
本地受保护区
附加受保护区
ProtDir
添加
删除
自动清理
清理本地受保护区
启动
每周
日 一 二 三 四 五 六
清理本地受保护区临时目录
启动
每周
日 一 二 三 四 五 六
清理本地受保护区内文件
下载后删除文件
0
天
修改后删除文件
0
天
删除文件如果
所有
符合
清理本地受保护区内回收站文件
删除后永久删除
10
天
复制到非受保护区
不允许(推荐)
允许所有不支持的类型
允许部分扩展名
允许的扩展名
添加
复制选项
删除
确定
取消
应用

以下是一个安全策略群组的设置简介:

于"设置"页
- 停止对受保护区的保护
- 附加本地受保护区
- 本地受保护区的自动清理
- 用扩展名设定"复制出去"策略
- "加密出去"策略

于"系统策略"页
- 在线/离线控制

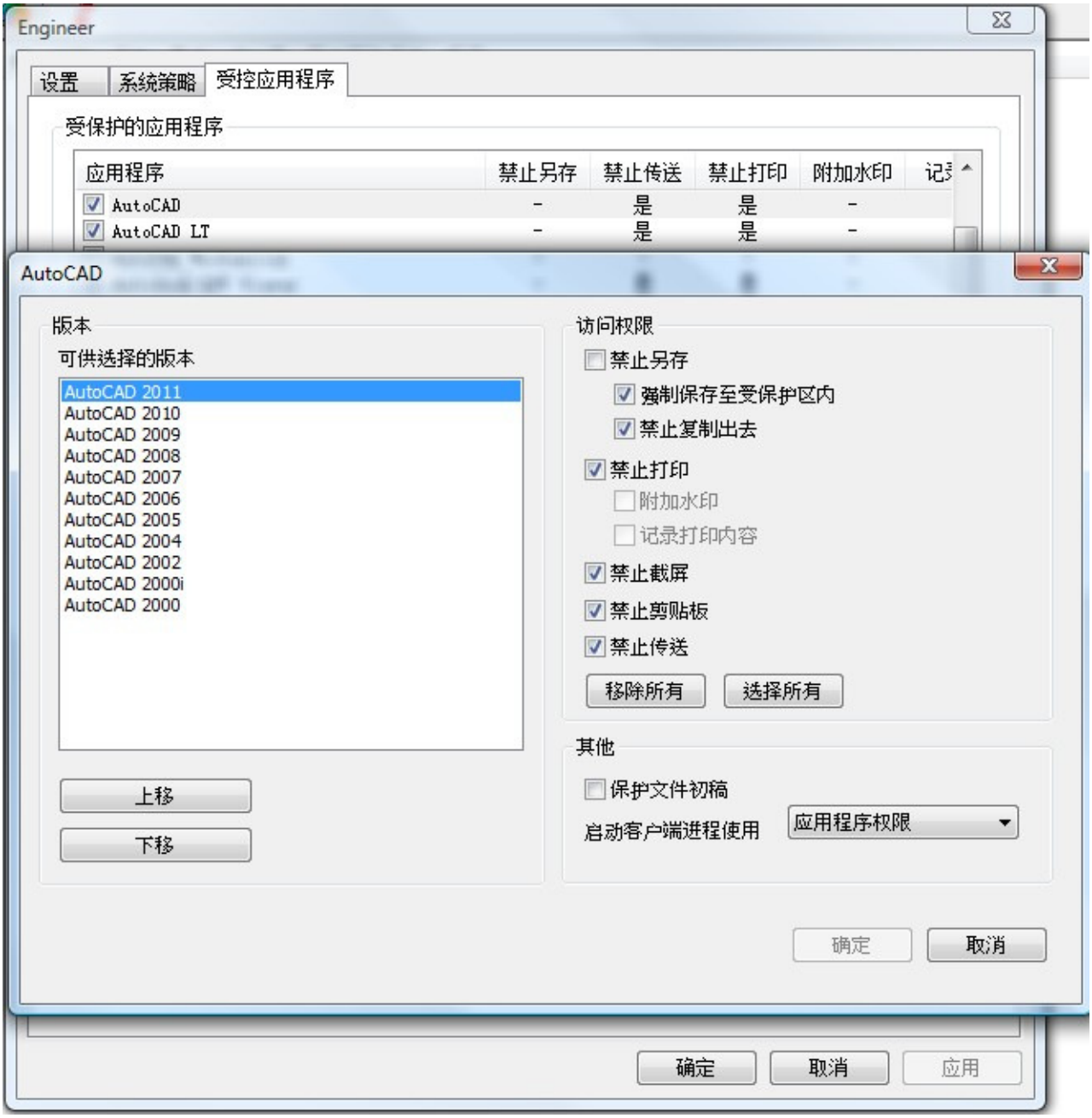
于"受控应用程序"页
- 设定如何控制应用程序使用受保护文档 (如:不容许列印和保存受保护文档到受保护区以外)

于"局部设置"页
- 设定此安全策略群组外发申请的审批人
- 设定此安全策略群组所包括的打印机

这里我们集中于"受控应用程序"页面的设定，其他的功能，请参考第六章。

2. 于"受控应用程式"页，双击你想修改设定的应用软件。

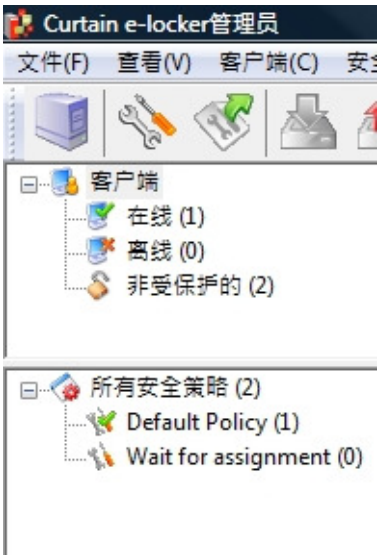
3. 修改Curtain权限控制，并按确定键确认。




4. 重覆步骤2至步骤3去修改其他应用软件的设定。

## 5.3 - 设定默认策略

当一个安全策略群组被设定为默认策略时，所有新安装的Curtain客户端会自动被指派到该安全策略。系统会在默认策略上加上绿色勾号以作识别。当在刚刚完成安装后第一次开启Curtain管理员，默认策略是"Default Policy"。




系统有两个预设的安全策略群组。
- Default Policy: 这个策略群组的预设控制是比较严谨的。用户可以如常使用受保护区内的机密文档，但是他们不能将文档带出受保护区。
- Wait for Assignment: 这个策略群组的预设控制是完全不容许用户阅读或修改受保护区内的机密文档。

所有新安装的Curtain客户端都会先连接到Curtain管理员，并自动被指派到默认安全策略。如果管理员想先确认Curtain客户端然后才容许它们阅读或修改受保护区内的机密文档，管理员可以将"Wait for Assignment"设定为默认策略。设置后，所有新安装的客户端都需要管理员指派它们到合适的安全策略才能使用机密文档。

将一个安全策略群组设定为默认策略的步骤:
1. 在Curtain管理员，点选一个安全策略，按鼠标右键。

2. 选择"设定为预设安全策略"


3. 完成

## 5.4 - 按用户/用户群组来配置安全策略

Curtain e-locker的安全策略可应用于计算机或用户/用户组。如果您希望通过AD用户/用户组授予安全策略，则需要连接AD以将用户信息导入Curtain管理员。当第一次Curtain管理员获取用户信息时，系统将使用默认安全策略来控制该用户/用户组。管理员需要手动将用户/用户组分配到适当的安全策略中。

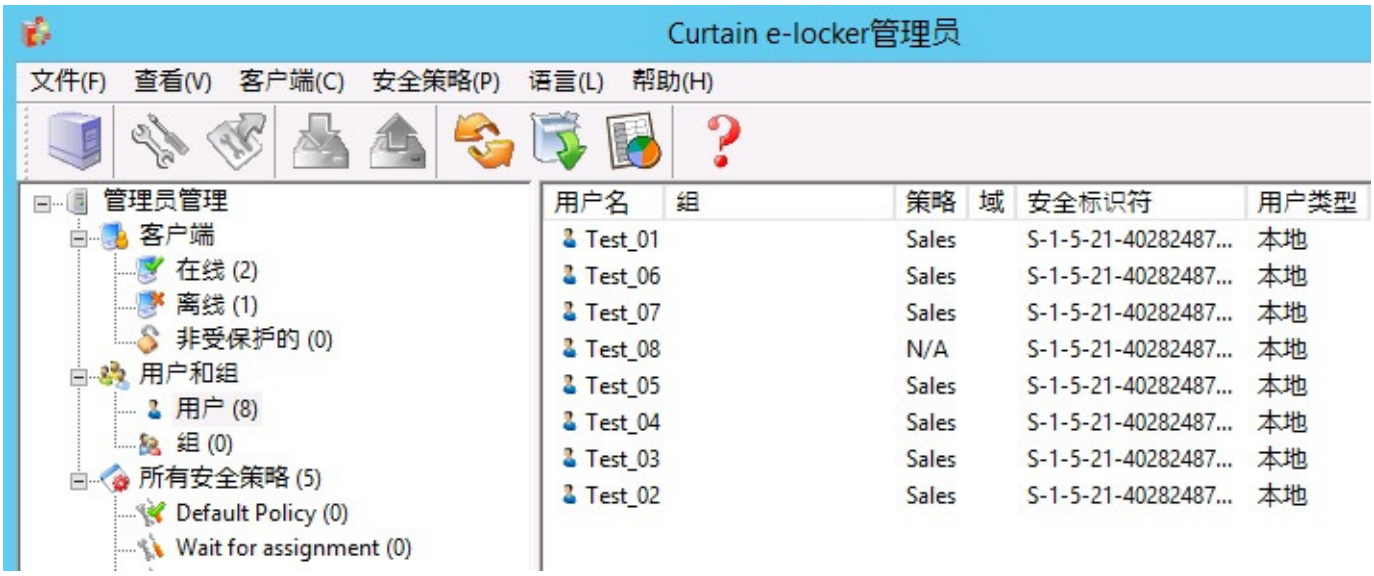
要按用户/用户组授予安全策略，请按照以下步骤在Curtain管理员中启用 “按用户分配” 。

在Curtain管理员中启用“按用户分配”的步骤：

1. 运行Curtain管理员，打开文件 -> 设定 -> 策略分配方式 。

2. 选择“按用户分配”，单击“确定”键。


然后“用户和组”将显示在Curtain管理员中。




3. 完成。

从AD域导入用户和用户组的步骤：

1. 运行Curtain管理员，打开文件 -> 设定 -> LDAP。

2. 选“启用LDAP”键。

3. 在“LDAP服务器地址”上输入LDAP服务器地址，DNS或IP地址。

4. “LDAP服务器端口”，默认端口为389。

5. 建议启用“使用安全LDAP连接”，表示使用安全的LDAP连接到AD（默认为不启用）。

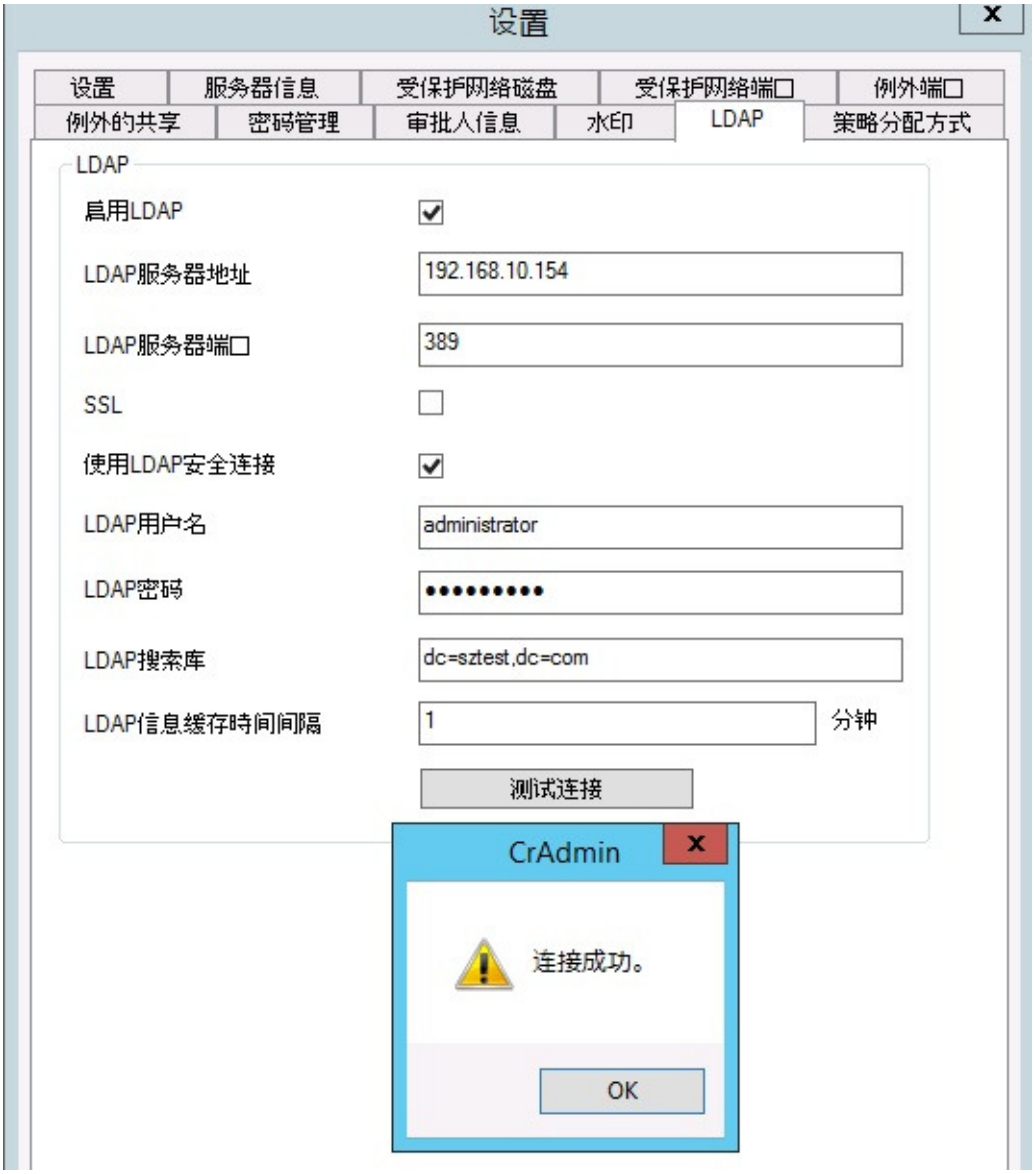
6. 在“LDAP用户名”下输入用户名，以连接LDAP服务器。

7. 在“LDAP密码”中输入密码。

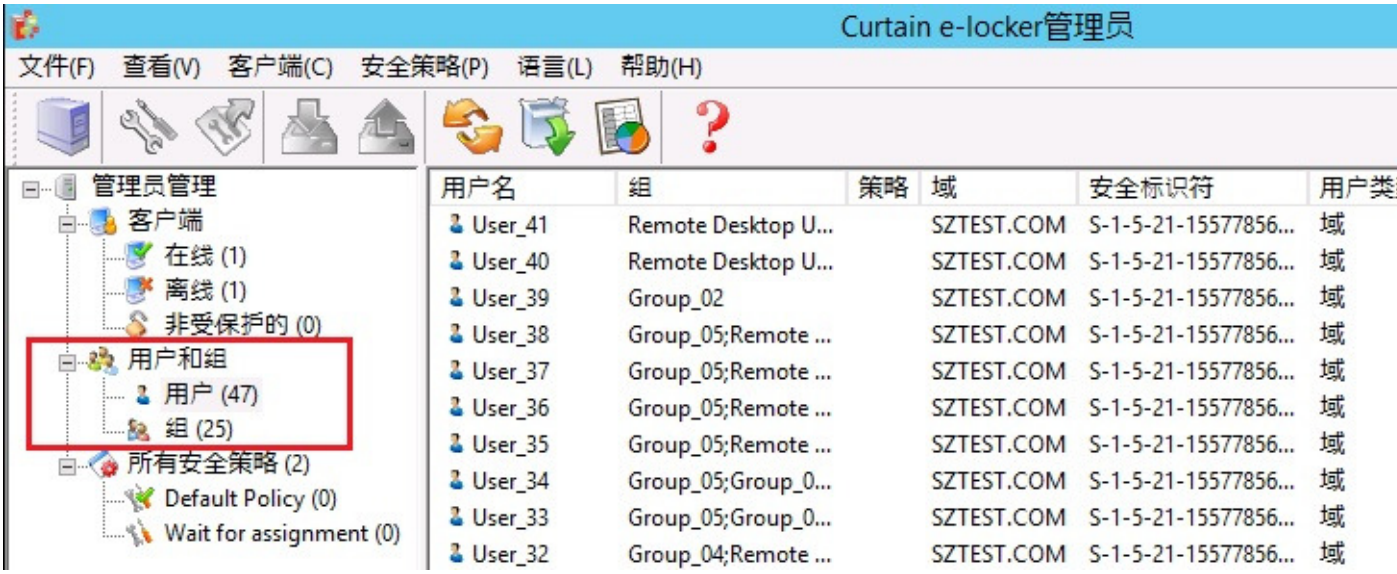
8. “LDAP搜索库”，输入用户或用户组的根，可输入CN，OU和DC。
   - 例如搜索整个域，可以输入“dc=域名，dc=域后缀”（例如：“dc=test，dc=com”）。
   - 例如搜索整个组，可以输入“ou=组织单元名称，dc=域名，dc=域后缀”（例如：“ou=it，dc=test，dc=com”）。
   - 例如搜索某用户，可以输入“cn=用户名，ou=组织单元名称，dc=域名，dc=域后缀”（例如：“cn=tester，ou=it，dc=test，dc=com”）。

9. “LDAP信息缓存”，用于AD的设置缓存信息（默认为15分钟）。

10. 设置完成后，单击“测试连接”键查看是否成功连接到AD。



11. 如果AD用户/用户组已成功导入Curtain管理员，则它们将显示在Curtain管理员中的 “用户和组” ，如下图。



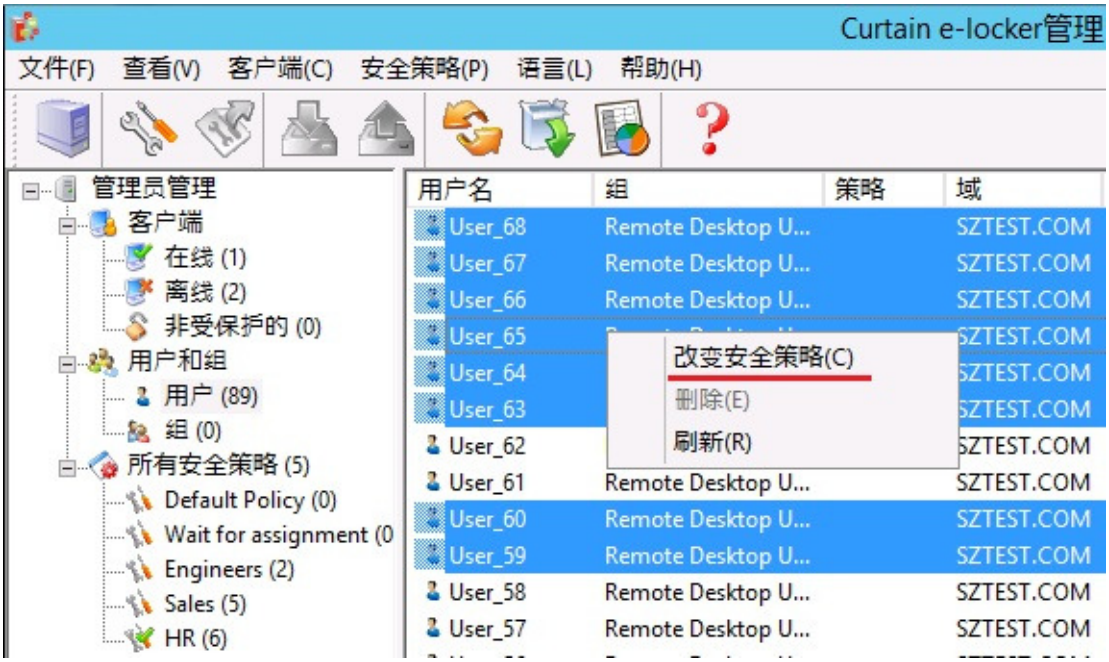

12. 完成。

备注： 对于本地/工作组用户，一旦他们打开Curtain客户端，它们将被列在 “用户和组” 下。

指派用户/用户组到合适的安全策略的步骤：
1. 在Curtain管理员中，左面控制板中选择用户/用户组。然后，用户/用户组将在右面控制板中列出。


2. 选择用户/用户组（按Ctrl键可选择多个用户/用户组）。

3. 右键单击并选择 “改变安全策略” 以将用户/用户组分配给适当的安全策略中。

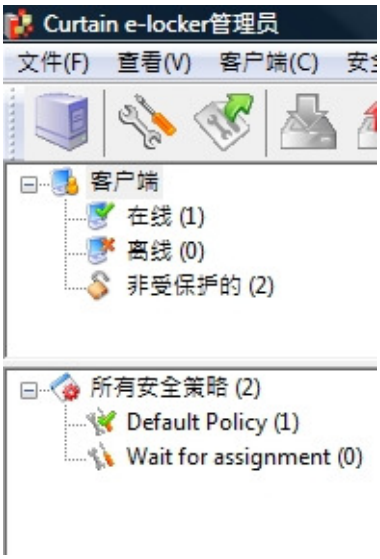



4. 重复步骤2-3，将其他用户/用户组分配到适当的安全策略。

5. 完成。

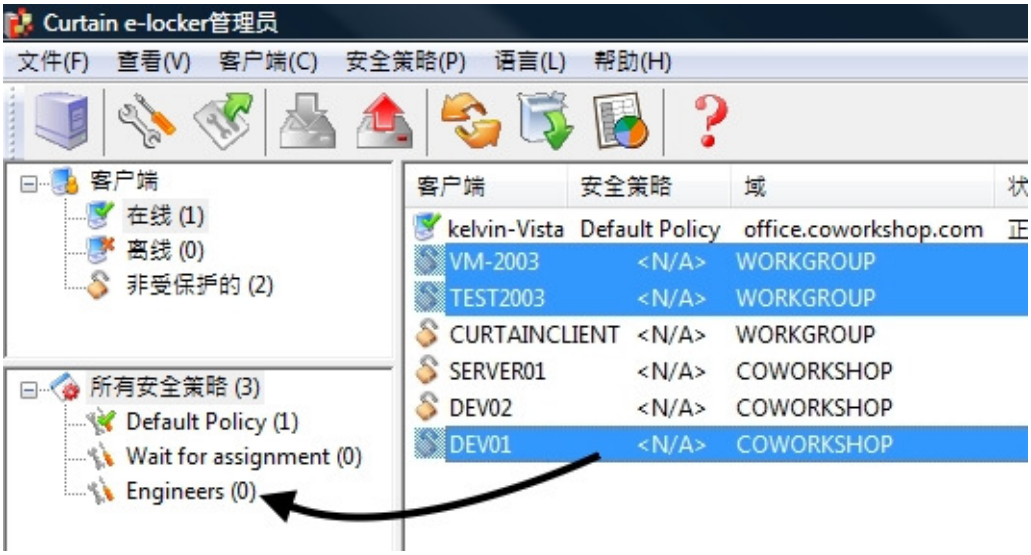
## 5.5 - 指派计算机/用户到合适的安全策略

指派Curtain客户端到合适的安全策略的步骤:
1. 在Curtain管理员左手面的控制板，点选"在线"或"离线"。




2. 选择用户计算机(按Ctrl键可选择多台计算机)。

3. 将选择好的用户计算机拖放到合适的安全策略。



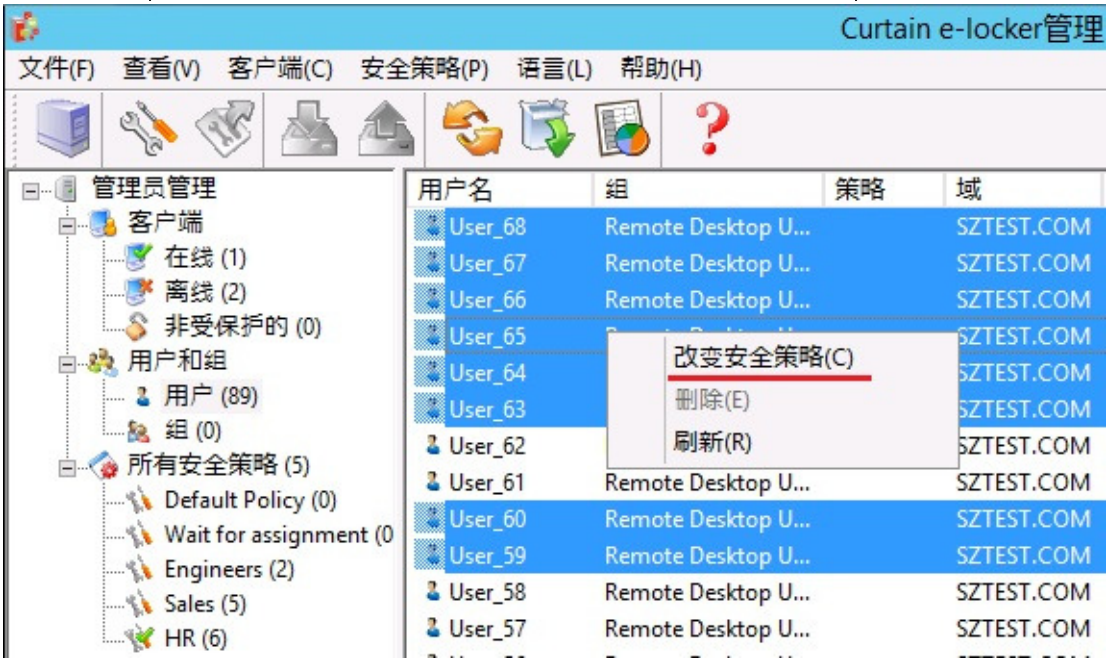

4. 重覆步骤2至步骤3，将其他Curtain客户端指派到合适的安全策略。

5. 完成。

指派用户到合适的安全策略的步骤：
1. 在Curtain管理员左手面的控制板，点选“用户/组”。


2. 选择用户/组(按Ctrl键可选择多个用户)。

3. 选择好用户/组后，点击鼠标右键，弹出面板中选择“改变安全策略”，将用户/组选择到合适的安全策略中。




4. 重覆步骤2至步骤3，将其他用户/组指派到合适的安全策略。

5. 完成。

## 5.6 - 设定服务器上的受保护区

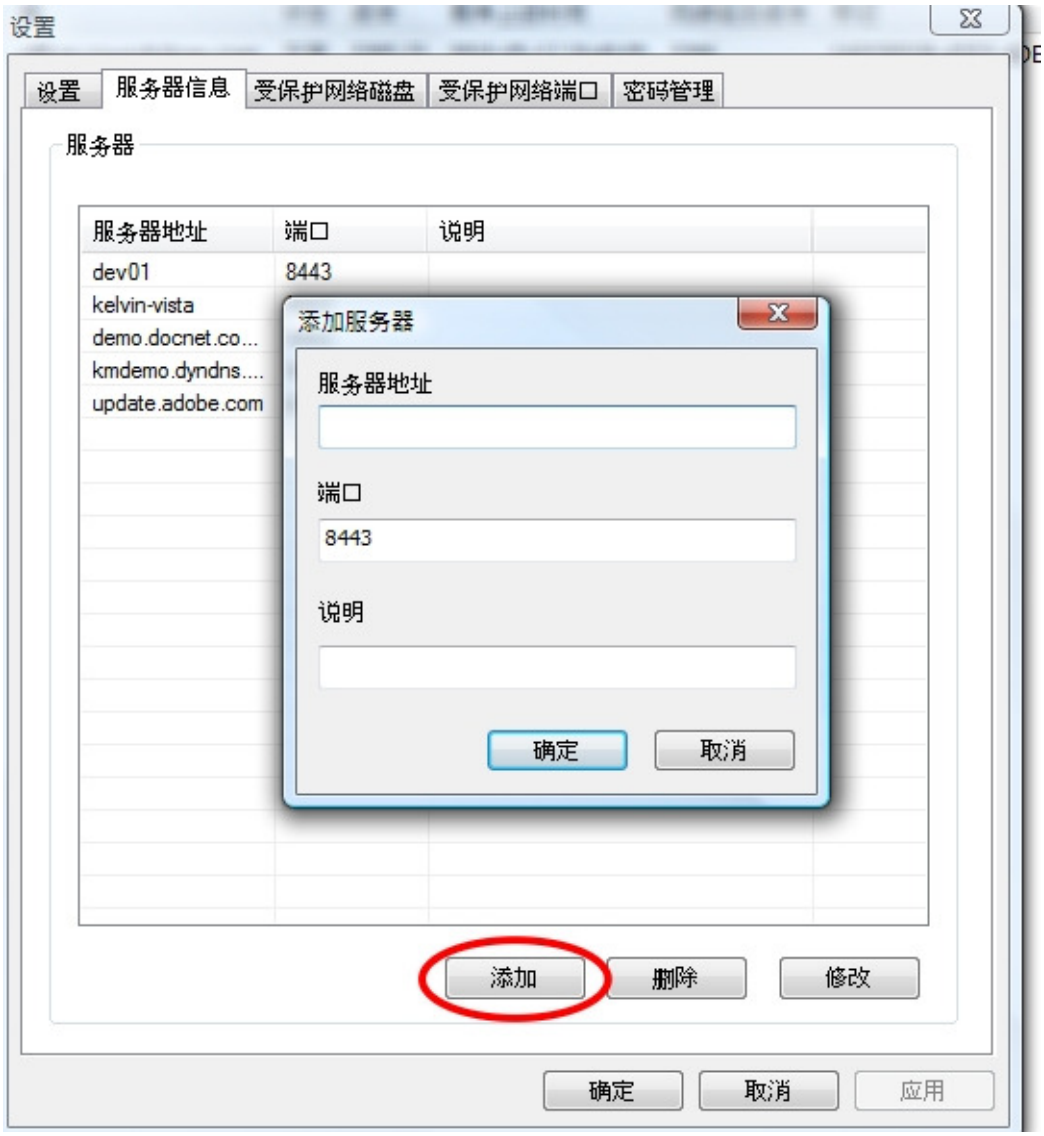
Curtain e-locker可以用来保护不同服务器上的资源(如:Windows文件服务器上的共享文件夹、网站、甚至自己开发的应用或后台系统)。请按以下的步骤来设定服务器上的受保护区。

设定服务器上受保护区的步骤:
1. 在Curtain管理员，于菜单上选择"文件>设置"。

2. 于"服务器信息"页，按"添加"按纽来新增服务器。举例:如果你想保护两台Windows文件服器上的共享文件夹和一个应用网站，你需要将那三台服务器添加在此页。

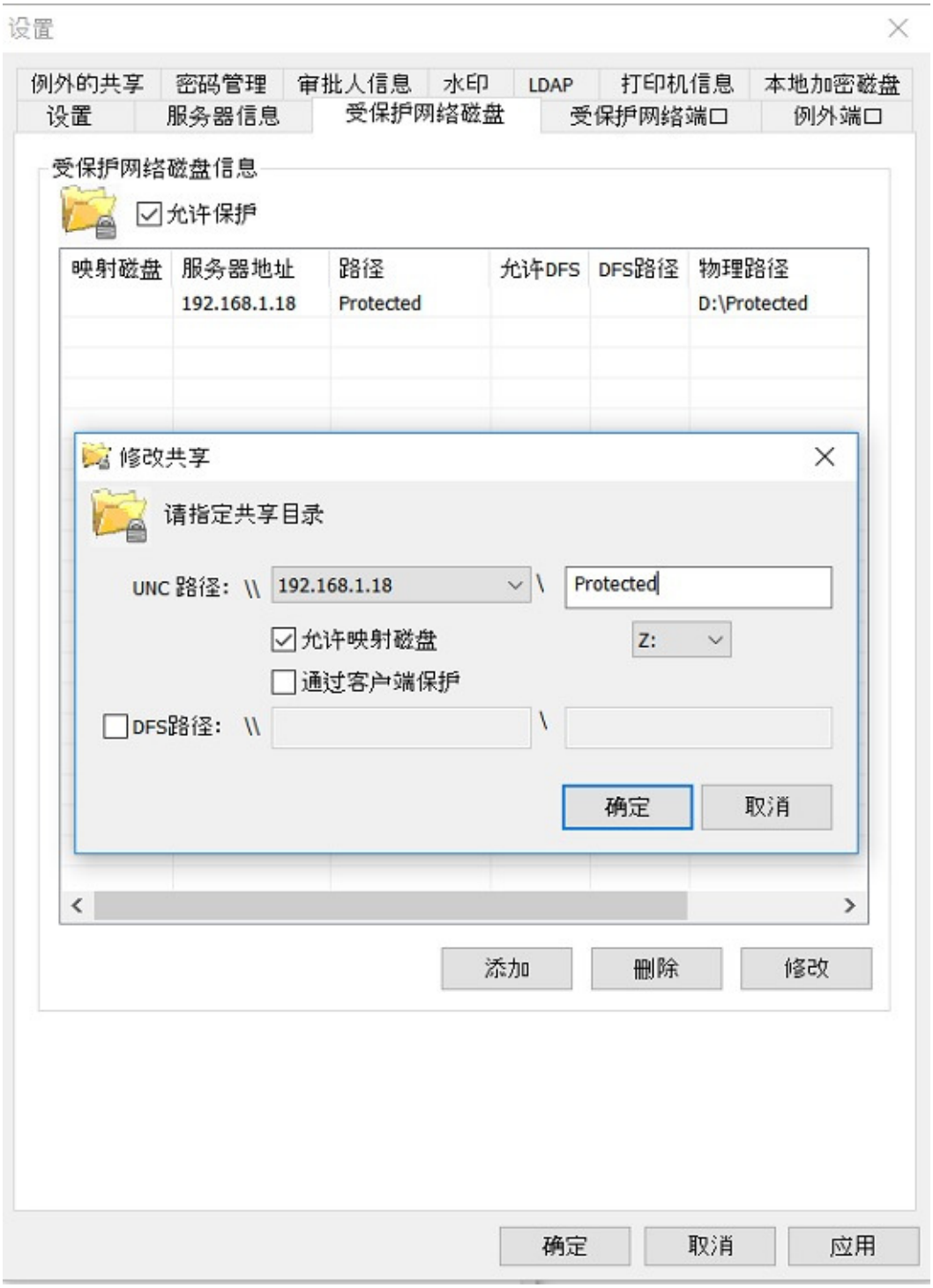
服务器地址: 服务器的计算机名称或IP地址。

端口: 默认的端口是8443(用作Curtain管理员和Curtain服务器插件之间的沟通)。




3. 新增服务器上受保护区。

情况1 - 保护Windows文件服器上的共享文件夹
- 于"受保护网络磁盘机"页，点选"允许保护"。
- 按"添加"按纽，系统会弹出对话框。




UNC路径: \\服务器\分享名称

- 服务器 - 选择服务器(计算机名称或IP地址)
- 分享名称 - 输入分享名称(不是文件夹名称，除非你使用文件夹名称来命名分享)

允许映射磁盘机: 如果你想Curtain客户端于启动时自动映射到指定的磁盘机，请点选此选项并选择磁盘机。要不然，用户需要手动进行磁盘机映射。

通过客户端保护: 此选项只适用于你需要保护没有安装Curtain服务器插件的共享文件夹(如: NAS - Network Attached Storage)。

DFS路径: 如果在上述的共享文件夹是由DFS(Distributed File System)来管理的，请点选此选项。

- 服务器 - 输入服务器名称(用户应该在我的网络上看到该服务器名称)
- 路径 - 输入路径(用户应该在我的网络上看到该路径)

情况2 - 保护应用网站
- 于"受保护网页应用"，点选"允许保护"。
- 按"添加"按钮，系统会弹出对话框。

受保护网页服务器: http://服务器:端口

- 服务器 - 选择服务器(计算机名称或IP地址)
- 端口 - 输入端口(大部份的应用网站都是用80的)

通过SDK保护: 如果应用网站使用我们的SDK(software development kit)来跟Curtain e-locker作出整合，请选择此选项。

通过服务器插件保护: 如果应用网站并没有专门跟Curtain e-locker作出整合，请选择此选项。

受保护上传位置: http://服务器/路径

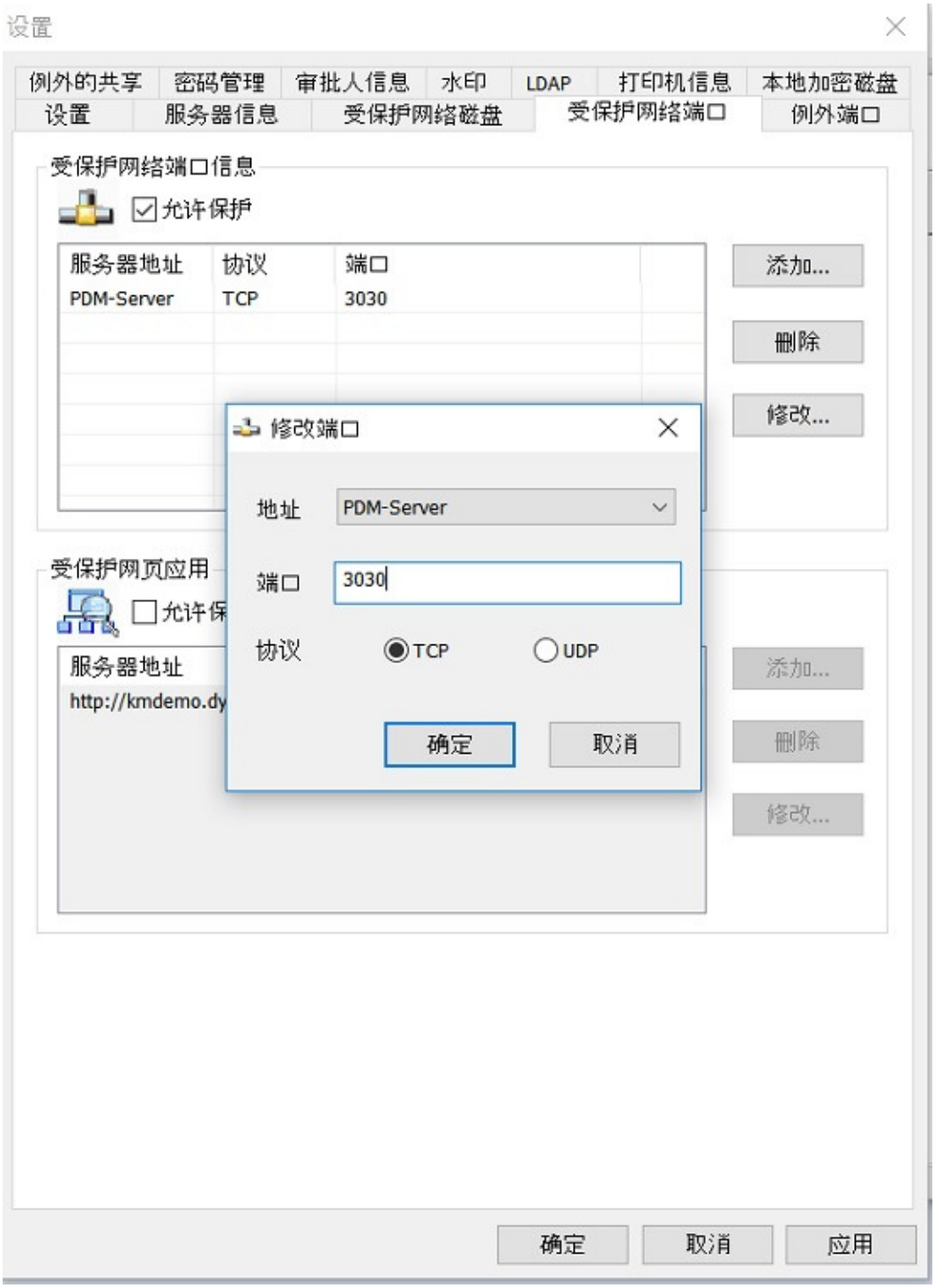
- 路径 - 输入你想保护的路径

例子1 - Microsoft SharePoint (如:http://SharePoint服务器/Site)
- 管理员可以于SharePoint上建立很多Site。如果管理员只想用Curtain e-locker来保护其中一些Site，管理员可以于路径上输入Site名称。设置后，用户需要使用受保护的Internet Explorer浏览器来访问受保护的Site，所有在这个Site内的资料都被Curtain e-locker保护起来。

例子2 - IBM Lotus Quickr (如:http://Lotus Quickr服务器/Place)- 管理员可以于Lotus Quickr上建立很多Place。如果管理员只想用Curtain e-locker来保护其中一些Place，管理员可以于路径上输入完整Place的路径(如: quickr/place1.nsf)。设置后，用户需要使用受保护的Internet Explorer浏览器来访问受保护的Place，所有在这个Place内的资料都被Curtain e-locker保护起来。

如果管理员想保护整个应用网站，请输入"<PROTECTALL>"。

情况3 - 保护网络端口(用于SolidWorks PDMWorks)
- 于"受保护网络端口信息"，点选"允许保护"。
- 按"添加"按钮，系统会弹出对话框。




- 地址 - 选择服务器(计算机名称或IP地址)
- 端口 - 输入端口(PDMWorks的默认值是3030)
- 协议 - 选择协议(PDMWorks的默认协议是TCP)

4. 按确定键确认

## 5.7 - 保护共享文件夹下的子文件夹

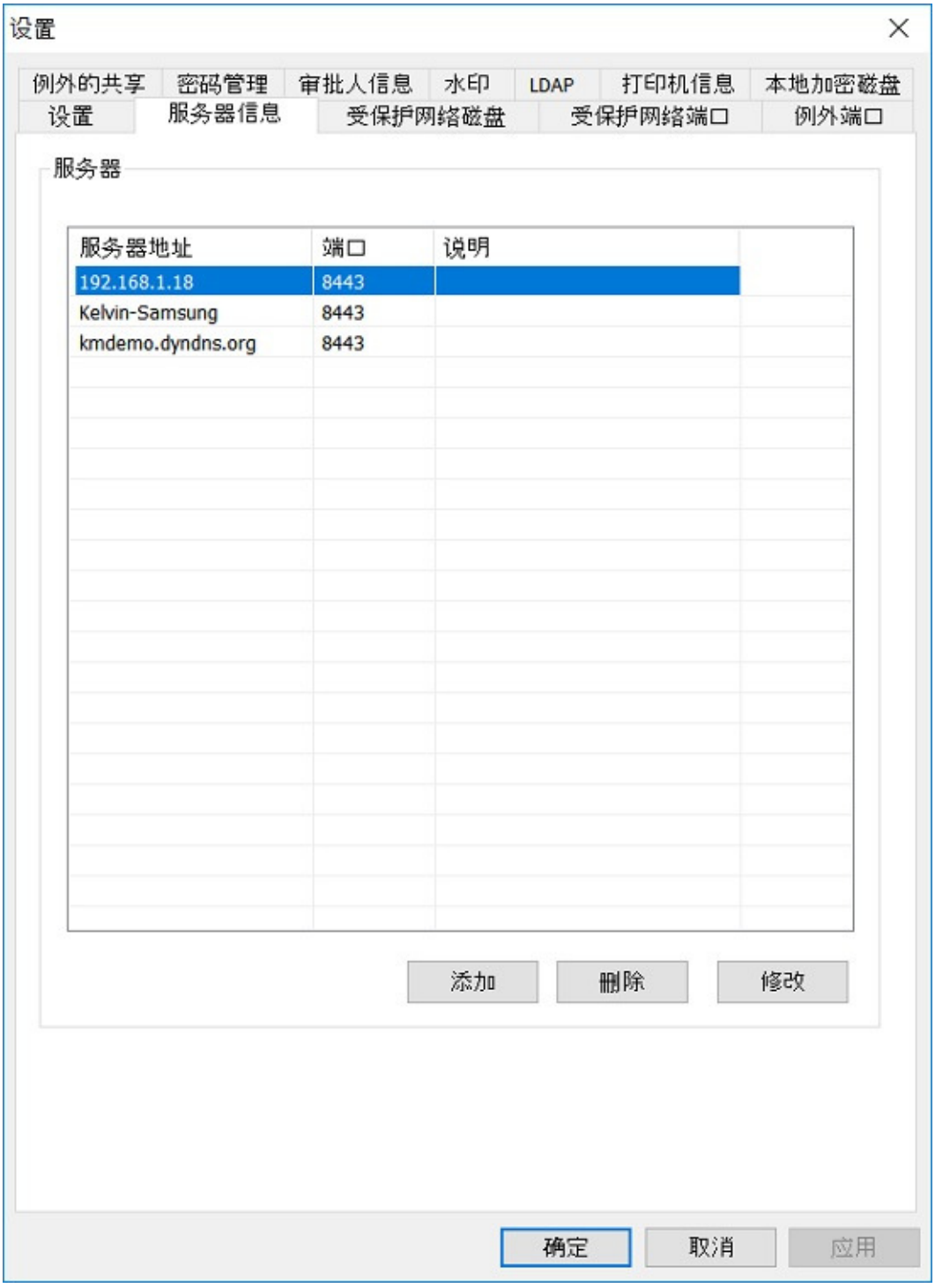
举例：文件伺服器上有一个共用文件夹pro（根目录）,下面分别有pro1, pro2, pro3 ... pro9共9个子文件夹（子目录），假如目前仅需要保护3个子文件夹即pro1 , pro2, pro3 ，其他的子文件夹不用受Curtain e-locker保护，那么如何来实现这一需求？

方法一：
在文件伺服器上，把那些需要保护的子文件夹设定为共享文件夹(即是pro1, pro2, pro3)，并且于Curtain管理端"受保护网路磁碟机"内设定为受保护的共享文件夹。

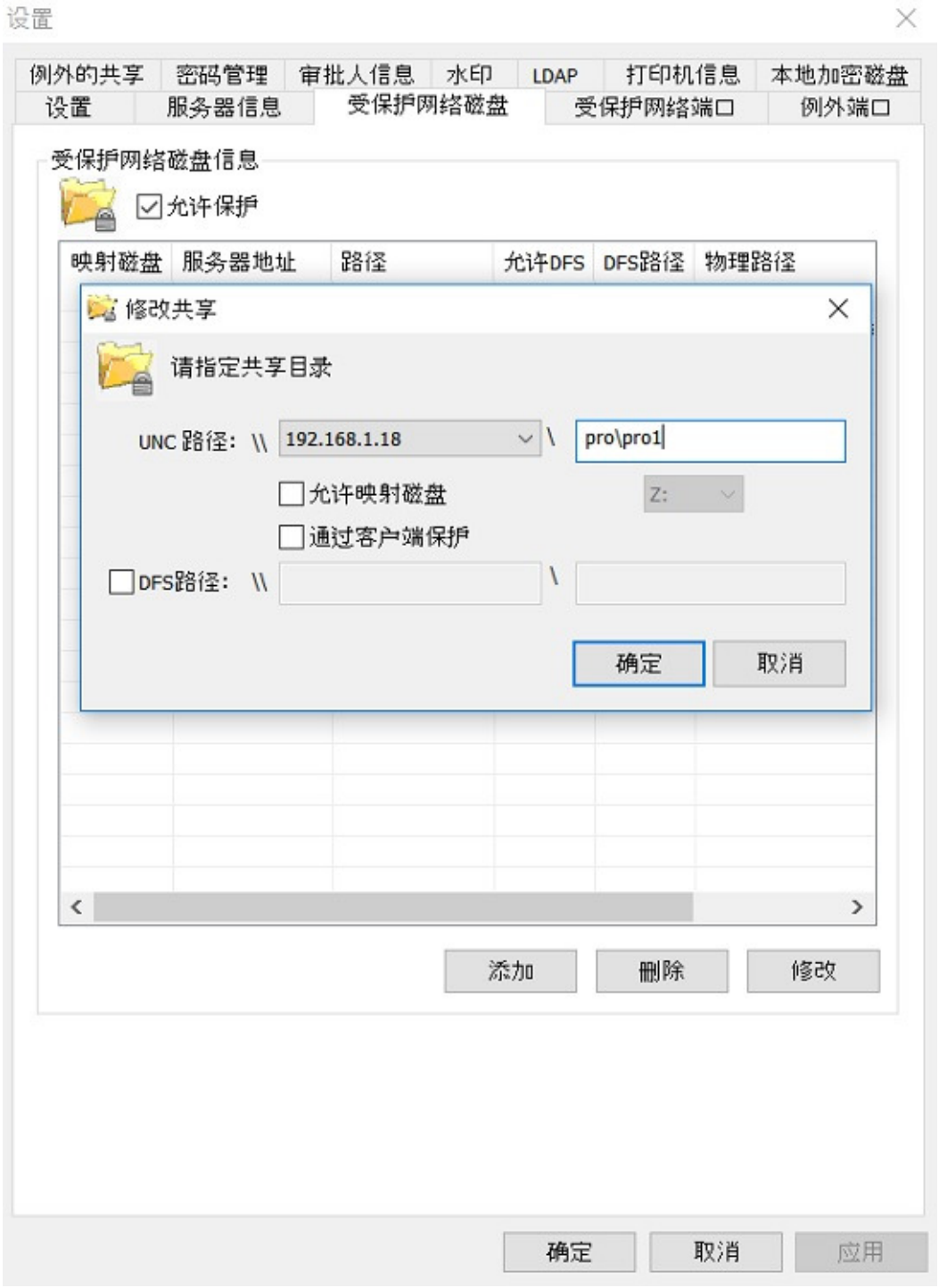
方法二：
不用于文件伺服器上把那些需要保护的子文件夹设定为共享(即是pro1, pro2, pro3)，只需要于Curtain管理端"受保护网路磁碟机"内直接将子文件夹设定为受保护即可，请参考以下步骤。

直接将子文件夹设定为受保护的步骤:
1. 在Curtain管理端，于菜单上选择"文件> 设定"。

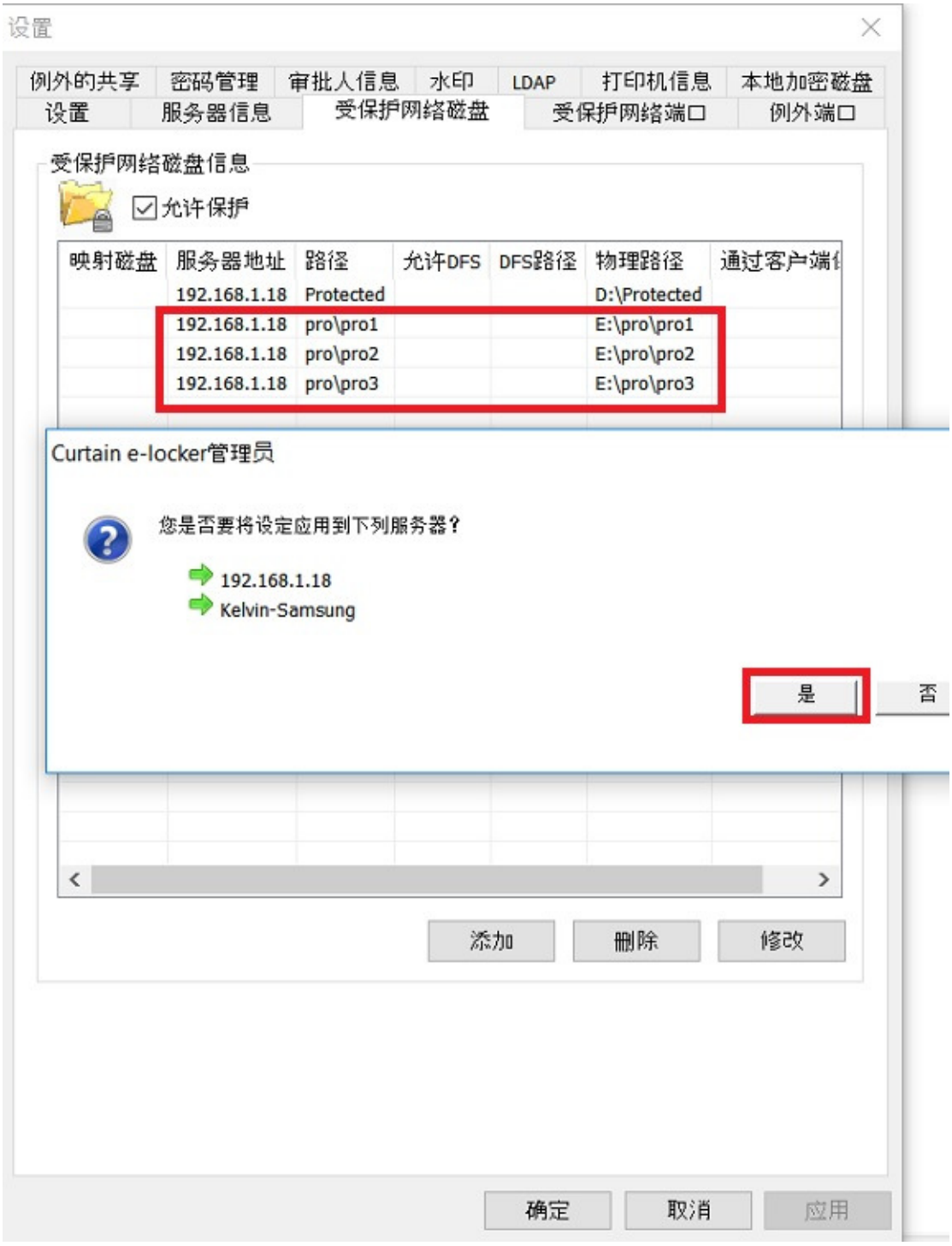
2. 添加伺服器资讯（IP或者主机名称）。



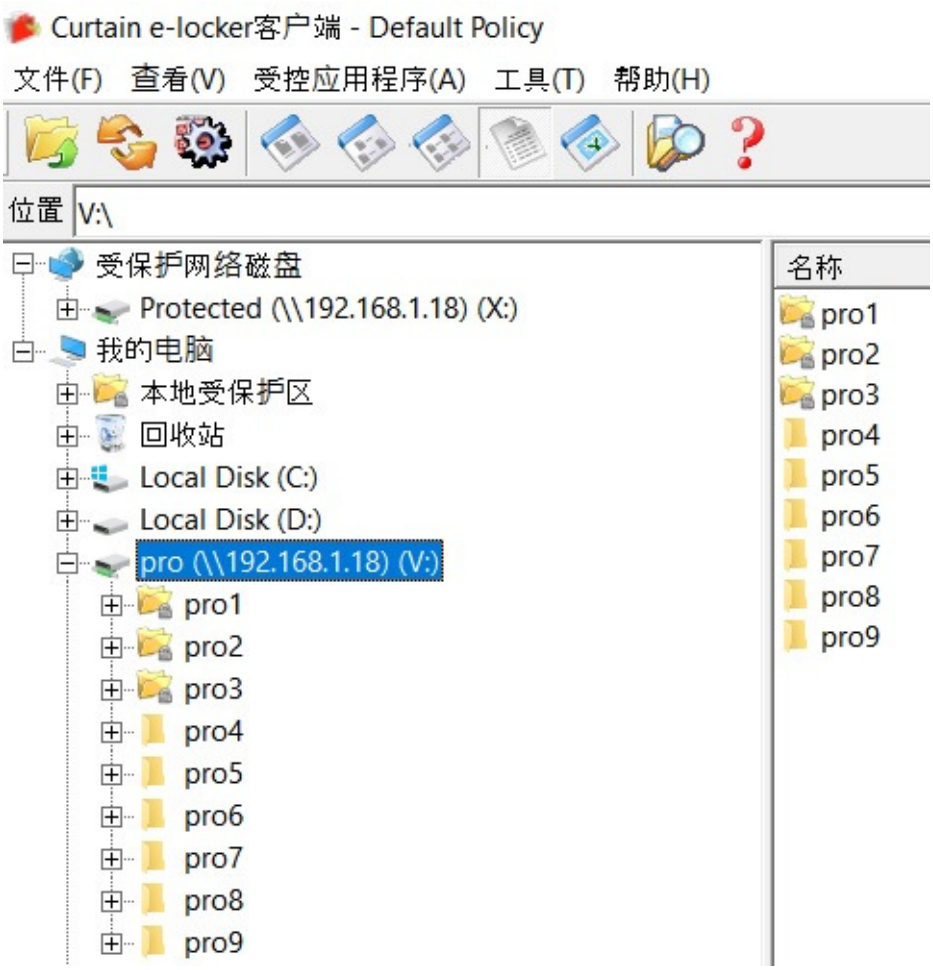
3. 然后依次序添加受保护的子文件夹路径：（下图为添加pro1示图）。



4. 接着依次序添加完成pro2, pro3的保护路径后，点击” 确定 “，推送并完成该设置。



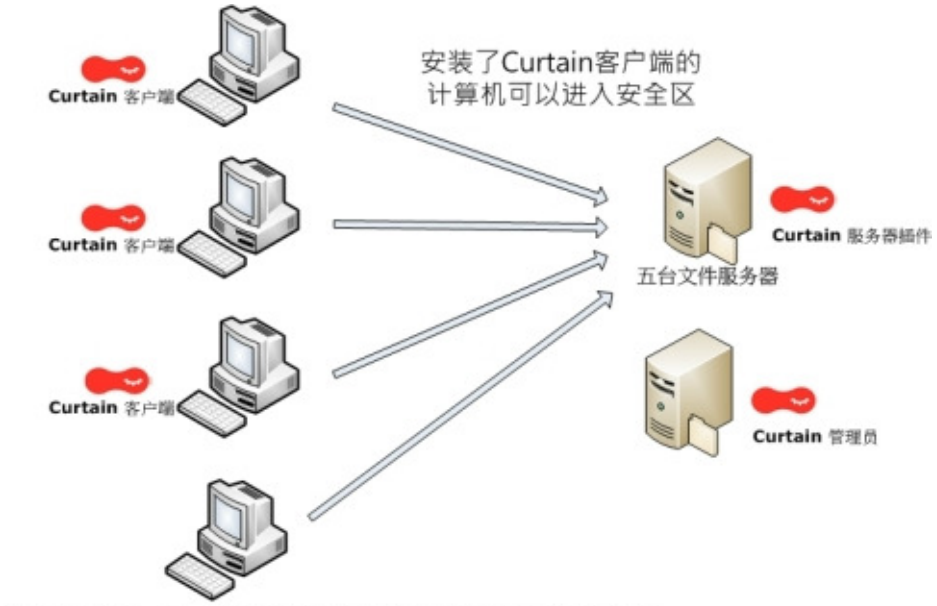
5. 于Curtain用户端，共用文件夹pro在我的电脑下方显示，其中带锁的3个子文件夹pro1, pro2, pro3为受保护的，而剩下的没有带锁的pro4至pro10这几个文件夹不受Curtain e-locker保护。




## 5.8 - 例外规则

### 5.8.1 - 例外规则

例外规则的功能一方面是为了方便用户使用保护环境的同时，又不会影响特定条件下没有安装Curtain客户端的电脑访问安全区。如下图所示架构，安装了Curtain客户端的电脑可以访问安全区（即文件服务器上的保护共享文件夹），而没有安装Curtain客户端的电脑只能够访问非受控区（即文件服务器上的普通共享文件夹）。有时候为了满足用户没有安装Curtain客户端的电脑（如经理，老板，管理层的电脑不需要管控）同样可以访问安全区，那么可以设置“例外规则”来实现这一需求。




例外规则的功能另一方面是方便了用户在现实环境中能够兼顾测试环境一起使用而不受影响，从而达到预期测试的效果。举例：公司研发部门正在使用EPDM系统，希望在现有工作环境中测试受e-locker保护的EPDM，其中抽出工程师A和B的电脑作为测试对象，那么在实施过程中A和B的电脑首先需要安装Curtain客户端，并且设置了“例外规则”保护，从而可以只针对这两台电脑测试受e-locker保护EPDM环境，那些没有安装e-locker客户端的用户电脑仍然可以正常使用EPDM系统工作。

保护规则类型共分为4种：全部保护，全部不保护，只对列表中的保护，除列表之外全部保护

- 全部保护：安装环境中该规则类型为默认设置，即安装了Curtain客户端的电脑将会被保护并且可以自由使用受保护区内的文件而不会外泄，而没有安装Curtain客户端的电脑访问受保护的共享文件夹或者保护端口等行为时将会被禁止。
- 全部不保护：相当于停止e-locker的保护功能，即安装了Curtain客户端的电脑和没有安装Curtain客户端的电脑都能够访问受保护的共享文件夹或者访问受保护端口等，保护区内的文件和控制等行为都可以通过非受控区途径来获取或操作。
- 只对列表中的保护：顾名思义加入该列表里面的电脑(以IP地址来设定)将会被保护起来，在列表外不管是安装了或者没有安装Curtain客户端的电脑都将被视为不保护。
- 除列表之外全部保护：加入到该列表里面的电脑(以IP地址来设定)将不会被保护，而在列表外安装了Curtain客户端的电脑仍然受到保护和没有安装Curtain客户端的电脑无法访问保护区内的文件或者保护端口等行为。

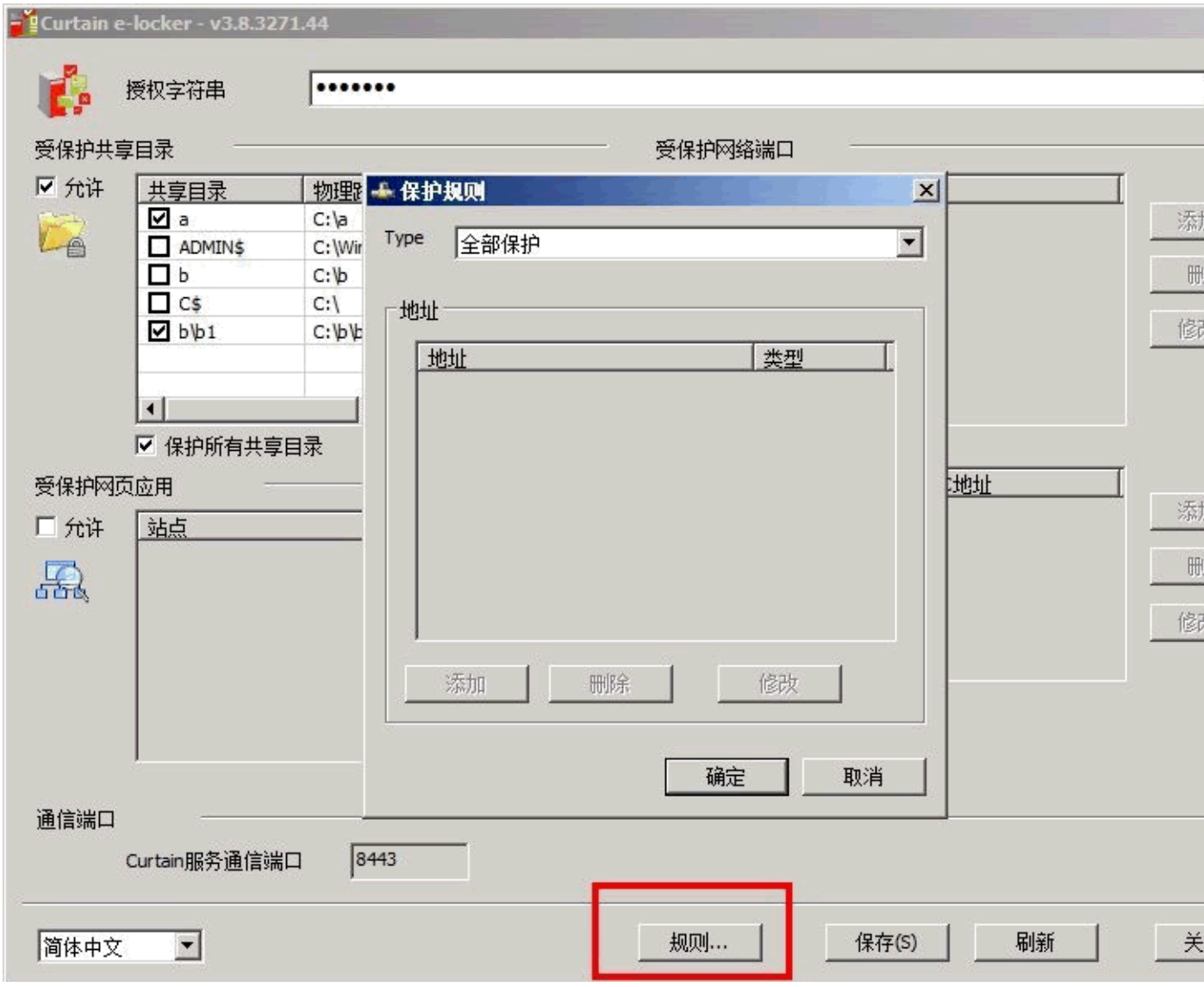

### 5.8.2 - 设置例外规则

例外规则的功能一方面是为了方便用户使用保护环境的同时，又不会影响特定条件下没有安装Curtain客户端的电脑访问服务器上的安全区。因此，这功能是在Curtain服务器插件上设置的。

设置例外规则的步骤:

1. 在开始菜单栏里找到Coworkshop Curtain e-locker文件夹，并打开“安全网络管理界面”。

2. 点击“规则”选项，弹出保护规则一栏，选择需要保护的规则类型。

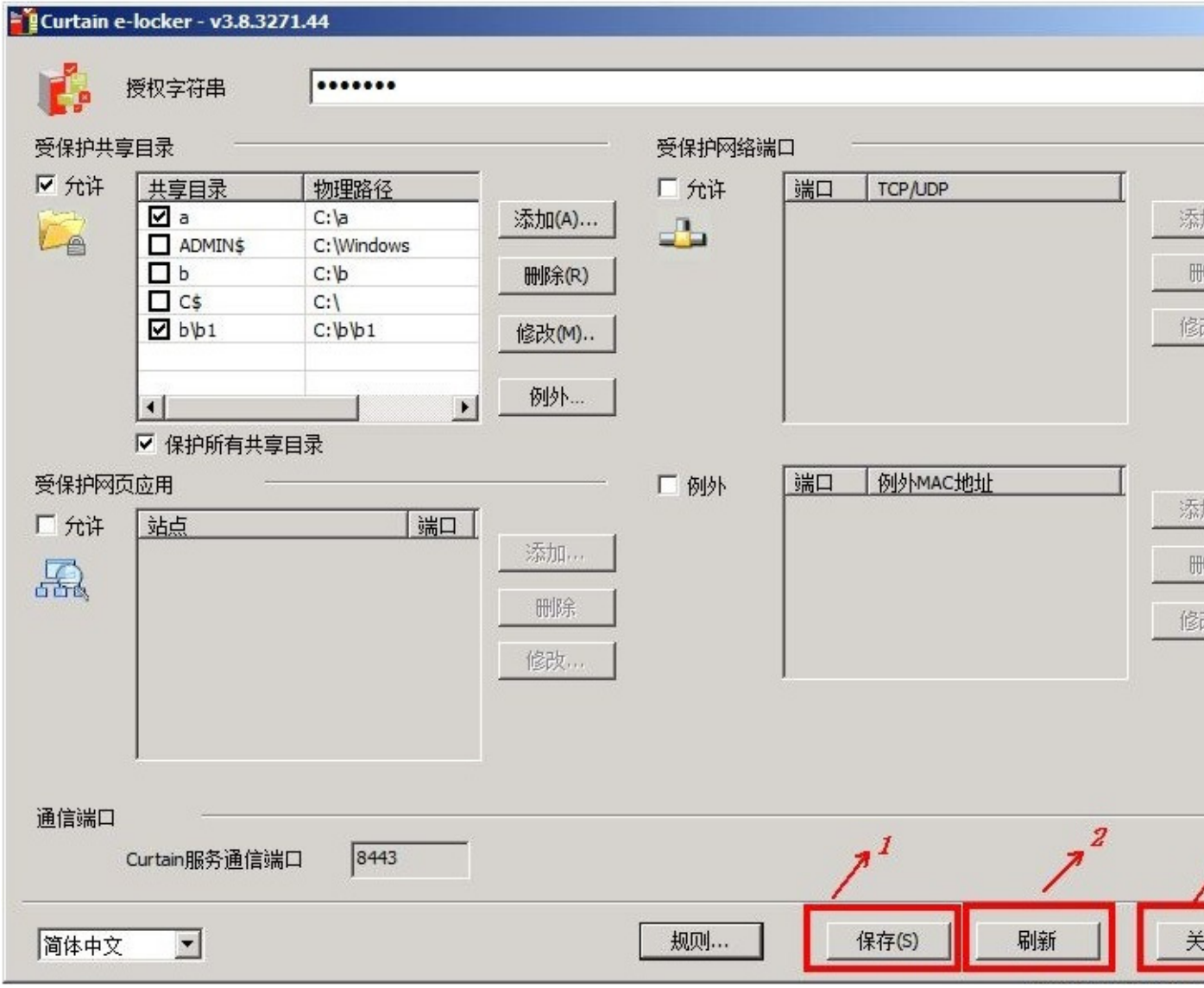



3. 如选择“只对列表中的保护”或“除列表之外全部保护”，按"添加"输入电脑的IP地址到列表中。

4. 选择类型并输入电脑的IP地址，可以选择IP地址段添加或者指定一个IP地址，如192.168.0.1。


5. 然后点击确定。

6. 然后在主界面依照顺序保存，刷新，最后关闭三个步骤：




注意：当第三步“关闭”时会提示“是否需要重启插件服务器”，在这里可以点击“NO”选择不重启。


7. 设置完成。

## 5.9 - 暂时停止受保护区的保护

"停止受保护区的保护" 为管理员提供弹性，管理员可以暂时停止对某安全策略群组下的电脑/用户的保护。因为使用此功能时客户端将不受保护，有机会导致敏感文档的外泄，因此一般情况不推荐使用。但是在某些情况下管理员需要暂时停止e-locker的保护，管理员可以预先创建一个安全策略群组并启动此功能(停止保护)，在有需要时就可以将电脑/用户指派到此安全策略群组中。

启动"停止受保护区的保护" 的步骤：

1. 在Curtain管理员，点选一个安全策略，按滑鼠右键，并选择"内容"。


2. 选择 "停止对受保护区的保护" 。


3. 然后单击 "确定" 。

当电脑/用户被暂时停止保护时，于Curtain客户端的标题会显示FULL ACCESS，如下图。


4. 完成。

# 6 - 其他功能

## 6.1 - 保护文件初稿

保护文件初稿这个功能，是用作保护新建立的文档。当此功能启动后，用户必需要将新建立的文档保存在受保护区之内，Curtain e-locker确保机密文档从一开始便受到严密的保护。

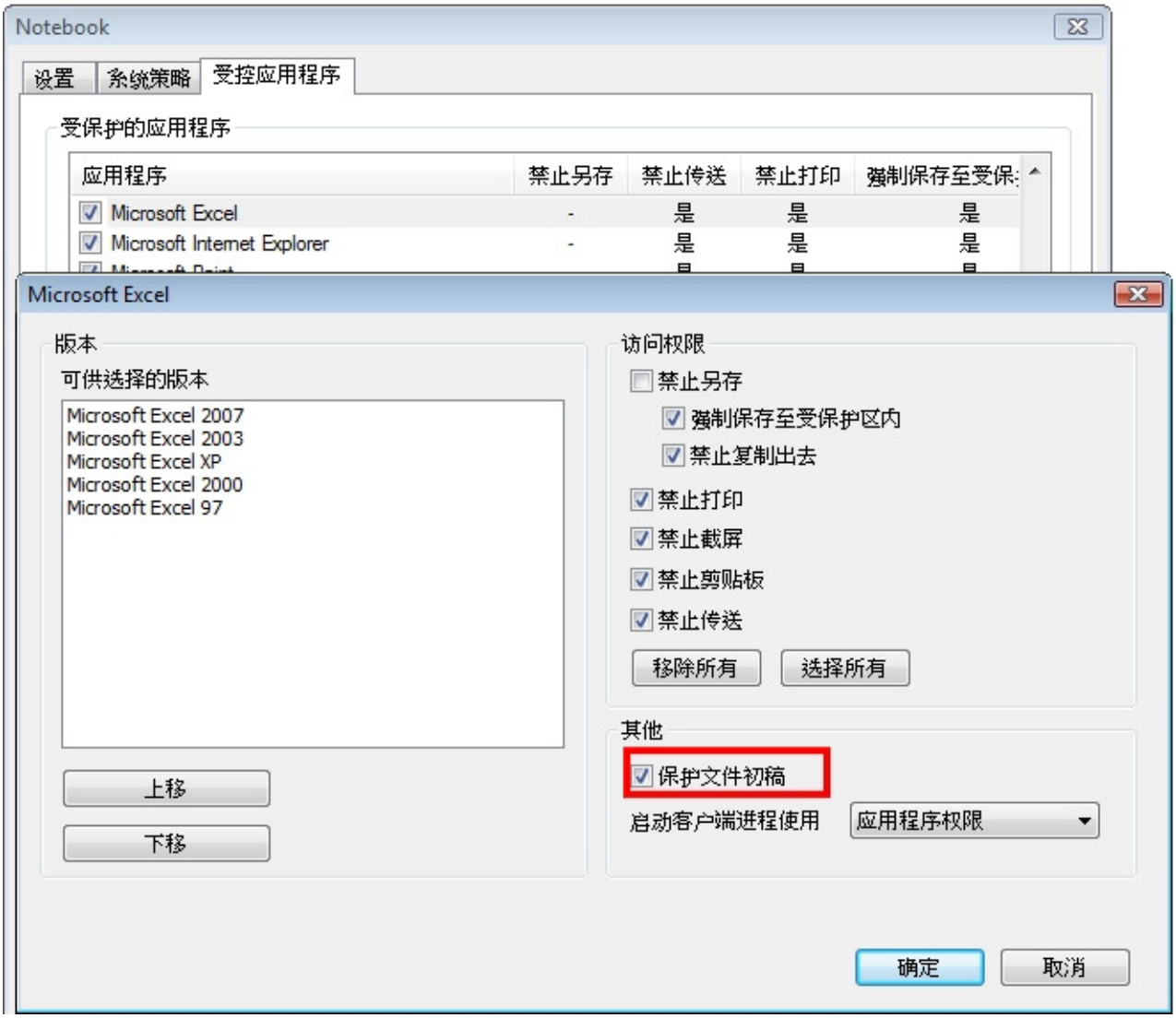
这功能可以针对个别安全策略群组和应用软件来启动的。以下是使用此功能的例子。
- 限制工程师只可以将所有新建立的AutoCAD和Photoshop文档保存在受保护区之内。

为个别应用软件启动"保护文件初稿"的步骤:
1. 在Curtain管理员，点选一个安全策略，按鼠标右键，并选择"内容"。

2. 于"受控应用程序"页，双击你想启动"保护文件初稿"的应用软件。

3. 选择"保护文件初稿"，并按确定键确认 。

"启动客户端进程使用>应用程式权限" - 此选项被选取时，代表保护文件初稿只针对此应用程式。
"启动客户端进程使用>父进程权限" - 此选项被选取时，代表保护文件初稿会保护此应用程式及其所有子进程(如:从AutoCAD下开启的Excel程序)。



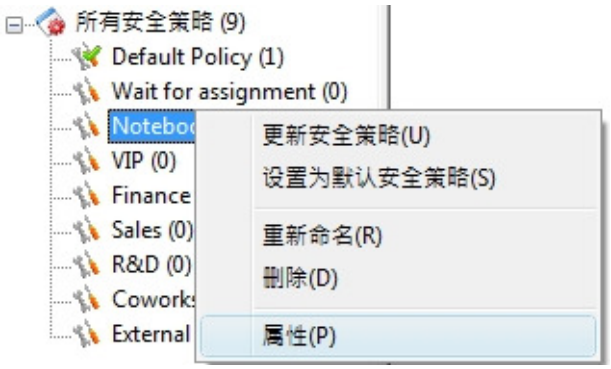
备注: 当个别应用软件的"保护文件初稿"已被启动(如:MS Excel)，代表该应用软件只容许在Curtain控制下使用。在这个例子，用户不能开启非受控的Excel，如果他们尝试开启非受控的Excel，Curtain e-locker会自动将该应用软件关闭。用户只可以开启受控的Excel来建立新的文档，所有新的Excel文挡只可以保存到Curtain保护区之内(故此这功能称之为"保护文件初稿")。对于在非受保护区下的文档，用户必需要先将文档复制到保护区之内才能打开，可以用复制粘贴或拖拉的方法将文档移到保护区之内。

## 6.2 - 在线/离线保护

在线/离线保护是一个控制用户使用已下载文档的功能。

此功能的主要目的:
- 当计算机离开公司后(意思是指当计算机不能连接Curtain管理员)，公司不想用户继续使用已被下载到本地受保护区内的机密文档。

启动"在线/离线保护"功能的步骤:
1. 在Curtain管理员，点选一个安全策略，按鼠标右键，并选择"内容"。

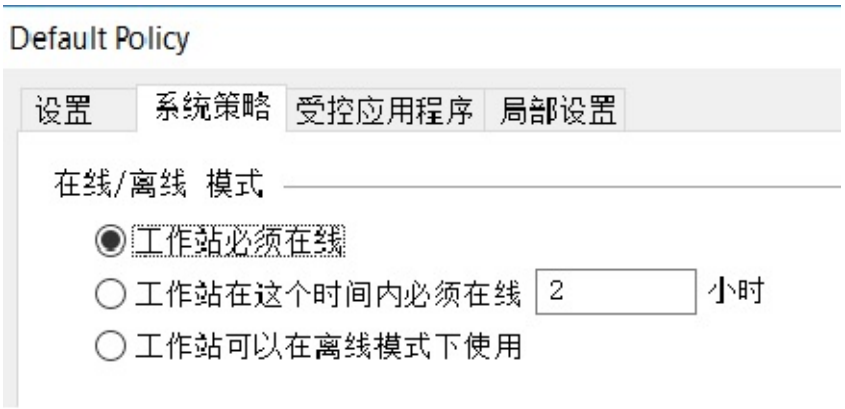



2. 于"系统策略"页的"在线/离线模式"下，有3个选项。

"工作站必需在线" - 此选项被选取时，如果用户计算机不能连接Curtain管理员，用户是不能开启Curtain客户端的。

"工作站在这个时间内必需在线[ ]小时" - 此选项被选取时，如果用户计算机超过指定的时间内依然不能连接Curtain管理员，用户是不能开启Curtain客户端的。

"工作站可以在离线模式下使用" - 此选项被选取时，无论用户计算机能不能连接Curtain管理员，用户依然可以开启Curtain客户端的。

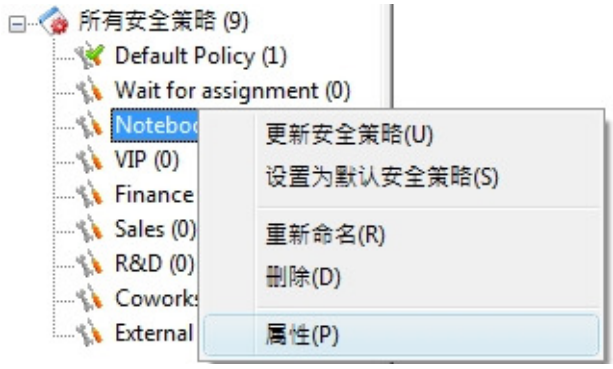


## 6.3 - 自动清理

“自动清理” 是一个自动清除用户计算机上本地受保护区内文件的功能。

此功能有两个主要用途：
- 不希望用户永久保存文件在本地受保护区中。
- 清理本地受保护区中的缓存，临时文档和回收站，以释放磁盘空间。

启动 “自动清理” 功能的步骤:
1. 在Curtain管理员中，选择一个安全策略，然后右键单击并选择 “属性” 。




2. 选择选择清理本地受保护区的方式，然后单击 “确定” 按钮进行确认。

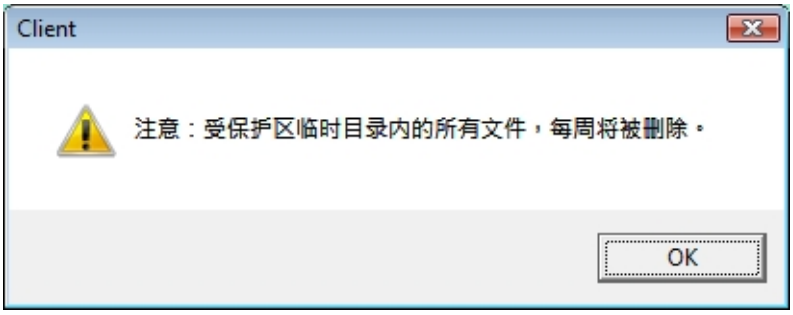

“清理本地受保护区” - 如果选择此选项，本地受保护区内的所有文件将被删除。
启动 - 如果选择此选项，系统会于用户计算机每次启动时，自动进行清理工作。
每周 - 如果选择此选项，系统会于用户计算机在选定的日子启动时，自动进行清理工作。

“清理本地受保护区临时目录” - 如果选择此选项，本地受保护区内的所有临时文件将被删除。
启动 - 如果选择此选项，系统会于用户计算机每次启动时，自动进行清理工作。
每周 - 如果选择此选项，系统会于用户计算机在选定的日子启动时，自动进行清理工作。

“清理本地受保护区内文件” 基于下载日期和/或修改日期 - 如果选择此选项，本地受保护区内符合准则（即下载日期和/或修改日期）的所有文件将被删除。
下载[ ]天后删除文件 - 如果选择此选项，下载日期超过指定天数的本地受保护区文档将被删除。
修改[ ]天后删除文件 - 如果选择此选项，最后修改日期超过指定天数的本地受保护区文档将被删除。

“清理本地受保护区内回收站文件”基于删除日期 - 如果选择此选项，回收站内符合准则（即删除日期）的所有文件将被删除。
删除[ ]天后删除文件 - 如果选择此选项，删除日期超过指定天数的回收站文档将被删除。

如果启动了自动清除功能，则每次启动Curtain客户端时系统都会提示用户。




## 6.4 - 截屏控制

Curtain e-locker很聪明地处理截屏这个功能:

- 使用截屏时，系统会聪明地将显示敏感资料的窗口变成灰色;
- 对于普通的资料，用户依然可以利用截屏功能带来的方便;
- 截屏软件同样被系统堵住。

## 6.5 - 智能复制粘贴控制

Curtain e-locker很聪明地处理复制粘贴这个功能:

- 在受保护区的文档之间复制粘贴是容许的;
- 从受保护区以外复制资料并粘贴到受控文档内也是容许的;
- 但是，从受控文档内复制资料并贴到受保护区以外是受Curtain e-locker控制的，如果没有授权是绝对不容许的。

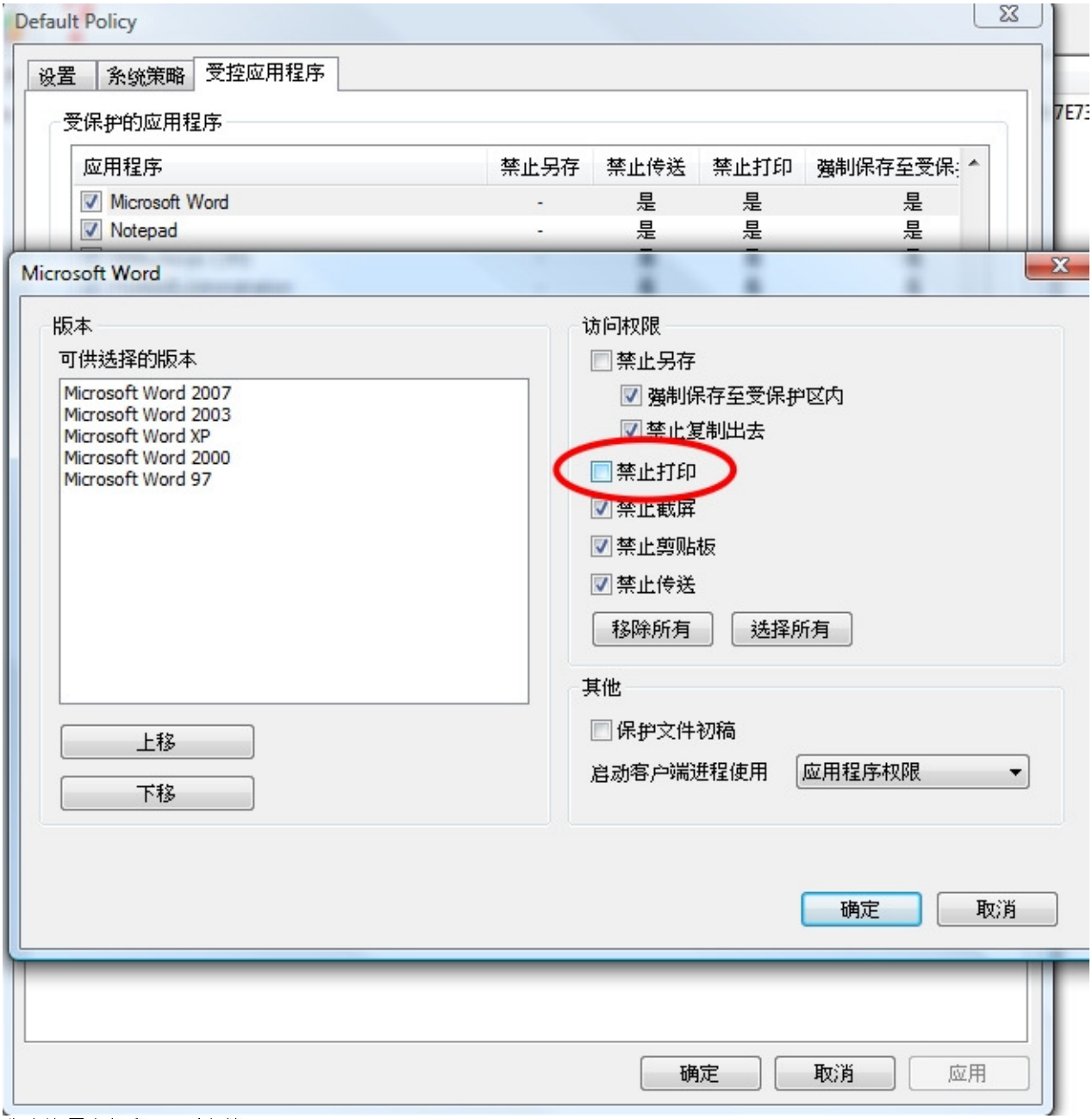
这方法既不影响正常操作，亦可以确保资料的安全，Curtain e-locker在方便性和资料保安之间取得很好的平衡。

## 6.6 - 安全生成PDF文档

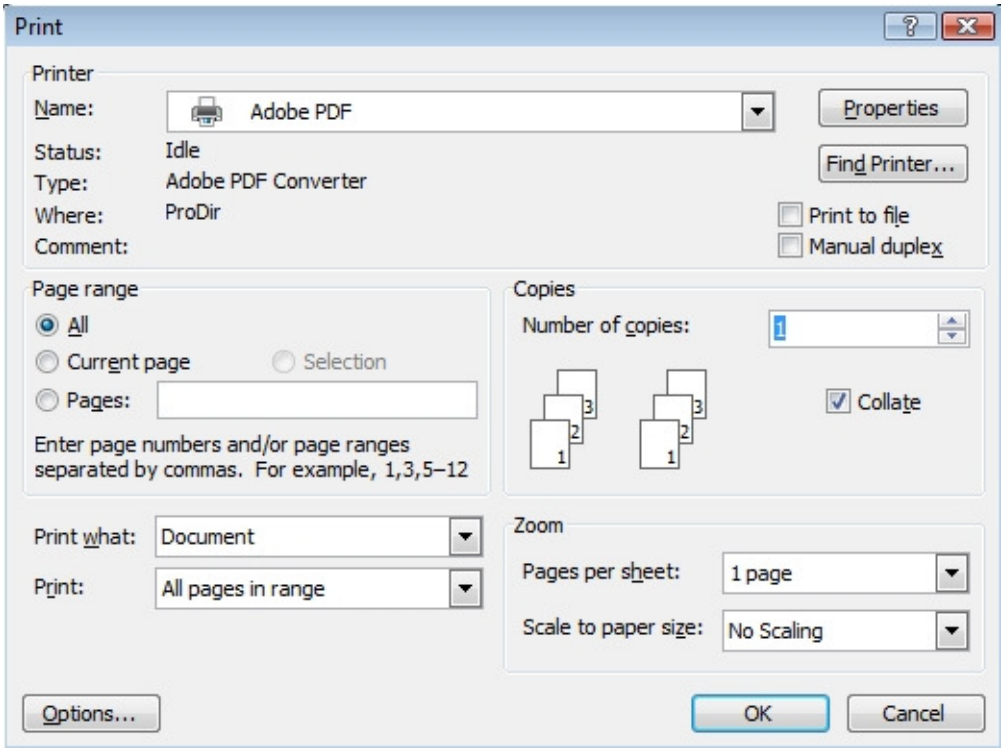
"安全打印成PDF文档"这个功能容许用户将敏感资料以"打印成PDF"的方法，将文档转成PDF格式，而又不会构成资料外泄的问题。

此功能的主要目的:
- 用户可以将敏感资料以"打印成PDF"的方法，将文档转成PDF格式。但生成的PDF文档只可以保存在受保护区内。此功能在方便性和保护机密资料中间取得很好的平衡。用户可以将文档转换成PDF格式的同时，机密资料又不能被带走。

例子: 容许用户将受保护的Word文档转成PDF格式
如果管理员容许用户将受保护的Word文档(即是在受保护内的Word文档)转成PDF格式，管理员应该先在Word的安全策略上容许"打印"。设定后，用户便可以打印受保护的Word文档，并将它们转成PDF格式。所有生成的PDF文档只可以保存在受保护区内。



先容许用户打印Word文档




以"打印成PDF"的方法，将文档转成PDF格式

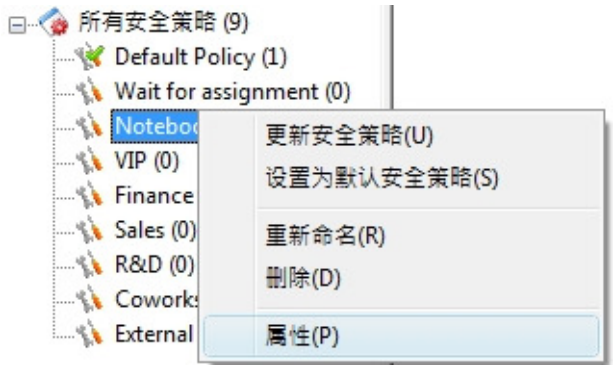
## 6.7 - 与其他人分享受保护文件

一般来说，有三种不同的权限级别：
(情况1) 用户被授权可以加密并将加密文档保存到保护区之外。这些文档只能在受保护区域中被解密。
(情况2) 用户被授权可以加密并将加密文档保存到保护区之外。只需输入正确密码就可以在任何地方解密文档。
(情况3) 用户有权储存/发送/复制文档到保护区之外（没有加密文档）。但这些文档不再受Curtain e-locker保护。

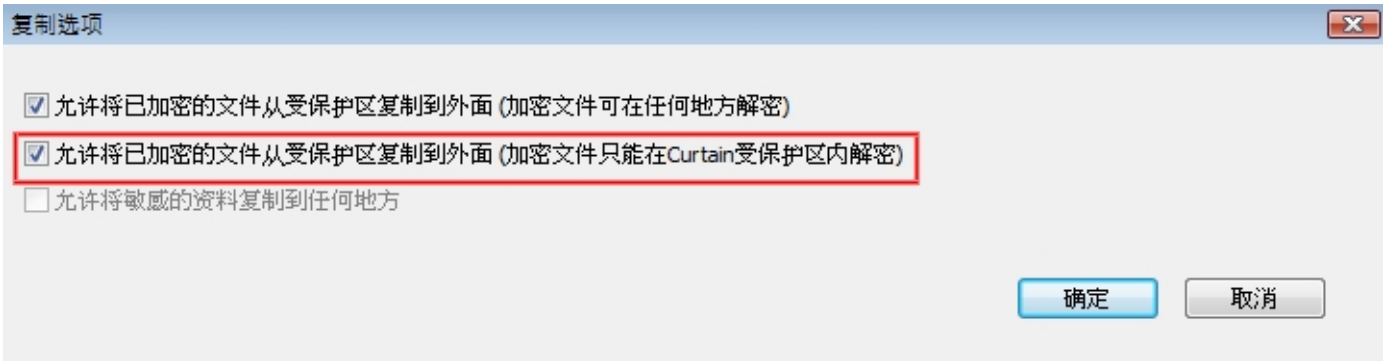
情况 1 - 加密（仅由客户端解密）：
此功能对于用户在公司内共享受保护的文档是非常有用的。因此，你可以将此功能授予大多数用户。

如果用户被允许加密（仅由客户端解密），用户可以加密受保护的文档，并与其他人分享加密的文档。当其他用户收到文档时，他们的电脑必须安装Curtain 客户端（并属于同一台Curtain管理员）。用户可以双击文档进行解密。文件将自动解密到本地保护区内。

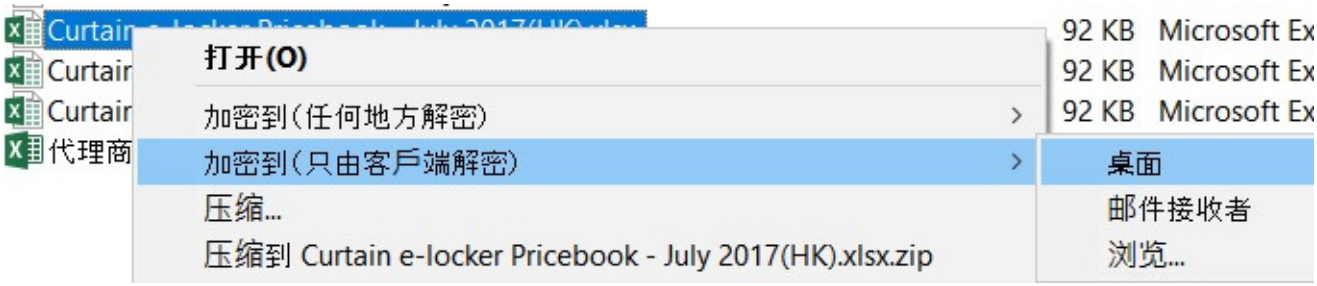
授予“加密（仅由客户端解密）”权限的步骤：
1. 在Curtain管理员，选择一个安全策略，然后右键单击以选择“属性”。



2. 点击“复制选项”按钮，选择如下图所示的第二个选项，单击“确定”。




与其他人分享加密文档的步骤：
1. 在Curtain客户端，选择受保护的文档，然后右键单击选择“加密到（仅由客户端解密）”。然后加密的文档将被复制到选择的位置。




2. 将加密文档发送给其他人。由于文档被加密，文档在传送过程中（例如：USB盘或电子邮件）是非常安全的。

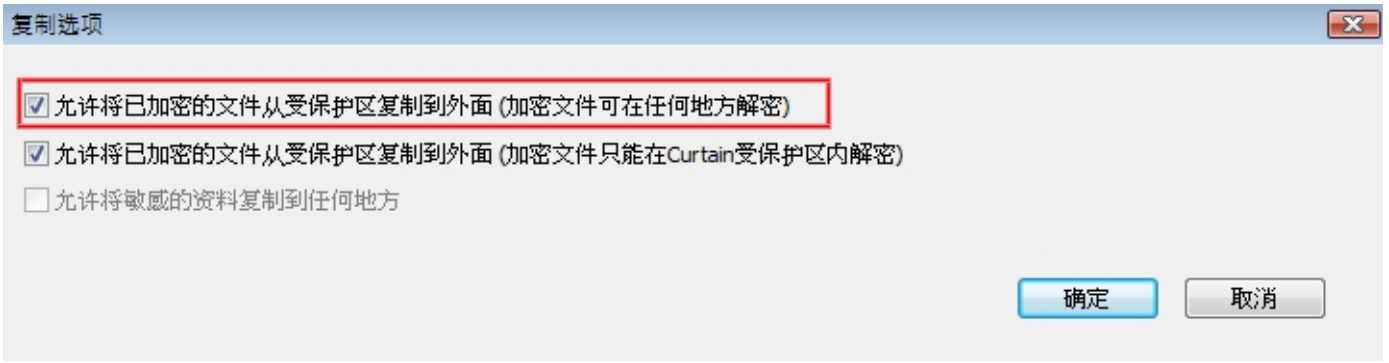

3. 当用户收到文档时，用户只需双击该文档即可。它将被解密到本地受保护区内。

情况 2 - 加密（任何地方解密）：
实际上用户只需输入正确密码后就可以获取文档。因此，此功能只能授予授权用户。

如果用户被允许加密（任何地方解密），用户可以使用密码加密受保护的文档，并与其他人分享加密的文档。当其他用户收到文档时，他们可以输入正确的密码对文档进行解密。
备注： 解密不需要Curtain客户端的。文档成功解密后，Curtain将不再保护文档。

授予“加密（任何地方解密）”权限的步骤：
1. 在Curtain客户端，选择一个安全策略，然后右键单击以选择“属性”。

2. 单击“复制选项”按钮，选择如下图所示的第一个选项，然后单击“确定”。




与其他人分享密码加密文档的步骤：

1. 在Curtain客户端，选择受保护的文档，然后右键单击，并选择“加密到（任何地方解密）”。

2. 设置密码，然后单击确定。然后加密的文档将被复制到选择的位置。


3. 将密码加密的文档发送给他人。由于文档被加密，文档在传送过程中（例如：USB盘或电子邮件）是非常安全的。


4. 当用户收到文档时，用户只需双击该文档即可。用户输入正确密码后，文档将被解密到选择的位置。

情况 3 - 拷走原文档（没有加密文档）：
当某些用户需要频繁地与外面分享受保护文档，又或者你不需要控制他们使用受保护文档时，你可以允许他们将受保护的文档储存到受保护区之外，而无需加密文档。此功能只能授予授权用户。
有关设置方法，请参阅FAQ00084或“安装指南”中的第5.2节。

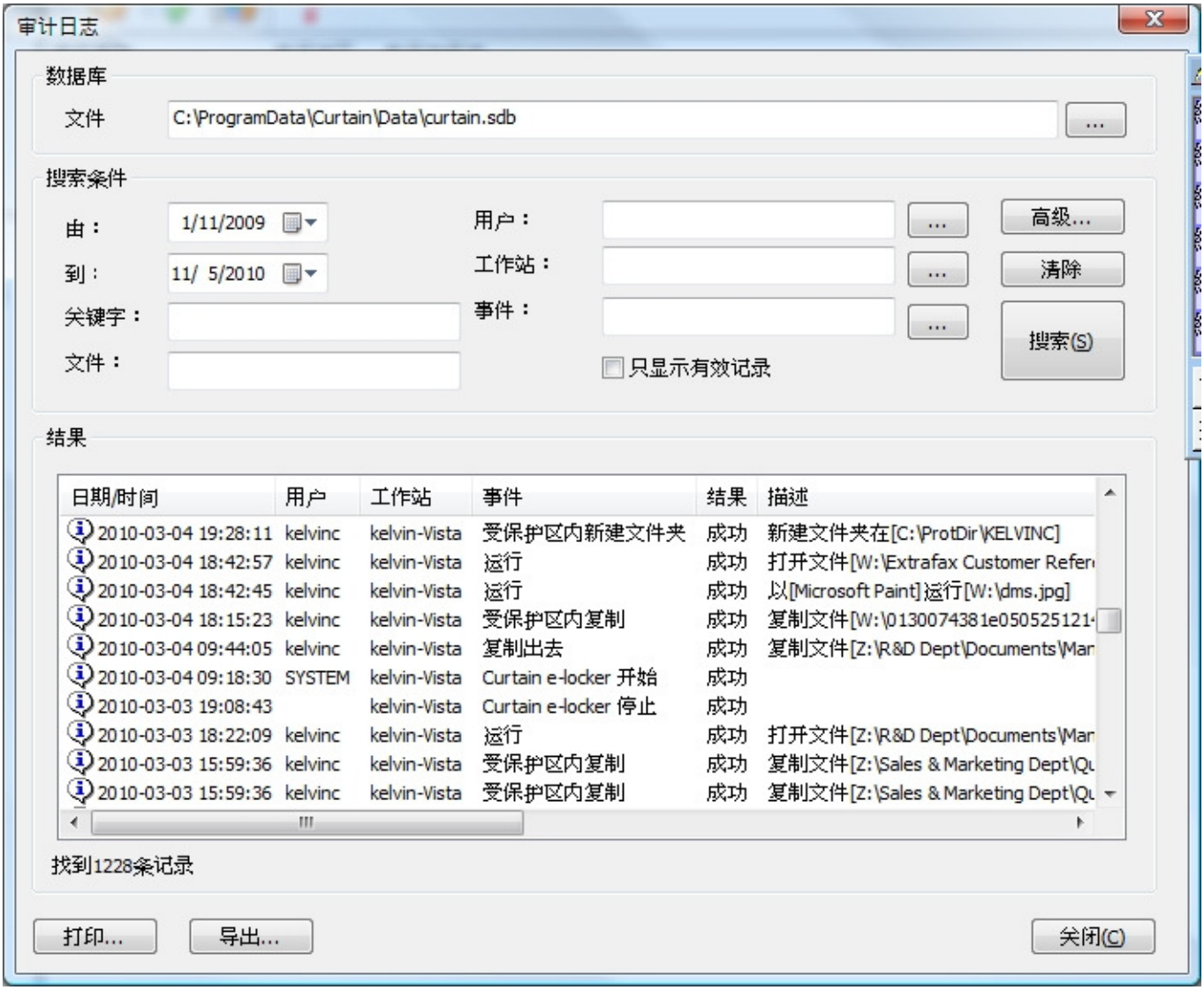
如果允许用户可以将文档以“储存到任何地方/发送/复制文档到任何地方”拷走，用户就可以与其他人分享未加密的文档（原文档）。由于文档未加密，用户可以不受Curtain保护下使用文档。 “储存到任何地方/发送/复制文档到任何地方”这三个控制的主要分别在于Curtain可以将“发送/复制文档到任何地方”作日志记录。但是，“储存到任何地方”是没有日志记录的。

## 6.8 - 审计日志

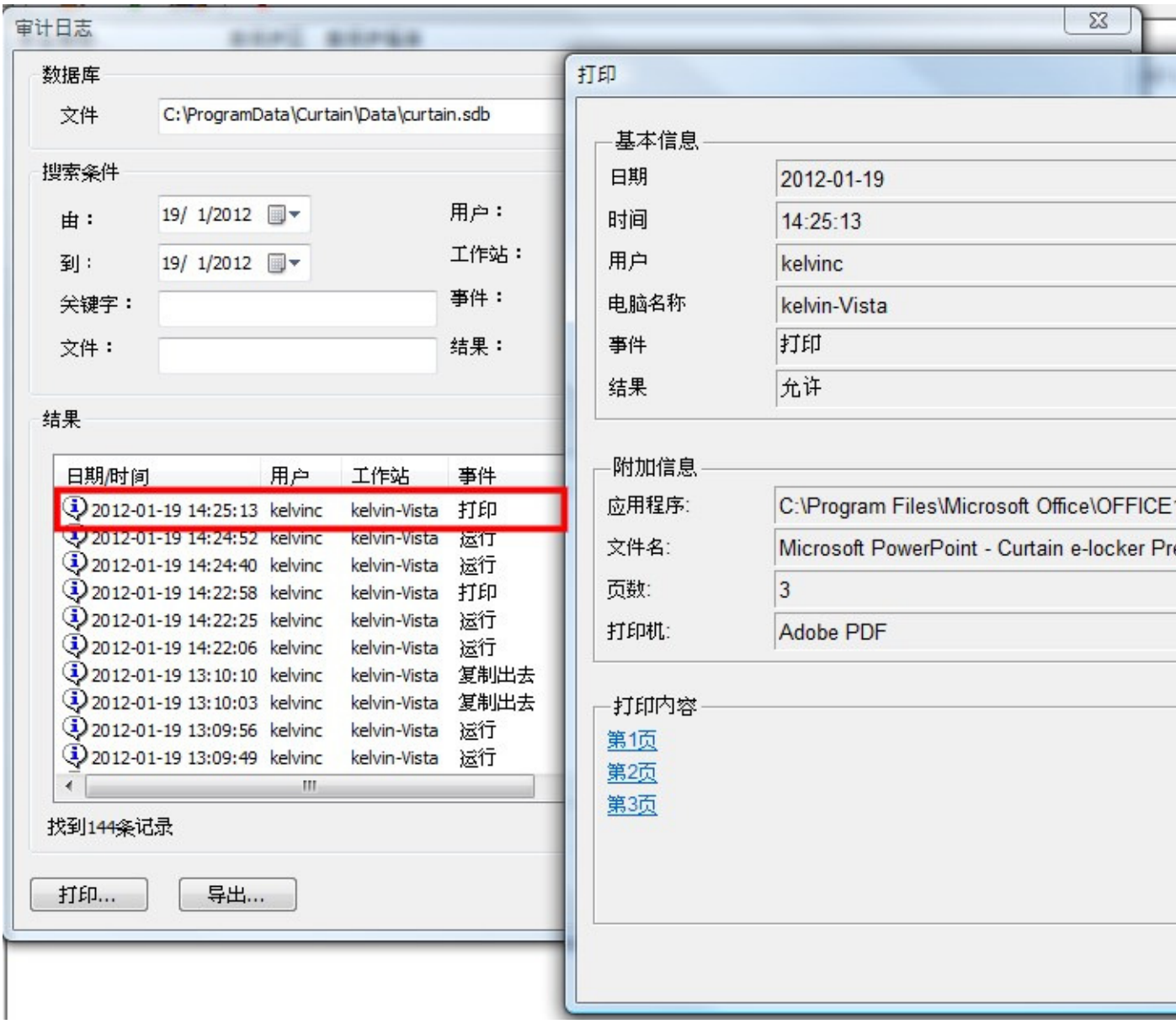
有的，Curtain e-locker是有审计日志的。

查看审计日志的步骤:
1. 开启Curtain管理员。

2. 于工具列上按"审计日志"按钮，或于菜单上选择"文件>审计日志"。接着，系统会显示审计日志。

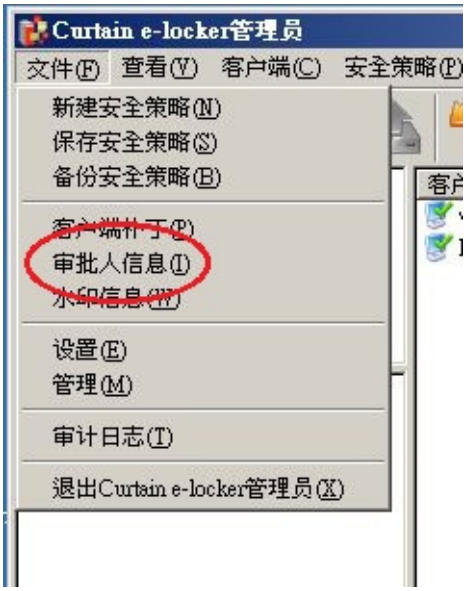
3. 如果有记录到打印内容，可以双击记录查看打印内容(快照)。



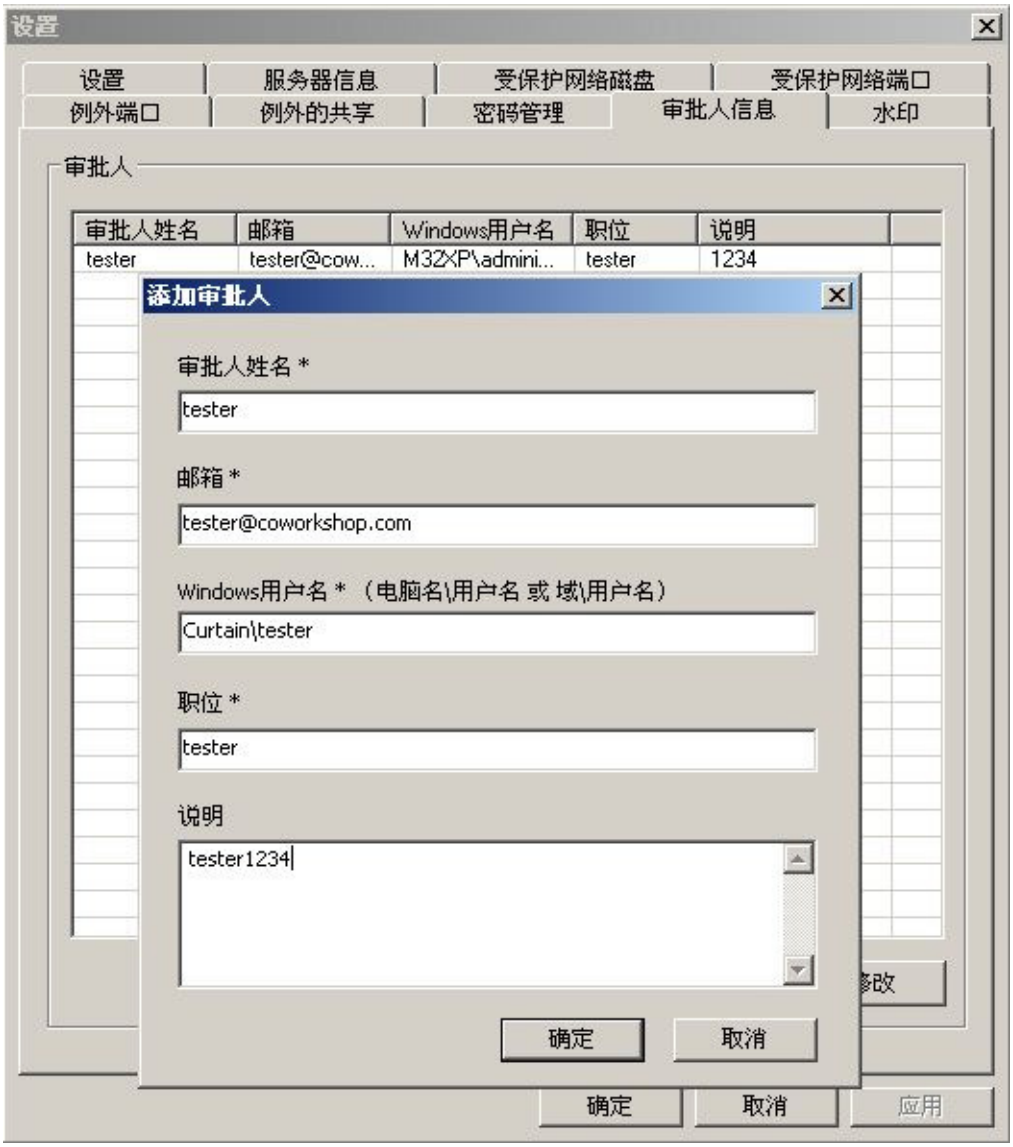
## 6.9 - 外发申请

如果用户需要将受控文件拿出受保护区给公司以外的人仕使用，而用户又没有此权限时，用户可以使用"外发申请"，如果审批人批准有关申请，该文件会以电邮形式发送给申请人，由于该文件已经离开了受保护区并且没有加密，申请人可以转发给公司以外的人仕使用而不受e-locker控制。整个审批过程都会记录在活动记录中。

设定审批人的步骤:
1. 在Curtain管理员，于菜单上选择"档案>审批人信息"。




2. 按"添加"按纽来新增审批人。
- 在此处填写审批人的名字，邮箱，职位；
- 在Windows用户名这里要注意，请以 "工作组\用户名" 或 "域\用户名" 格式填写 (如：M32w2k8-PC\Administrator 或 Curtain\Tester)。




备注: 审批人和申请人的电脑必需安装Curtain客户端才可以提交或批准申请。

提交申请的步骤:

1. 在Curtain客户端，点选一个或多个文件，按滑鼠右键，并选择"外发申请"。


备注:

- 不支持文件夹操作
- 支持多个文件 (按Ctrl键选择多个文件)

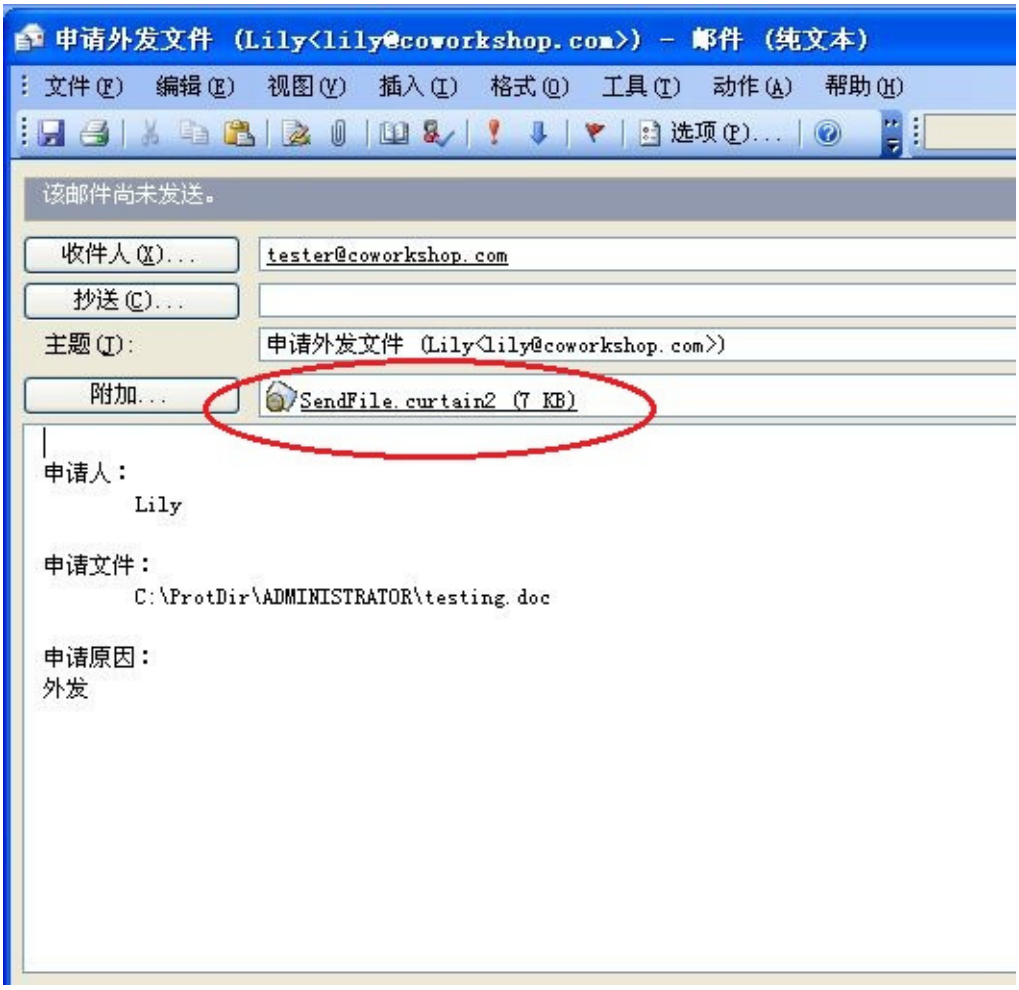
2. 填写申请人，邮箱以及申请原因等信息，并选择审批人。

3. 完成后按确定键确认。

系统会使用你预设的电邮客户端新增一份草稿，并自动附加一个附件(文件名为SendFile.curtain2)，用户可以简单地按 "发送" 来将申请发送到审批人。现时Curtain支持Microsoft Office Outlook、Outlook Express和Windows Mail。

允许/拒绝申请的步骤:

1. 当审批人收到该电邮时，审批人可以双击附件(档案名为"SendFile.curtain2")来审批有关申请。审批人可查看申请原因，申请人名，申请文件等，若要查看文件内容，单击该文件名即可打开，此时的文件不受Curtain保护。

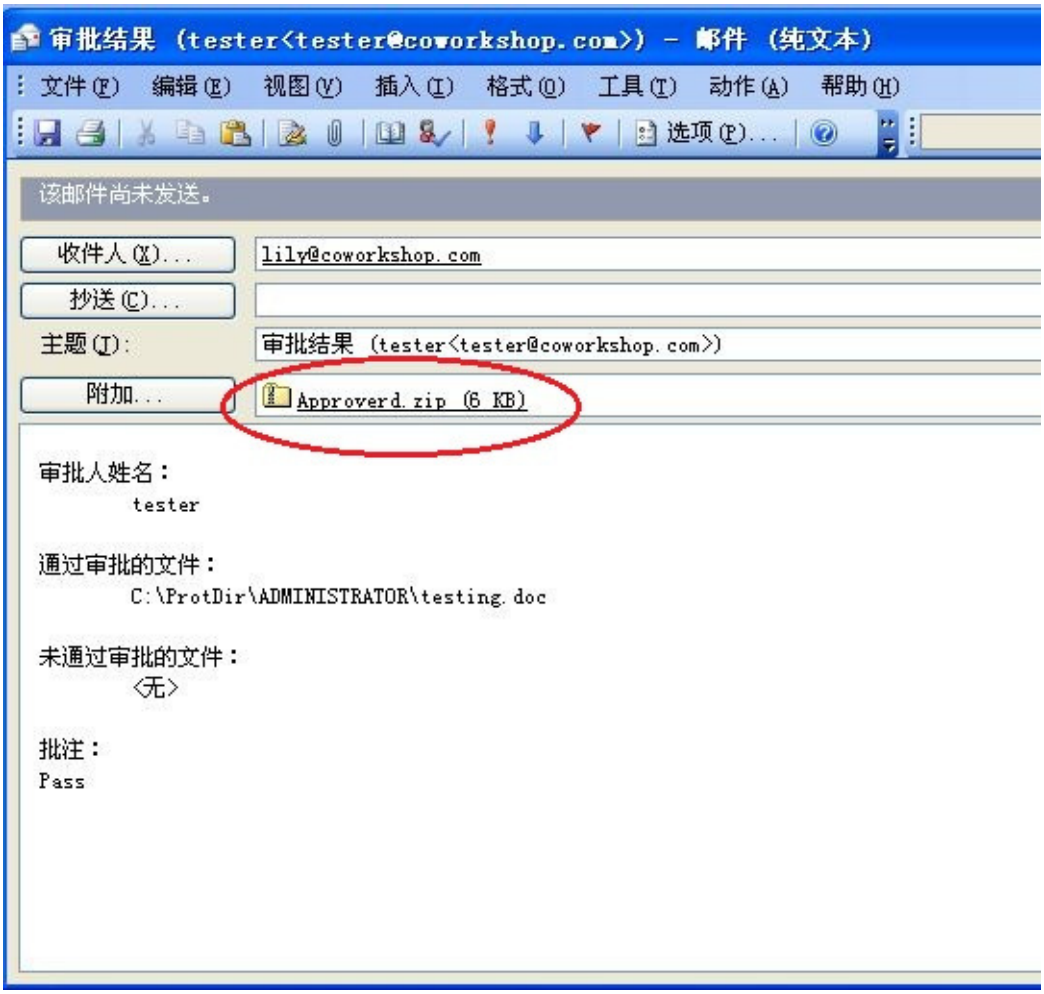



系统会对比当前Windows用户以确认审批人身份，如当前用户跟记录不一样，则不能打开"SendFile.curtain2"档案，系统会弹出如下提示对话框：

2. 选择允许或拒绝，并输入意见(如适用)。

3. 按确定键确认。

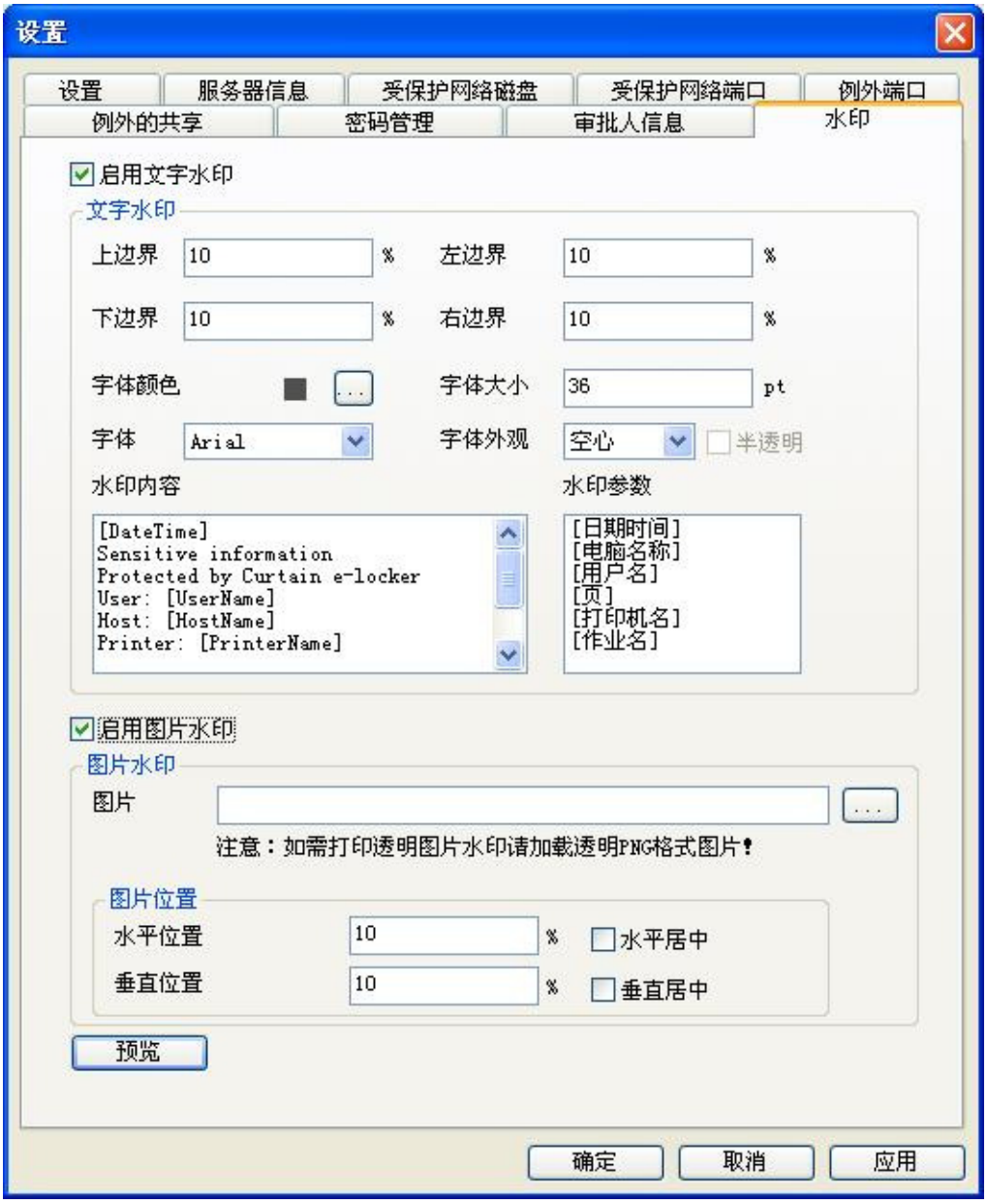
系统会使用预设的电邮客户端新增一份草稿，如果审批人批准有关申请，系统会并自动附加一个附件(文件名为Approved.zip)，审批人可以简单地按"发送"来回覆申请人。由于该文件已经离开了受保护区并且没有加密，申请人可以转发给公司以外的人仕使用而不受e-locker控制。



## 6.10 - 附加水印

如果你想在打印文件时加上水印，你可使用此功能，水印分别有文字水印和图片水印。

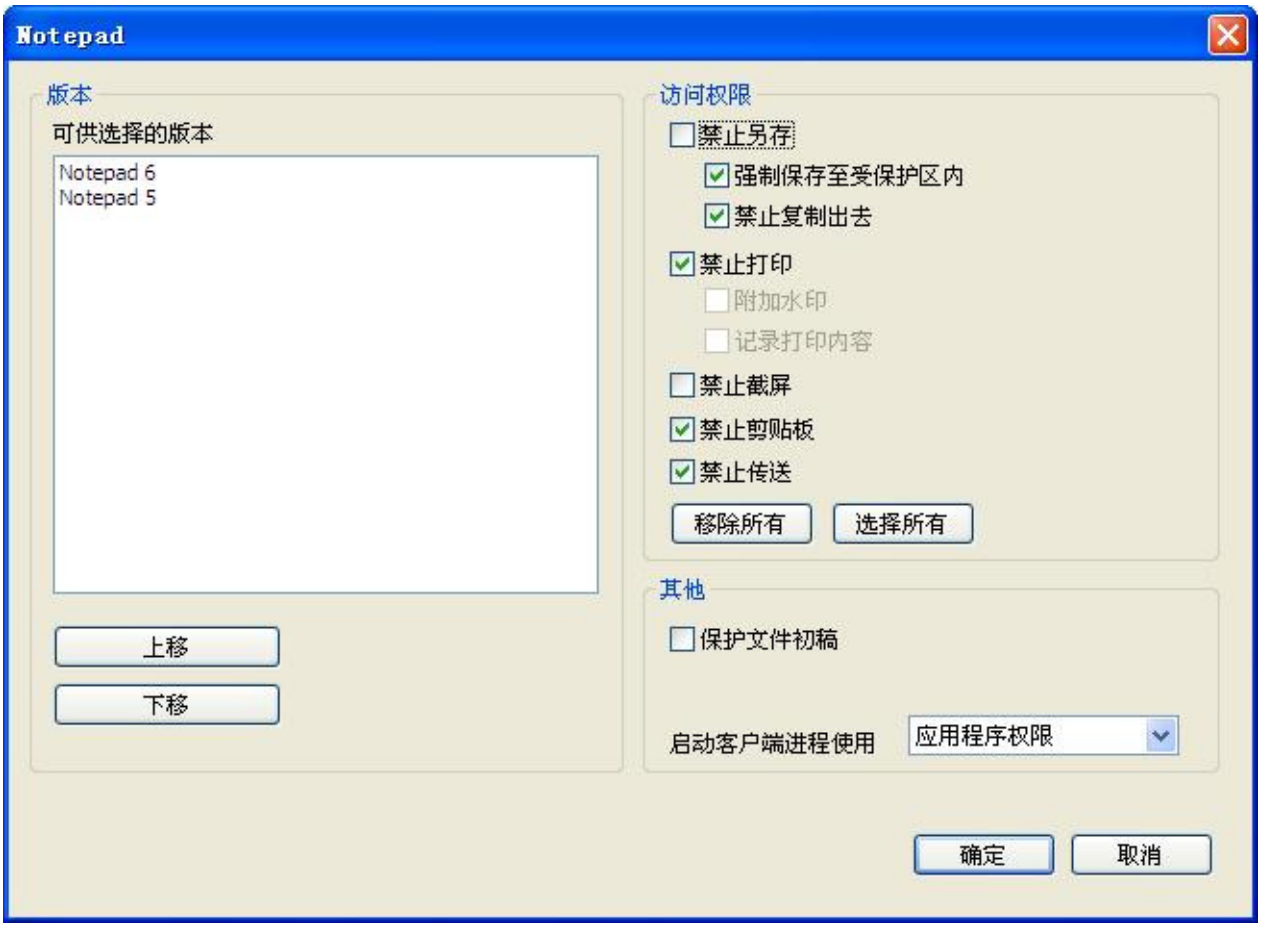
设定"水印"的步骤:
1. 在Curtain管理员菜单：选择 “文件-> 设置-> 水印” 。



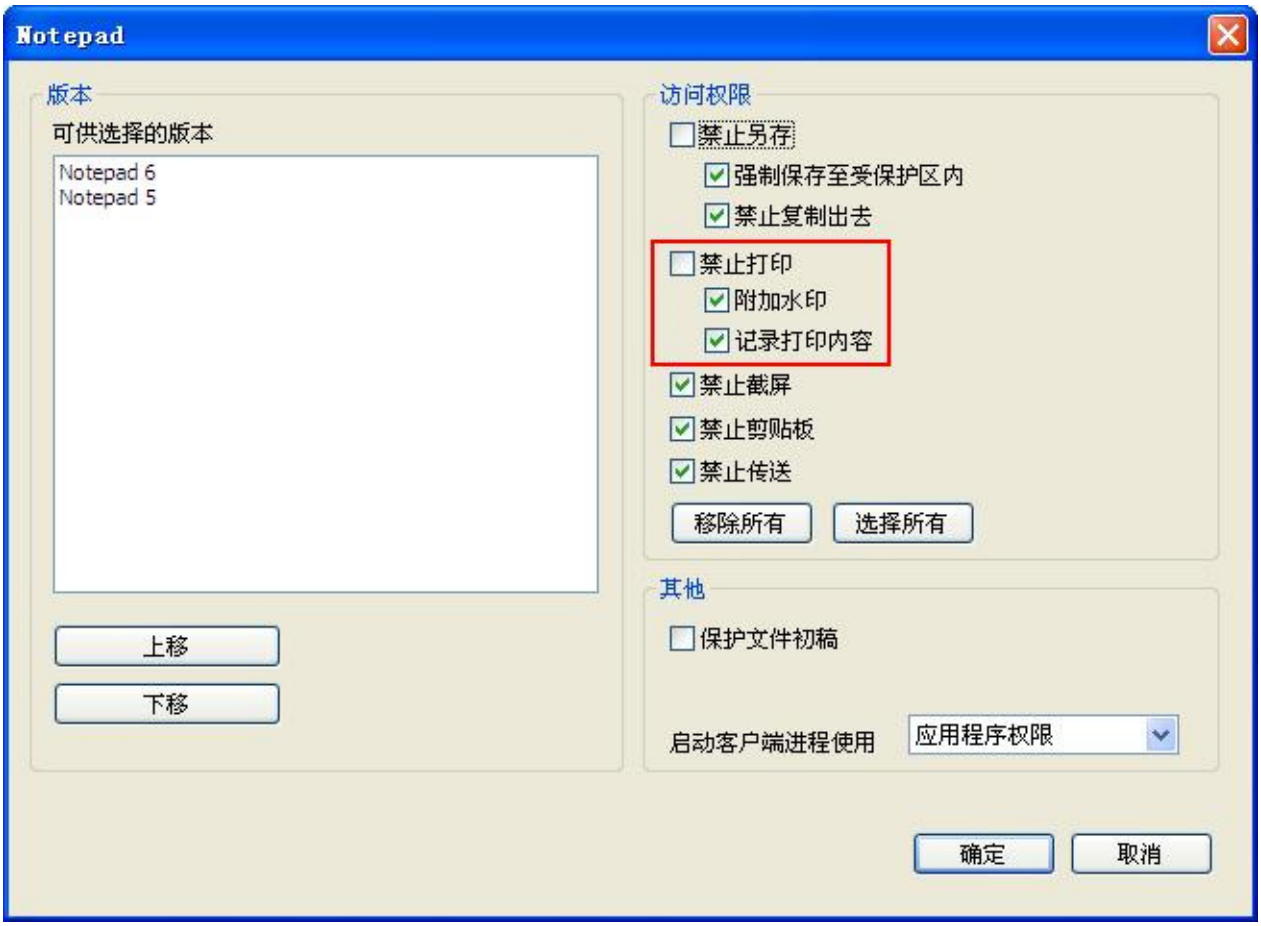
2. 完成后按"确定"。

为个别应用软件启动"水印"的步骤:
1. 在Curtain管理员，点选一个安全策略，按滑鼠右键，并选择"内容"。

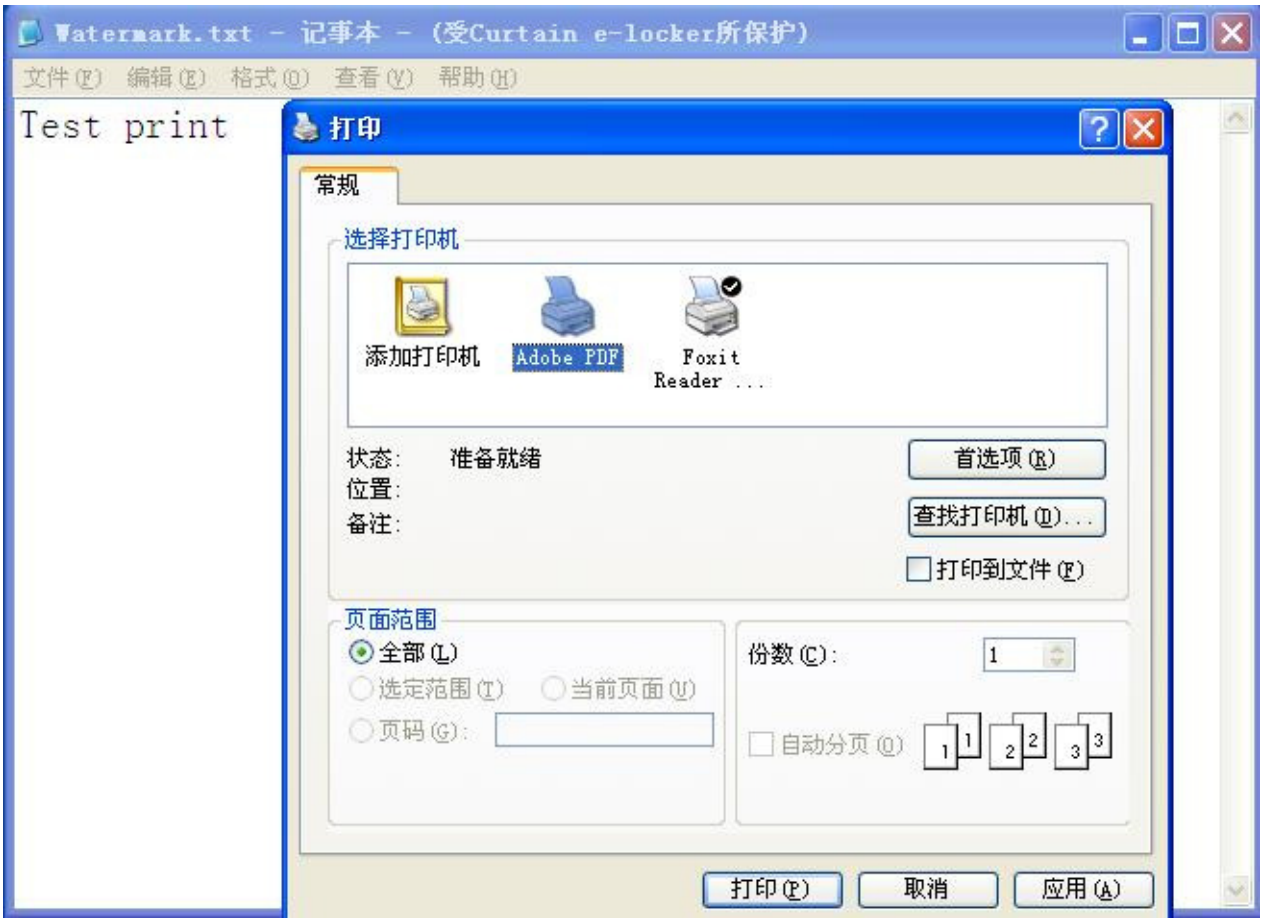
2. 于"受控应用程式"页，双击你想启动"水印"的应用软件。



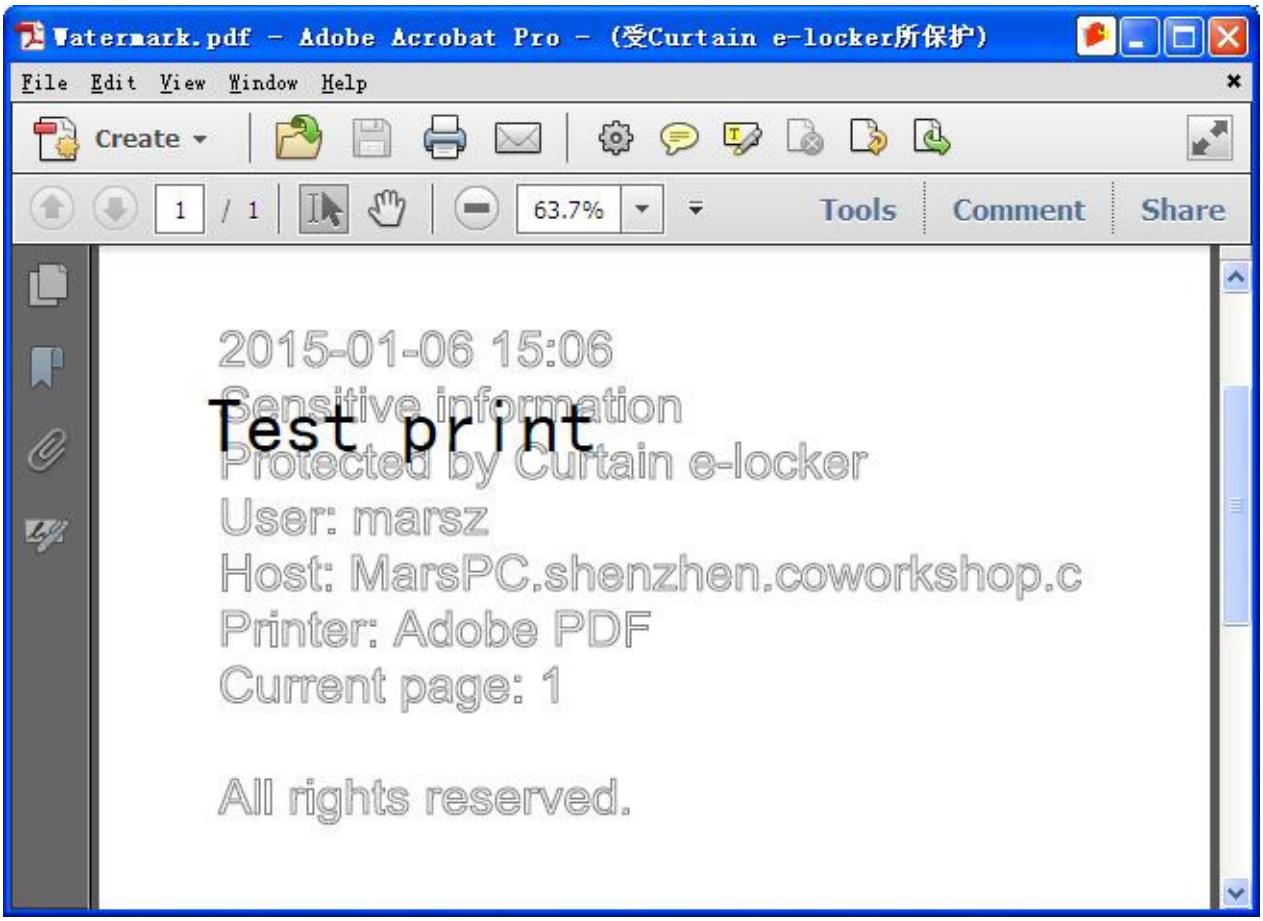
3.将 “禁止打印” 权限的勾去掉，再选择 “附加水印” ， 完成后按"确定"。



水印例子:
完成后，当使用此应用软件打印时，系统会自动加上水印。



如果使用"打印成PDF"功能，水印会加到生成出来的PDF上。

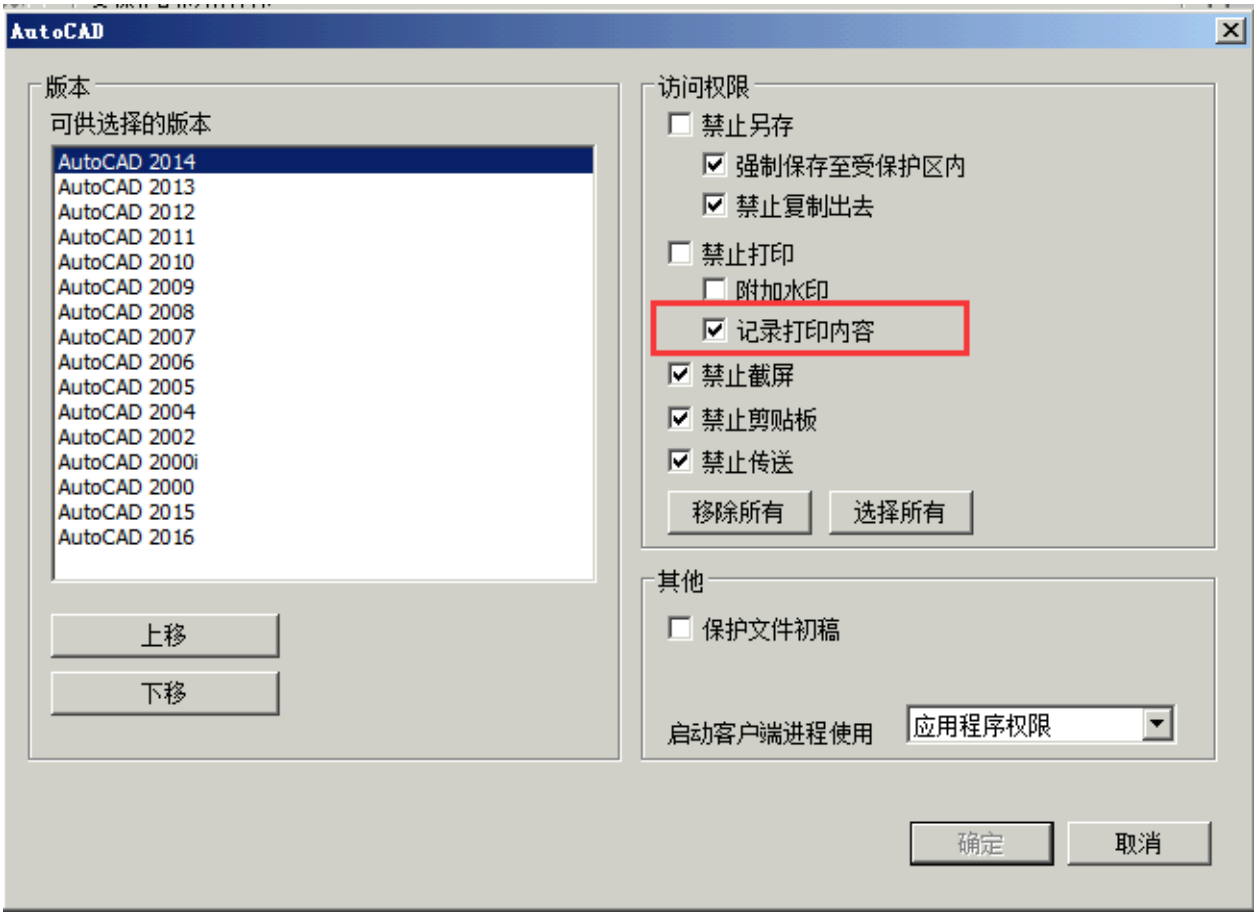



## 6.11 - 记录打印内容

在默认情况下，Curtain e-locker管理员通过打印日志来跟踪用户的文档打印情况。然而，管理员只能猜测这个文件名到底打印了什么信息。管理员如果想要知道打印的内容，他们需要使用到“记录打印内容”这个功能。开启这个功能后，系统将记录所有打印的文档内容并将其储存为JPG文件。管理员可以查看审计跟踪里的打印记录。

开启“记录打印内容”应用的步骤:
1. 在Curtain管理端，选择策略组并右键查看“属性”。

2. 在应用中，双击你需要开启 “记录打印内容” 的应用。




3. 选择 “记录打印内容” 并确定。

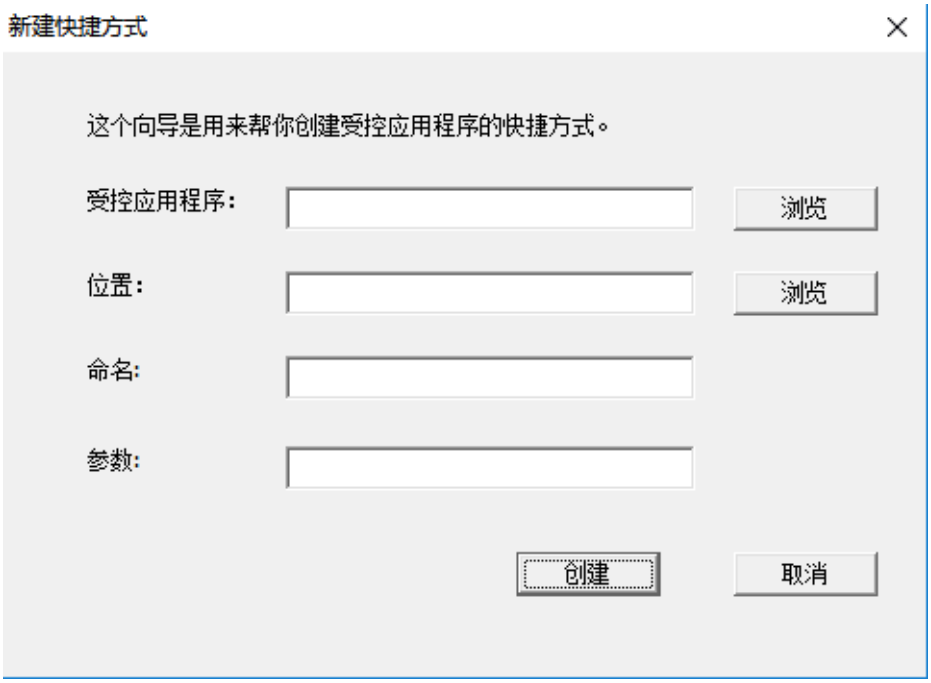
备注：如果开启这个功能，请注意系统日志文件的大小。

## 6.12 - 为受控应用程序创建快捷方式

用户可以使用Curtain客户端的菜单，来开启受Curtain e-locker控制的应用程序，用户亦可以为受控应用程序创建快捷方式，以下是创建快捷方式的步骤。

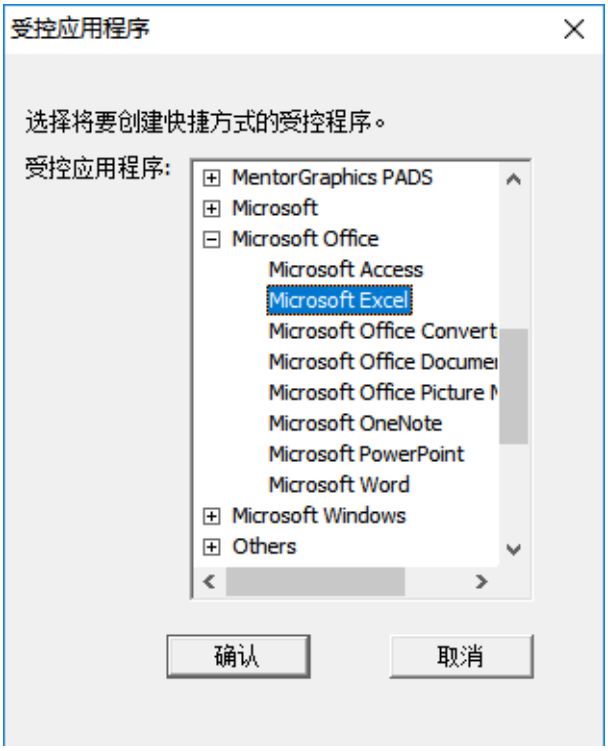
为受控应用程序创建快捷方式的步骤：
1. 在Curtain客户端，于菜单上选择 "工具 > 新建快捷方式"。

"新建快捷方式" 窗框会如下图显示。




备注：选择的应用程序必须已安装在电脑上。

2. 使用 "浏览" 按钮，来选择你想创建快捷方式的应用程序。完成后按确认键确定。




3. 使用 "浏览" 按钮，来选择创建快捷方式的位置。完成后按确认键确定。

4. 按 "创建" 键。

5. 完成。

## 6.13 - 本地加密磁盘

预设情况下，刚刚安装Curtain客户端后本地受保护区是并没有加密的，管理员可以启动本地加密磁盘来将本地受保护区加密来提升保安性，电脑启用了本地加密磁盘后是不能退回使用原先没有加密的本地受保护区。

本地加密磁盘其实是一个虚拟磁盘，当电脑关机时此虚拟磁盘是一个加密文件，当电脑启动时，此加密文件会以虚拟磁盘形式挂载，由于当电脑关机时，虚拟磁盘上的资料以加密文件形式保存，故此就算电脑丢失或被盗，资料依然受到很好的保护。本地加密磁盘的空间等同于该加密文件的大小，因此必须要确保储存该加密文件的位置有足够空间，这就是本地加密磁盘的设计。

于管理端启动本地加密磁盘的步骤：
1. 在Curtain管理端，于菜单上选择"文件>设定"。

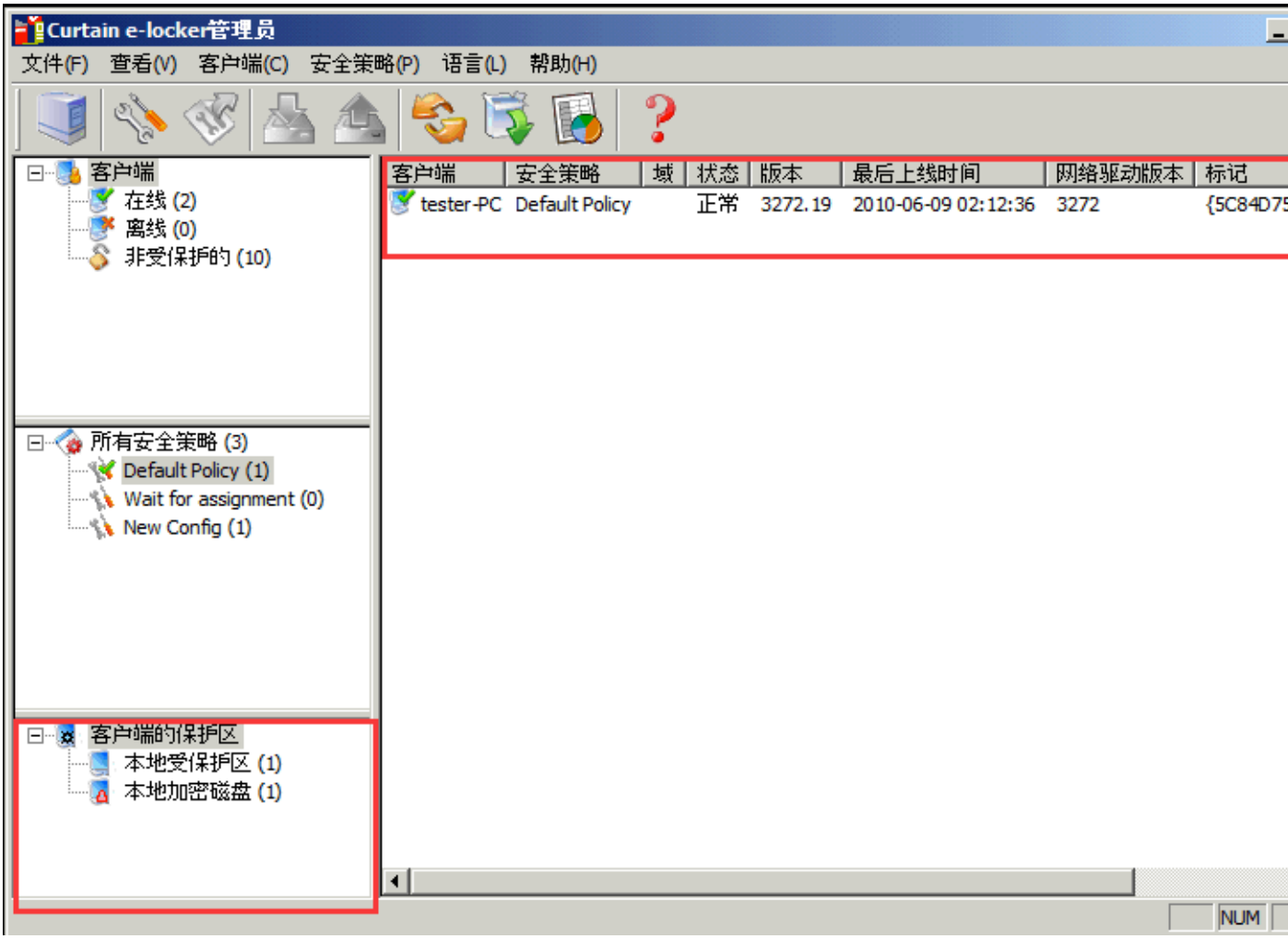
2. 于"本地加密磁盘"页，如图下勾选"启动本地加密磁盘"。
现时Curtain e-locker支持三个广为人知的加密工具来加密本地保护目录，分别是VeraCrypt、BitLocker和TrueCrypt，你可以选择其中一个加密工具。


3. 按确定键确认 (确认后不能关闭本地加密磁盘)。

4. 启动本地加密磁盘后，于菜单上会多了一个"本地加密磁盘配置"选项，并且在左手边新增了"客户端的保护区"视窗。

菜单上多了一个"本地加密磁盘配置"选项

左手边新增了"客户端的保护区"视窗

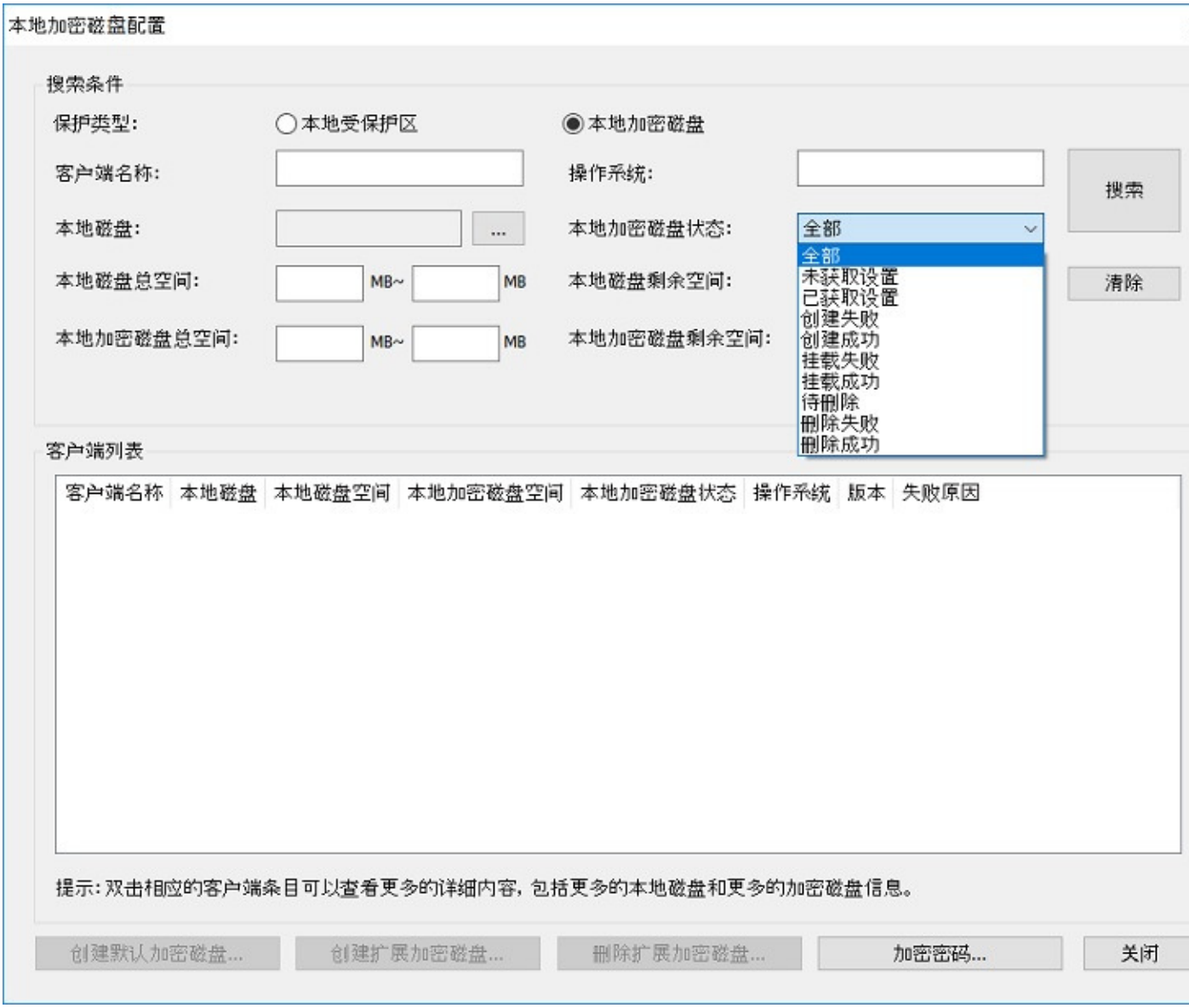



在"客户端的保护区"视窗内，会显示两种不同的客户端：
本地受保护区 - 会列出所有正在使用预设的本地受保护区的客户端，代表在本地受保护区内的资料并没有加密。
本地加密磁盘 - 会列出所有正在使用本地加密磁盘的客户端，代表所有本地受保护资料会储存在加密磁盘内。

启动本地加密磁盘后，管理员可以搜寻合适的客户端并为它们创建本地加密磁盘，请参考以下步骤。

于管理端搜寻合适的客户端并为它们创建本地加密磁盘的步骤：
1. 在Curtain管理端，于菜单上选择"文件>本地加密磁盘配置"。

本地加密磁盘配置窗框会如下图显示出来，管理员可以输入不同的搜寻条件，找出合适的电脑并进行设置。举例：
你可以搜寻最少有10GB剩余空间的电脑，并为它们建立1GB空间的本地加密磁盘。




以下是每个搜寻条件的详细介绍：

- 保护类型：本地受保护区或本地加密磁盘。
- 客户端名称：客户端的电脑名称 (支援模糊查询)。
- 操作系统：输入作业系统关键字，如Vista 。
- 本地磁盘：搜索有指定本地磁盘盘符的电脑。
- 本地磁盘总空间：指定一个搜索本地磁盘总空间的区间值，只要有一个本地磁盘满足条件都当成查询找到。
- 本地磁盘剩余空间：指定一个搜索本地磁盘剩余空间的区间值，只要有一个本地磁盘满足条件都当成查询找到。
- 本地加密磁盘总空间：指定一个搜索本地加密磁盘总空间的区间值，只要有一个本地加密磁盘满足条件都当成查询找到。
- 本地加密磁盘剩余空间：指定一个搜索本地加密磁盘剩余空间的区间值，只要有一个本地加密磁盘满足条件都当成查询找到。

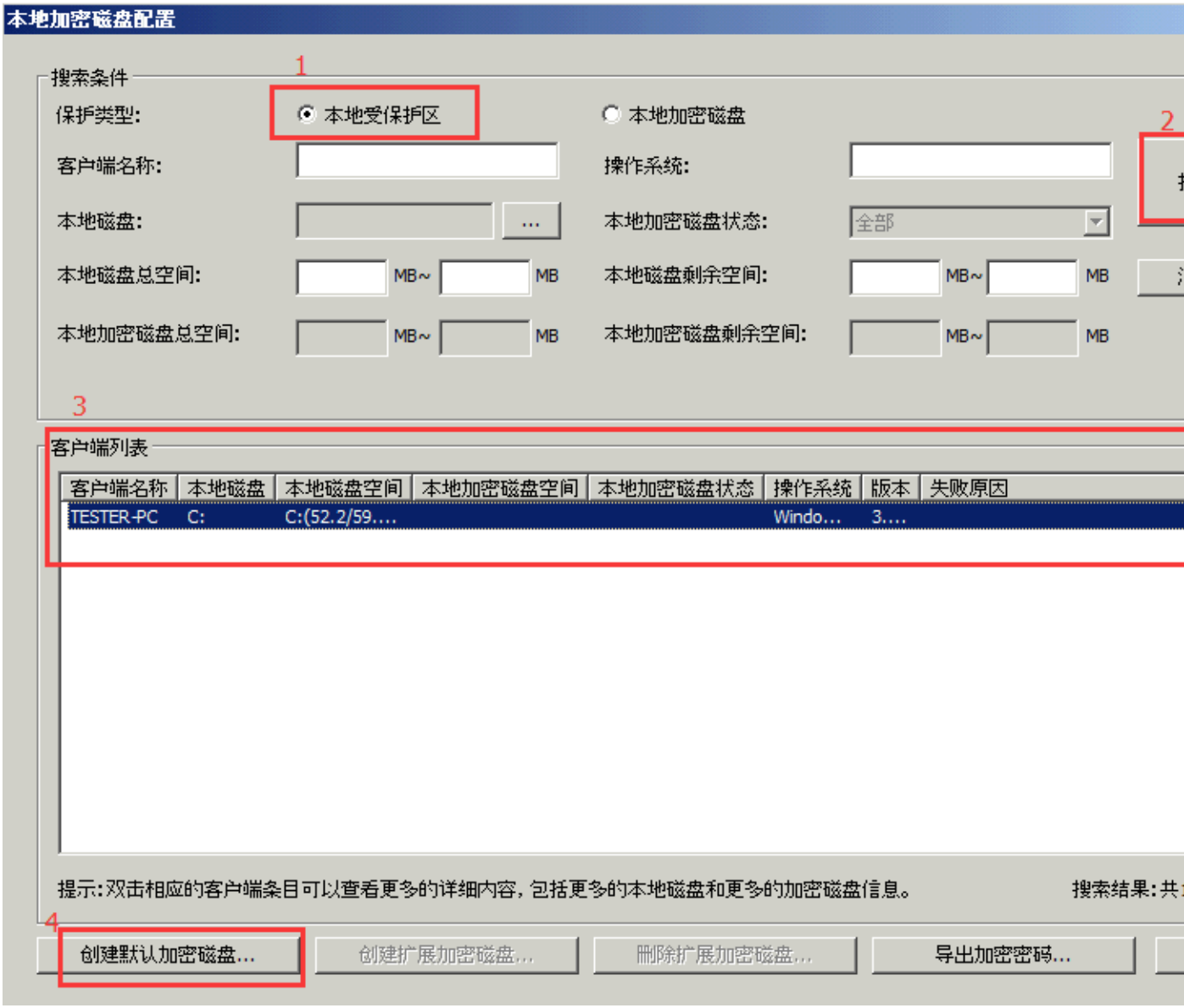
- 本地加密磁盘状态：指定欲搜索本地加密磁盘目前的状态，包括以下状态。
  - 全部：所有状态。
  - 未获取配置：客户端未获取到管理端的本地加密磁盘设置。
  - 已经获取配置：客户端已接收到管理端的本地加密磁盘设置。
  - 创建失败：客户端本地加密磁盘创建失败。
  - 创建成功：客户端本地加密磁盘已创建成功。
  - 挂载失败：客户端本地加密磁盘挂载失败。
  - 挂载成功：客户端本地加密磁盘已挂载成功（已映射为某个设置的盘符）。
  - 待删除：管理端已配置删除本地加密磁盘（只用于扩展本地加密磁盘）。
  - 删除失败：客户端删除本地加密磁盘失败（只用于扩展本地加密磁盘）。
  - 删除成功：客户端删除本地加密磁盘成功（只用于扩展本地加密磁盘）。

2. 点击 “加密密码...” 按钮，设定用于加密的密码。
在对客户端配置本地加密磁盘之前，必须先设定加密密码。

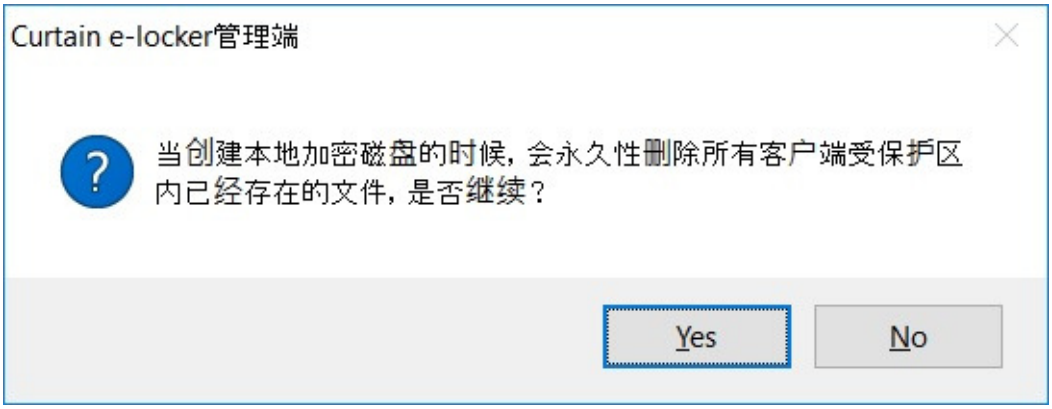

3. 输入密码，并按确认键确定。
按确认键后，系统会要求你把密码文件保存起来，请小心保存此文件。

现在，你可以搜寻合适的客户端并为它们创建本地加密磁盘(有需要可以参考上方的介绍)。举例：你可以选择保护类型为"本地受保护区"来找出所有还未使用本地加密磁盘的客户端。又或是选择保护类型为"本地加密磁盘"来找出所有已经使用本地加密磁盘的客户端。

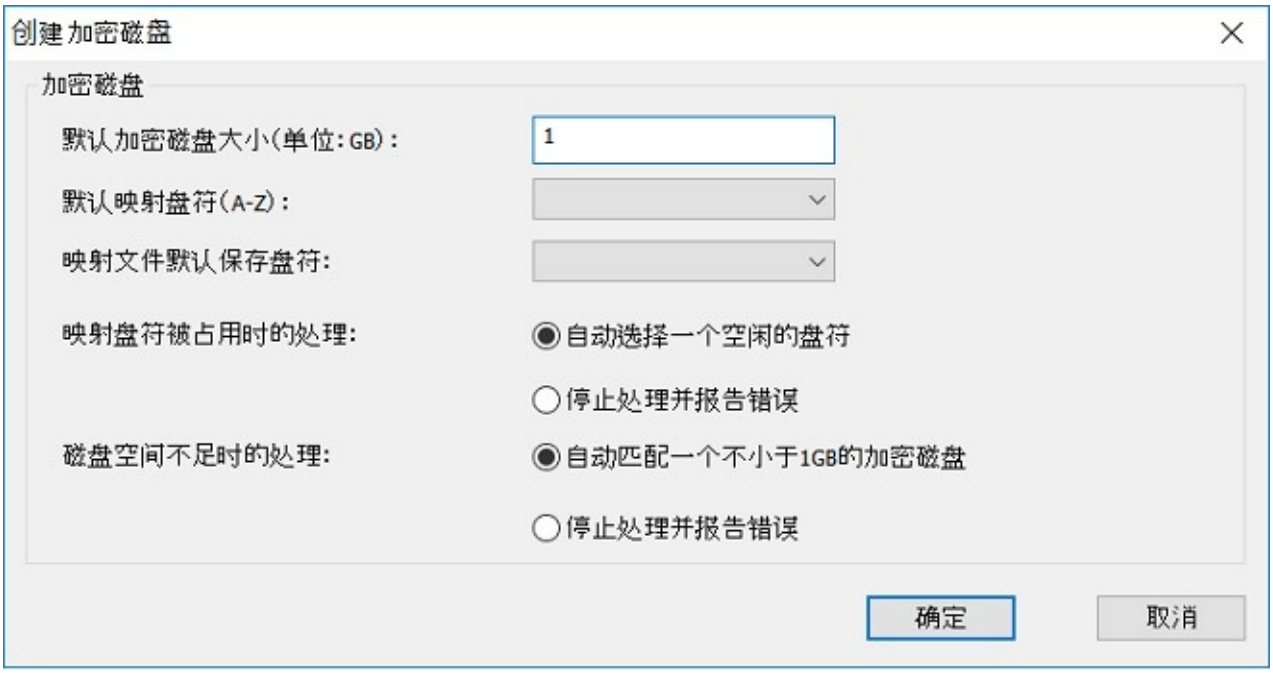
4. 选择保护类型为"本地受保护区"，并按搜寻键。
系统会列出所有还未使用本地加密磁盘的客户端(亦即是还在使用预设的本地受保护区)。




5. 选择客户端，并按"创建默认加密磁盘..." (按Ctrl键可选择多个客户端)。
系统会提醒你在将本地受保护区升级到本地加密磁盘前，要先将本地受保护区内的资料备份。



6. 当已经将本地受保护区内的资料备份好，可以按 "Yes" 继续。
然后，"创建默认加密磁盘"窗框会如下图显示，你可以为选择了的客户端设定如何创建本地加密磁盘。




"创建默认加密磁盘"窗框的选项：

- 默认加密磁盘大小（单位：GB）：要创建的本地加密磁盘的大小。
- 默认映射盘符名称（A-Z）：用作映射本地加密磁盘的盘符。
- 映射文件默认保存档符：用作储存本地加密磁盘的加密文件的默认盘符。
- 映射盘符被占用时的处理：如果用作映射本地加密磁盘的盘符被占用时的处理。
  - 自动选择一个空闲的盘符: 系统会自动将本地加密磁盘映射到一个空闲的盘符
  - 停止处理并报告错误: 系统会停止处理并报告错误
- 磁碟空间不足时的处理：如果要创建的本地加密磁盘的大小超出实际磁碟空间时的处理。
  - 自动匹配一个不小于1GB的加密磁盘: 系统会自动创建1GB的本地加密磁盘 (不理管理员原先设定的大小)
  - 停止处理并报告错误: 系统会停止处理并报告错误

7. 配置好相应的参数后，点击 “确定” 。
当下一次用户打开Curtain客户端时，系统会提示用户创建本地加密磁盘。

下面是一个例子，可以作为参考:

- 默认加密磁盘大小（单位：GB）：10
- 默认映射盘符名称（A-Z）：F:
- 映射文件默认保存档符：C:
- 映射盘符被占用时的处理：自动选择一个空闲的盘符
- 磁碟空间不足时的处理：自动匹配一个不小于1GB的加密磁盘

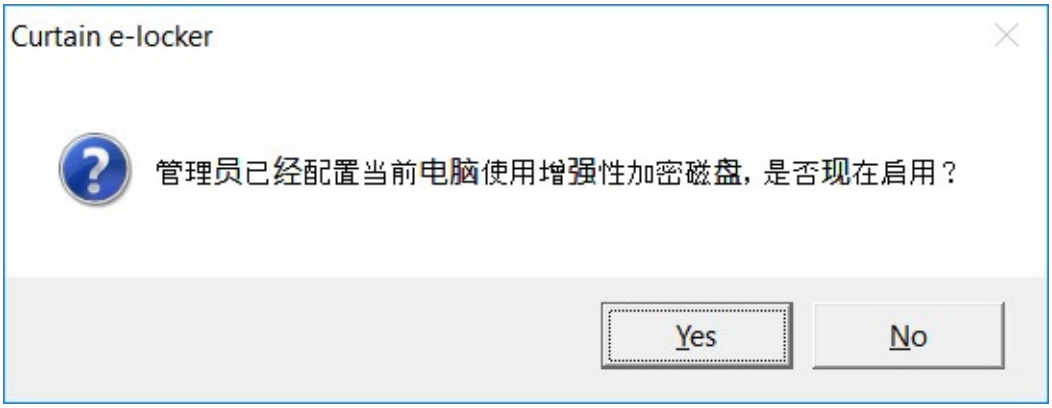
这个例子代表会创建一个10GB大的本地加密磁盘，并将本地加密磁盘映射为F: 盘。当电脑关机时，本地加密磁盘的加密文件会储存在C: 盘。如果C: 盘没有10GB空间，系统会自动创建1GB的本地加密磁盘。如果F: 盘符被占用时，系统会自动将本地加密磁盘映射到一个空闲的盘符。

8. 于"本地加密磁盘配置"窗框，双击一个客户端，可以查看客户端详细资讯。

下图表示该客户端已经成功创建了本地加密磁盘。


回到Curtain客户端上，完成创建本地加密磁盘的步骤：

1. 当下一次用户打开Curtain客户端时，系统会提示用户创建本地加密磁盘。




2. 按 "Yes" 继续，或按"No"推迟创建本地加密磁盘。

按 "Yes" 后，当用户重启电脑后，系统会创建本地加密磁盘，请记得要先将本地受保护区内的资料备份。

3. 重启电脑并打开Curtain客户端后，系统会如下图弹出提示。


4. 按 "OK" 继续，系统会立即创建本地加密磁盘。

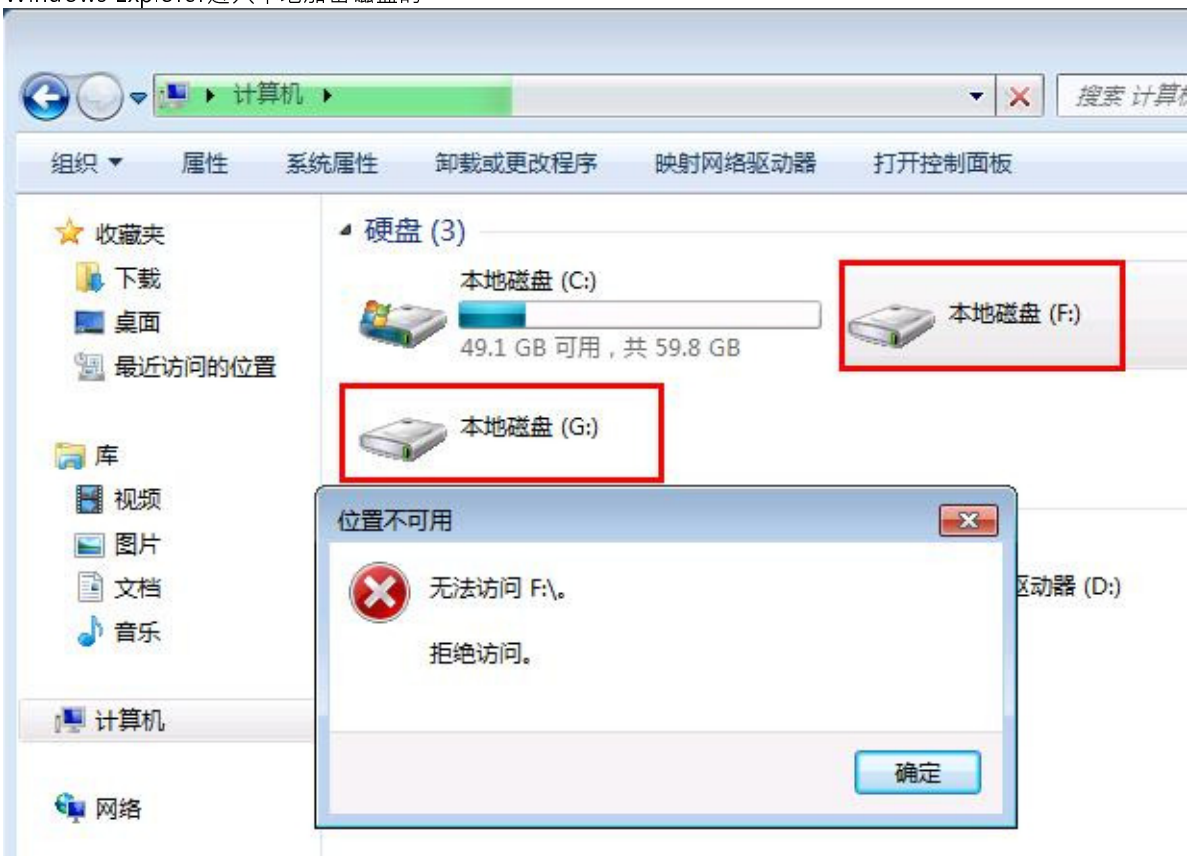

5. 完成后，Curtain客户端的介面会显示本地加密磁盘。

于Curtain客户端，本地加密磁盘会显示在我的电脑下面。

第一次创建的本地加密磁盘必定为默认的本地加密磁盘，如有需要，管理员可以创建扩展的本地加密磁盘。在加密磁盘下面，你可以看到有两个文件夹，分别是个人及公共。个人的文件夹是只给当前登录的用户使用，所以个人文件夹可以用作存放个人敏感的文件，而公共的文件夹是给所有用户使用的，所以公共文件夹可以用作于客户端上分享文件。

如果在升级本地加密磁盘前，在Curtain客户端已有使用本地附加受保护区，则该本地附加受保护区会维持不变，本地加密磁盘不适用于本地附加受保护区的。

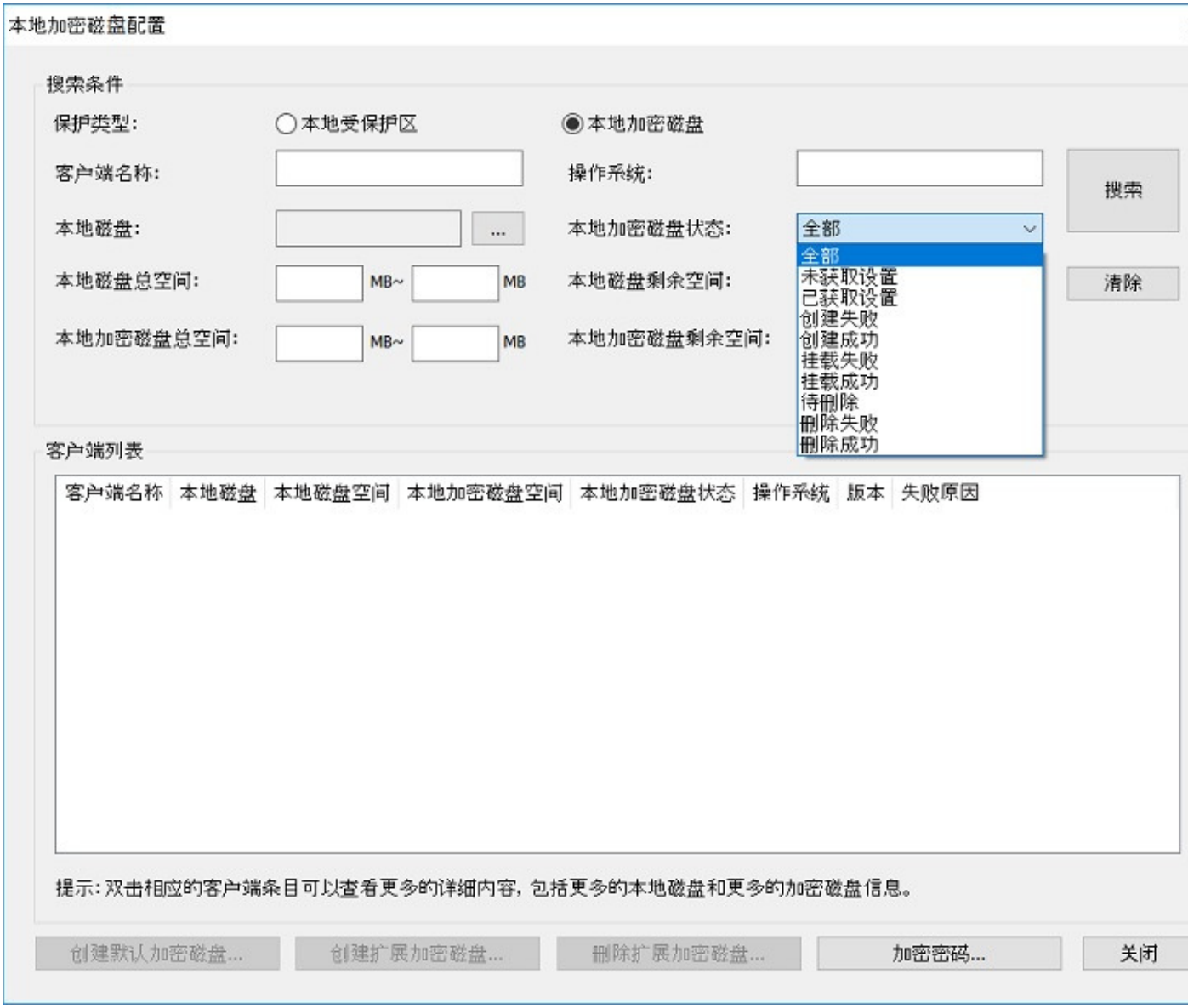
在上图的例子中，F:盘是默认本地加密磁盘，而G:盘是扩展本地加密磁盘，用户可以通过受Curtain e-locker保护的介面(如:Curtain客户端或受保护的应用程式)来使用保护区内的资料(包括本地加密磁盘)，用户是不能使用Windows Explorer进入本地加密磁盘的。




管理员处理那些创建/挂载失败的客户端的步骤：

有些客户端会因为不同原因不能创建或挂载本地加密磁盘，例如：没有足够硬碟空间或映射盘符被占用等，管理员可以找出那些创建/挂载失败的客户端，修改设定并再次为它们创建本地加密磁盘。

1. 在Curtain管理端，于菜单上选择"文件>本地加密磁盘配置"。



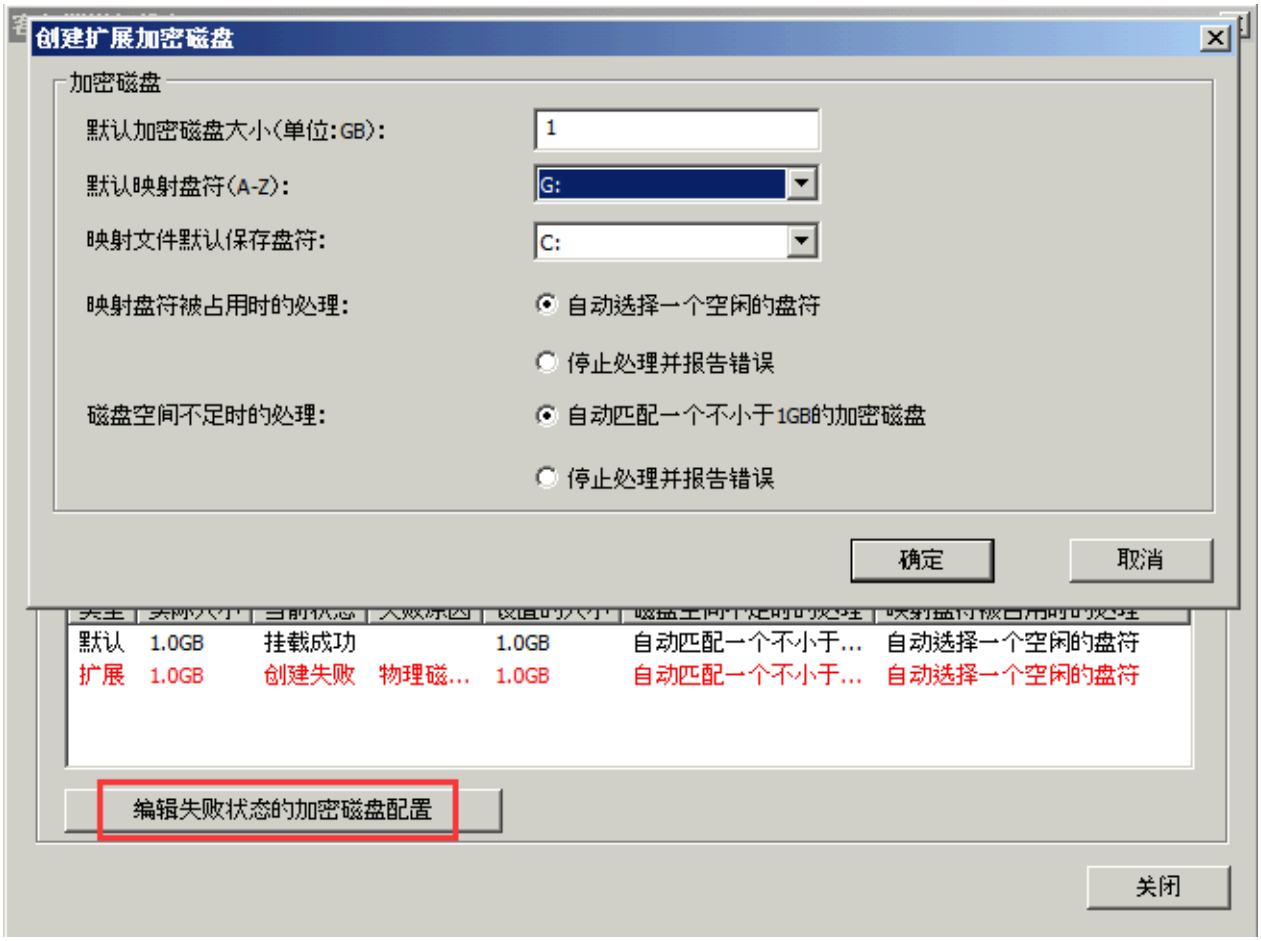

2. 于保护类型，选择"本地加密磁盘"。

3. 于本地加密磁盘状态，选择"创建失败"或"挂载失败"。

4. 按搜寻键找出那些创建/挂载失败的客户端。

5. 双击一个客户端，可以查看客户端详细资讯。

6. 按下图的按钮来修改本地加密磁盘的设定。




7. 配置好相应的参数后，点击“确定”。
当下一次用户打开Curtain客户端时，系统会再次提示用户创建本地加密磁盘。

于管理端搜寻合适的客户端并为它们创建扩展本地加密磁盘的步骤：
有时管理员需要为客户端创建扩展本地加密磁盘，例如：默认本地加密磁盘的空间已经不够使用，这时管理员可以为这些客户端创建扩展本地加密磁盘。

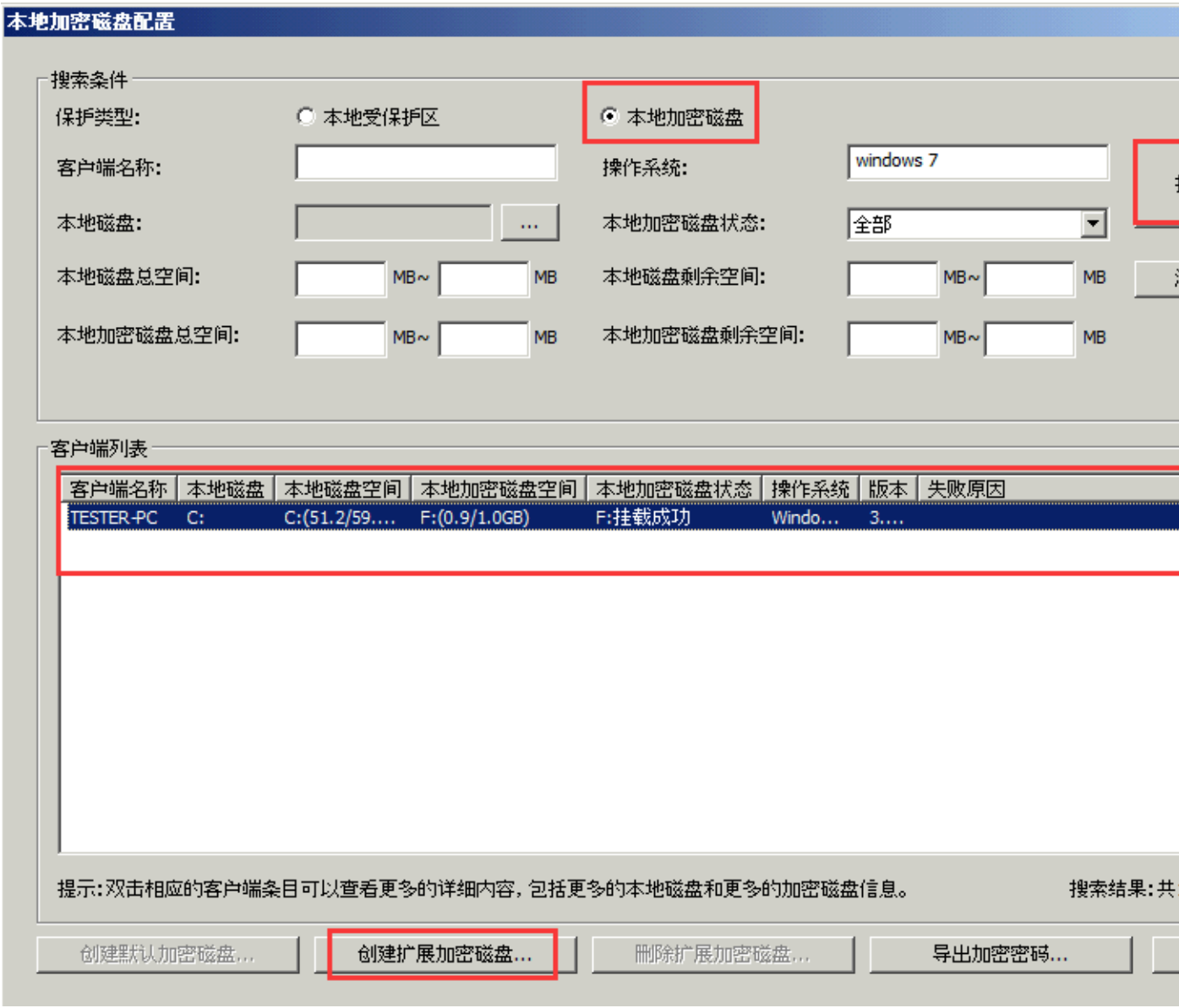
1. 在Curtain管理端，于菜单上选择"文件> 本地加密磁盘配置"。

本地加密磁盘配置窗框会如下图显示出来，管理员可以输入不同的搜寻条件，找出合适的电脑并进行设置。举例：你可以搜寻本地加密磁盘剩余空间少于500MB的客户端。

2. 输入条件，并按搜寻。

3. 选择客户端，并按"扩展默认加密磁盘..." (按Ctrl键可选择多个客户端)。

创建扩展本地加密磁盘的步骤和创建默认本地加密磁盘是差不多的，你可以参考之前创建默认本地加密磁盘的步骤。

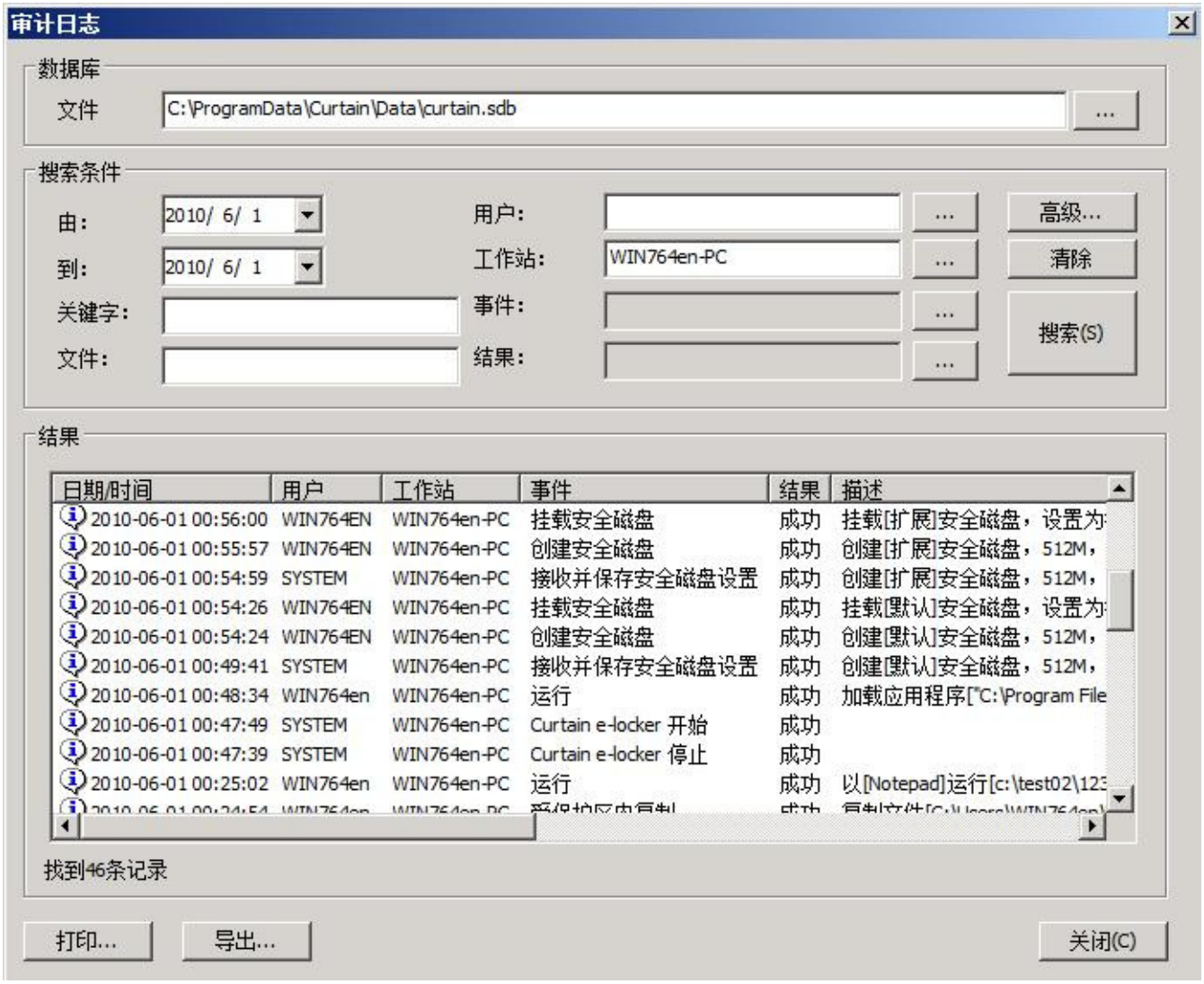



于管理端查看关于本地加密磁盘的审计日志的步骤：
所有关于本地加密磁盘的操作(如:创建、挂载、删除本地加密磁盘等)都会记录到审计日志中，以供查看。

1. 在Curtain管理端，于菜单上选择"文件>审计日志"。

2. 输入条件，并按搜寻。

下图是一个例子，以作参考。

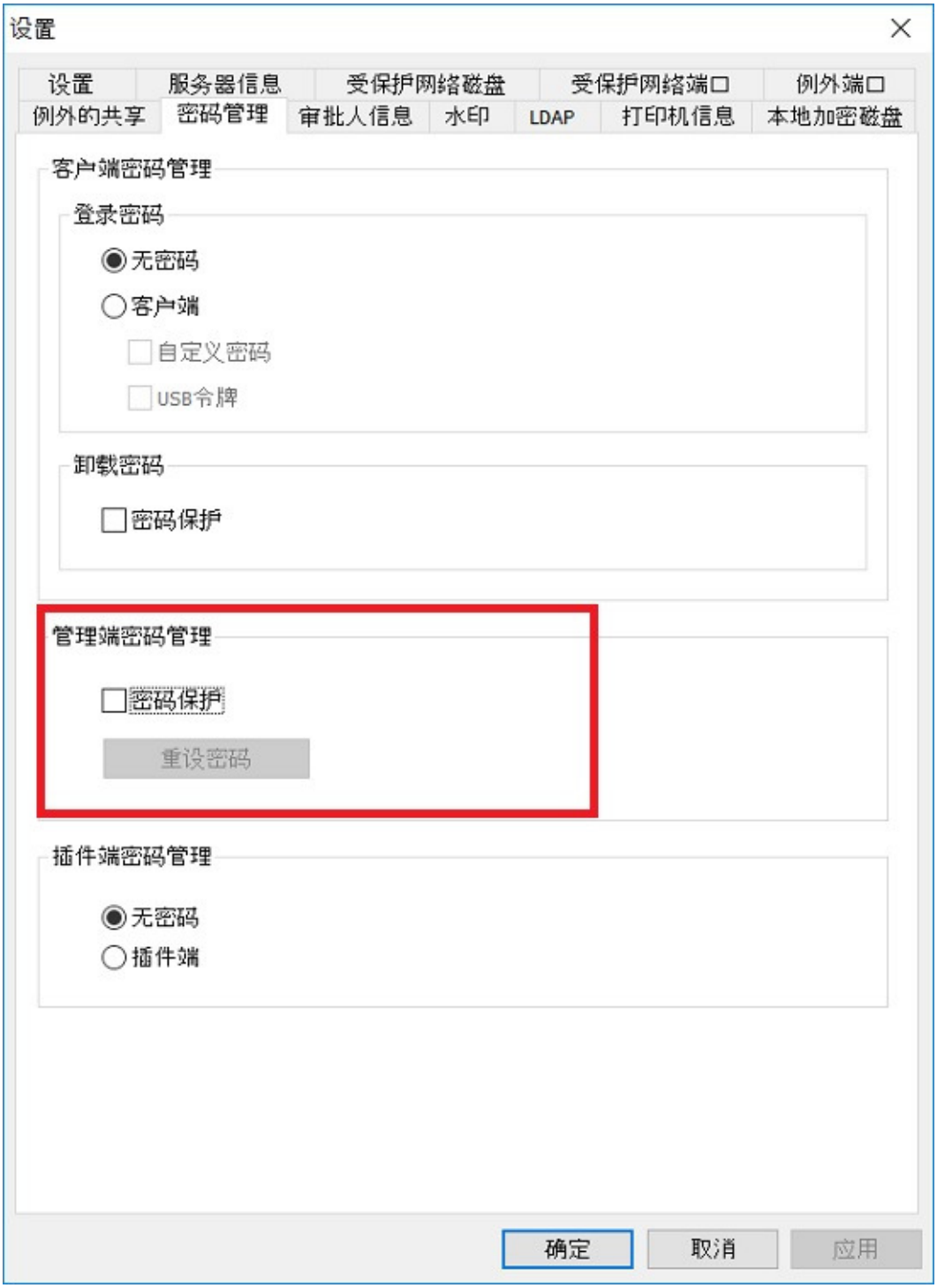


## 6.14 - 为Curtain管理端、服务器插件和客户端设定登录密码

在预设情况下，打开Curtain管理端、服务器插件或客户端，是不用输入密码的，管理员可以启动密码保护来加强系统保安。

开启Curtain管理端密码保护的步骤:
1. 在Curtain管理端，于菜单上选择"文件>设定"。

2. 于"密码管理"页，启动"管理端密码管理"下的密码保护。如果是第一次启动管理端密码保护，系统会弹出对话框要求设定密码。如果之前启动过此功能，则会使用原有完有密码。



3. 输入密码后按确定键确认。


4. 完成，下一次管理员必需输入正确密码才能打开Curtain管理端。

开启Curtain服务器插件密码保护的步骤:
1. 在Curtain管理端，于菜单上选择"文件>设定"。

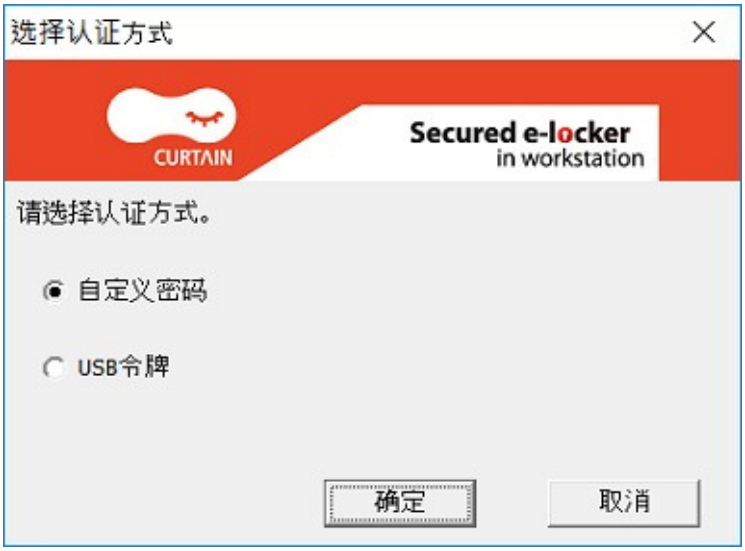
2. 于"密码管理"页，"插件端密码管理"下选择插件端。如果是第一次启动插件端密码保护，下一次打开Curtain服务器插件时，系统会弹出对话框要求设定密码。如果之前启动过此功能，则会使用原有完有密码。

开启Curtain客户端密码保护的步骤:
1. 在Curtain管理端，于菜单上选择"文件>设定"。

2. 于"密码管理"页，"客户端密码管理 > 客户端"下有两个选项:
自定义密码 - 用户下一次打开Curtain客户端时，系统会弹出对话框要求设定密码。如果之前启动过此功能，则会使用原有完有密码。
USB令牌 - 用户下一次打开Curtain客户端时，系统会弹出对话框要求插入载有个人电子证书的USB令牌作登入之用。

3. 按确定键确认。

4. 在管理员同时选择了"自定义密码"和"USB令牌"，代表用户可以决定用其中一种方式登入。



## 6.15 - 为Curtain管理端、服务器插件和客户端更改或重设登入密码

如果管理员已为Curtain管理端、服务器插件或客户端启动了密码保护，使用者必需输入密码才能打开相关程序，如果想更改或重设登入密码，请参考以下步骤。

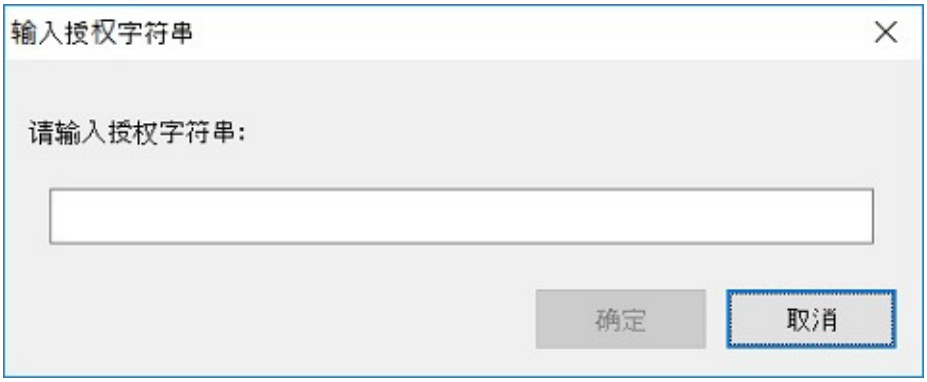
为Curtain管理端、服务器插件和客户端更改或重设登入密码的步骤:
1. 当登入Curtain管理端、服务器插件或客户端时，选择 "修改密码"。


"密码设置" 窗框会如下图显示。

2. 输入旧密码和新密码。

3. 按确定键确认。

4. 如果你忘记了密码，请联络管理员，管理员可以选择 "忘记密码"，并输入授权字符串来重设你的登入密码。



# 7 - 后续维护

## 7.1 - 补丁的管理

系统管理员可以从我们的网站下载最新补丁，然后将补丁安装在Curtain管理员上，所有Curtain客户端的程序便会自动被更新，系统管理员不需要在每一台用户计算机上安装最新补丁。

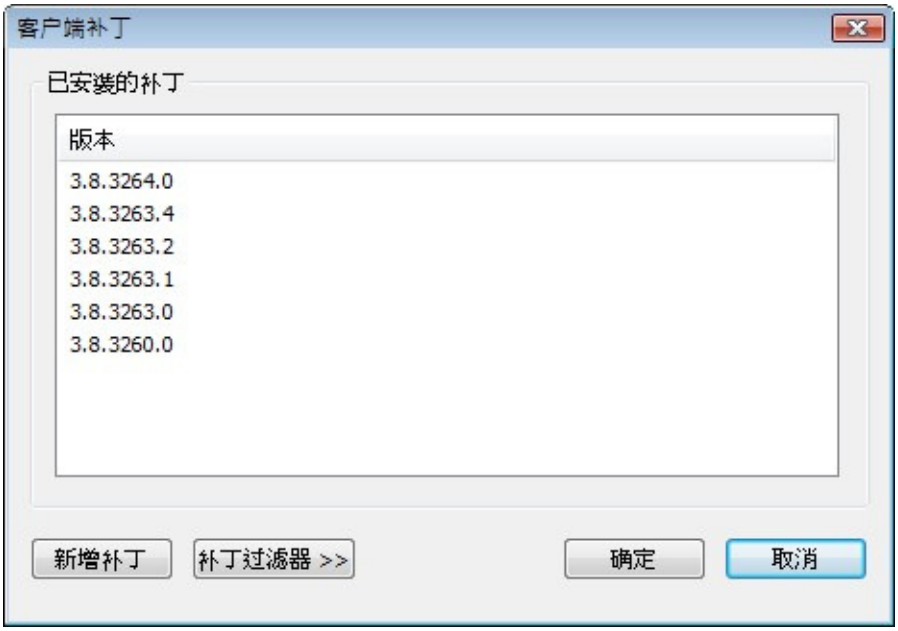
安装补丁方法:
1. 从我们的网站下载适当的补丁。当发布一个新的版本时，一般情况下会有五个补丁。举例 (版本号是3273.04):
   - CurtainFullPatch_Win32(327304).zip - 给安装在32位元操作系统上的Curtain管理员
   - CurtainFullPatch_X64(327304).zip - 给安装在64位元操作系统上的Curtain管理员
   - CurtainAdminPatch_Win32(327304).zip - 如果你只想为Curtain管理员或Curtain服务器插件安装新的版本，你可以运行此补丁，此补丁并不会更新客户端的
   - CurtainAdminPatch_X64(327304).zip - 如果你只想为Curtain管理员或Curtain服务器插件安装新的版本，你可以运行此补丁，此补丁并不会更新客户端的
   - CurtainClientPatch(327304).zip - 如果你只想为个别的Curtain客户端安装新的版本，你可以直接在客户端上运行此补丁

2. 解压补丁。

3. 于安装了Curtain管理员那台服务器上执行 CurtainFullPatch_Win32.exe 或 CurtainFullPatch_X64.exe 补丁，当下一次Curtain客户端连接到Curtain管理员时，Curtain客户端的程序便会自动被更新。

4. 如有其他Curtain服务器插件，需要执行 CurtainAdminPatch_Win32.exe 或 CurtainAdminPatch_X64.exe 补丁把服务器插件更新。

查看所有已安装的补丁:
- 按"更新补丁"按钮 或 选"文件>客户端补丁"

## 7.2 - 管理员迁移到另一台计算机上

有以下两种情况:
(1) 新的Curtain管理员的计算机名称与IP地址和现时的Curtain管理员的计算机名称与IP地址是一样的。
(2) 新的Curtain管理员的计算机名称与IP地址和现时的Curtain管理员的计算机名称与IP地址是不一样的。

迁移前的准备事项:
1. 将现时Curtain管理员上的安全策略先作备份，请将以下文件夹和文档复制一份。
- C:\Program Files\Coworkshop\Curtain 3\bin\Config
- C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.dat
- C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.enx

2. 将现时Curtain管理员上的活动记录先作备份，请将以下文档复制一份。
- C:\Program Files\Coworkshop\Curtain 3\bin\Curtain.mdb (它存在于旧版本中)
- 将整个 "Curtain" 文件夹备份
  - 于Windows 2000 / XP / 2003，此文件夹位于 C:\Documents and Settings\All Users\Application Data
  - 于Windows 2008 / Vista / Win7，此文件夹位于 C:\ProgramData

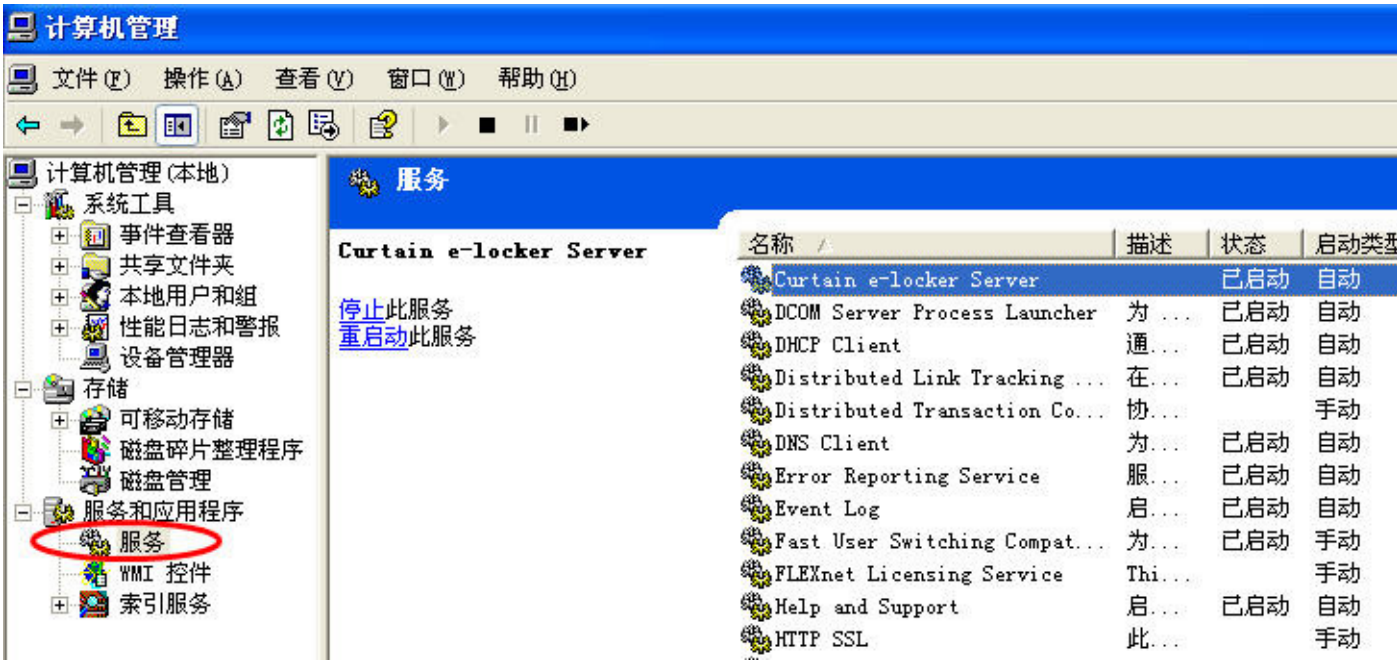
情况1 - 新的Curtain管理员的计算机名称与IP地址和现时的Curtain管理员的计算机名称与IP地址是一样的:
以下是迁移步骤:
1. 将现时Curtain管理员关机，或将它从网络环境中断开。

2. 安装一台新计算机，并使用一样的计算机名称与IP地址。

3. 在该台新计算机上，安装Curtain管理员(详细步骤请参考相关资料)。

4. 激活刚安装好的Curtain管理员(详细步骤请参考相关资料)。

5. 将之前备份好的安全策略和活动记录复制到新的Curtain管理员上。
- 于计算机管理，将"Curtain e-locker Server"服务停止。
- 将之前备份好的文件夹和文档复制到相关位置。
- 于计算机管理，将"Curtain e-locker Server"服务启动。



6. 由于新的Curtain管理员使用一样的计算机名称与IP地址，Curtain客户端会自动连接到新的Curtain管理员。

7. 完成迁移

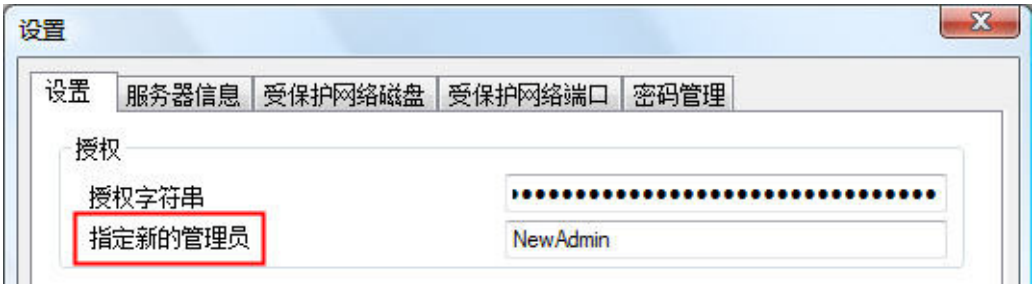
情况2 - 新的Curtain管理员的计算机名称与IP地址和现时的Curtain管理员的计算机名称与IP地址是不一样的:
以下是迁移步骤:
1. 安装一台新计算机，并使用不一样的计算机名称与IP地址。

2. 在该台新计算机上，安装Curtain管理员(详细步骤请参考相关资料)。

3. 激活刚安装好的Curtain管理员(详细步骤请参考相关资料)。

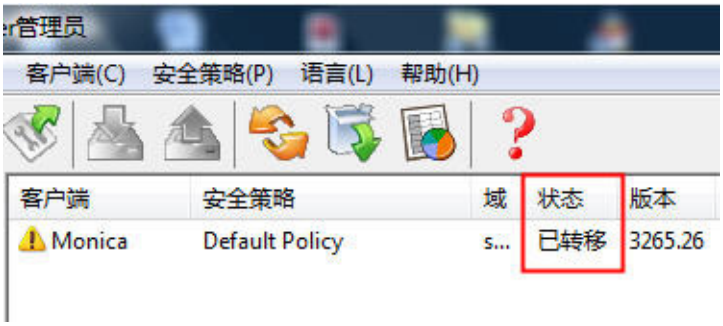
4. 将之前备份好的安全策略和活动记录复制到新的Curtain管理员上。
- 于计算机管理，将"Curtain e-locker Server"服务停止。
- 将之前备份好的文件夹和文档复制到相关位置。
- 于计算机管理，将"Curtain e-locker Server"服务启动。

5. 在现时的Curtain管理员，于菜单上选择"文件> 设置"。




6. 于"指定新的管理员"上，输入新的Curtain管理员的计算机名称或IP地址，并按确定。

当Curtain客户端连接到现时的Curtain管理员时，系统会通知客户端有新的Curtain管理员。知悉后，Curtain客户端的状态会转成"已转移"。当所有的Curtain客户端的状态都会转成"已转移"后，管理员可以将旧的Curtain管理员关机，所有的Curtain客户端正式被新的Curtain管理员管理。




7. 完成迁移

备注: 新的Curtain管理员必须使用与旧的Curtain管理员使用的"授权字符串"一样。

## 7.3 - 手动备份与恢复Curtain管理员的安全策略和活动记录

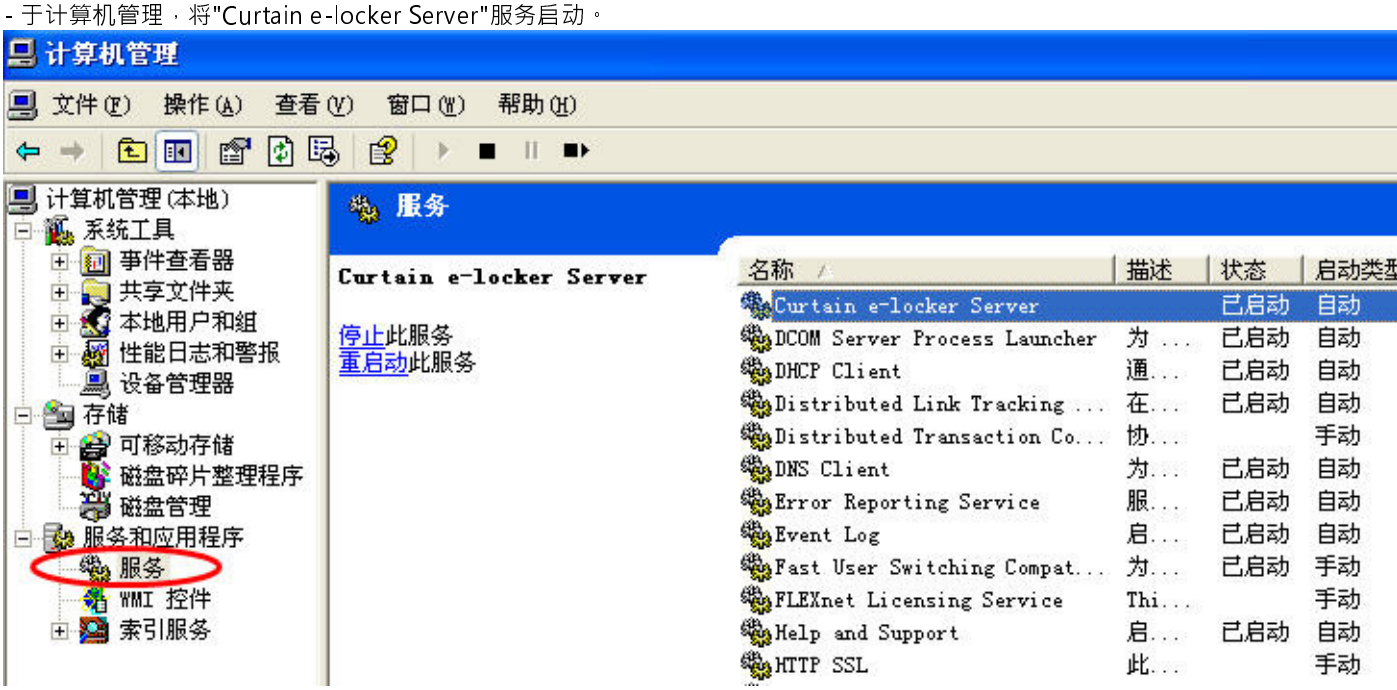
备份安全策略和活动记录:

1. 将现时Curtain管理员上的安全策略先作备份，请将以下文件夹和文档复制一份。
   - C:\Program Files\Coworkshop\Curtain 3\bin\Config
   - C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.dat
   - C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.enx

2. 将现时Curtain管理员上的活动记录先作备份，请将以下文档复制一份。
   - C:\Program Files\Coworkshop\Curtain 3\bin\Curtain.mdb (它存在于旧版本中)
   - 将整个 "Curtain" 文件夹备份
     - 于Windows 2000 / XP / 2003，此文件夹位于 C:\Documents and Settings\All Users\Application Data
     - 于Windows 2008 / Vista / Win7，此文件夹位于 C:\ProgramData

恢复安全策略和活动记录:

- 于计算机管理，将"Curtain e-locker Server"服务停止。
- 将之前备份好的文件夹和文档复制到相关位置。
- 于计算机管理，将"Curtain e-locker Server"服务启动。



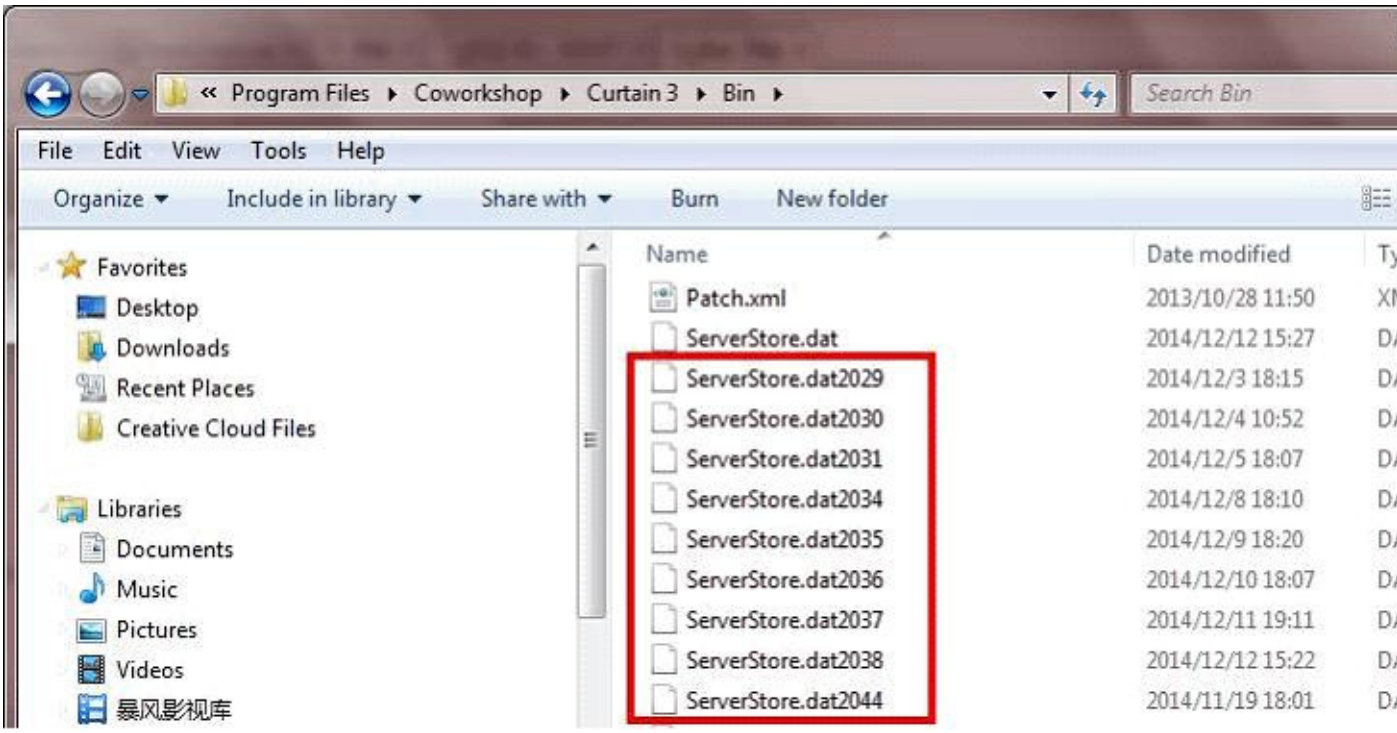

## 7.4 - 自动备份Curtain管理员的安全策略

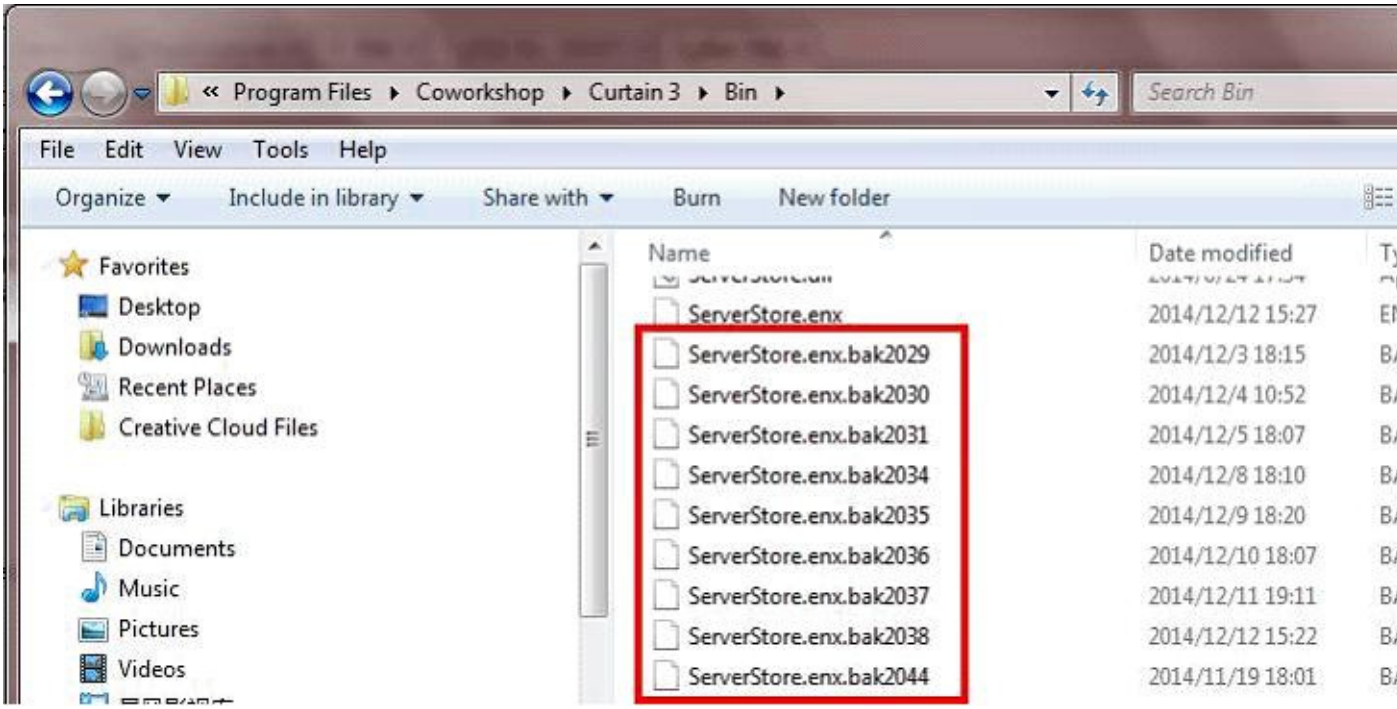
Curtain管理员有自动备份安全策略的功能，如果因为突发状况而导致策略被损坏(如:异常关机)，管理员可以手动恢复安全策略。

安全策略是储存在以下文件夹和文档中：

- C:\Program Files\Coworkshop\Curtain 3\bin\Config
- C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.dat
- C:\Program Files\Coworkshop\Curtain 3\bin\ServerStore.enx

在相关位置，你可以找到相同名称的文件夹和文档其后缀名会以数字编号标识(如下图)，你可以按最后修改日期找出希望恢复的安全策略。




恢复安全策略:
- 于电脑管理，将"Curtain e-locker Server"服务停止。
- 将要恢复的安全策略的文件夹和文档，重命名原名称即可。
- 于电脑管理，将"Curtain e-locker Server"服务启动。

重新开启Curtain管理端，会发现之前的策略和设置已经全部还原。

# 8 - 常见问题

## 8.1 - 如何避免和杀软冲突？

如今市场上流行的安全软件有很多，例如趋势(Trend Micro)，卡巴斯基(Kaspersky)，迈克菲(Mcafee)，360杀毒，爱维士(Avast)，AVG，金山毒霸等，有些杀毒软件不需要更改任何设置即可和Curtain客户端完美兼容，而有些杀毒软件则需要设置Curtain客户端相关文件为“信任”或“例外”才能正常工作。以下是相关文件列表和路径：

Curtain驱动路径及文件路径：

- 32位系统： C:\Program Files\Coworkshop\Curtain 3\CBin\
- 64位系统： C:\Program Files\Coworkshop\Curtain 3\CBin\ and C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\
- 驱动： C:\windows\system32\drivers （curtain.sys, CurtainP.sys, CurtainPM.sys, CurtainWfp.sys, CurtainRP.sys, CurtainPD.sys, CrNetFltW.sys）

如果杀毒软件不允许添加路径，那么需要手动添加以下.EXE执行文件：

- CrClient.exe
- CrClientSvc.exe
- CrCmd.exe
- CrCmdAppMon.exe
- CrCmdAW.exe
- CrCmdW.exe
- CrCryptFormat.exe
- CrFileDialog.exe
- CrProcMonSvc.exe
- CrShellExecProxy.exe
- CrUtilSvc.exe
- CurtainCB.exe
- CurtainParser.exe
- CurtainTips.exe
- PDMWEClient.exe
- searchmonkey.exe

备注: 包括C:\Program Files\Coworkshop\Curtain 3\CBin\ 和 C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\目录下所有的EXE文件。

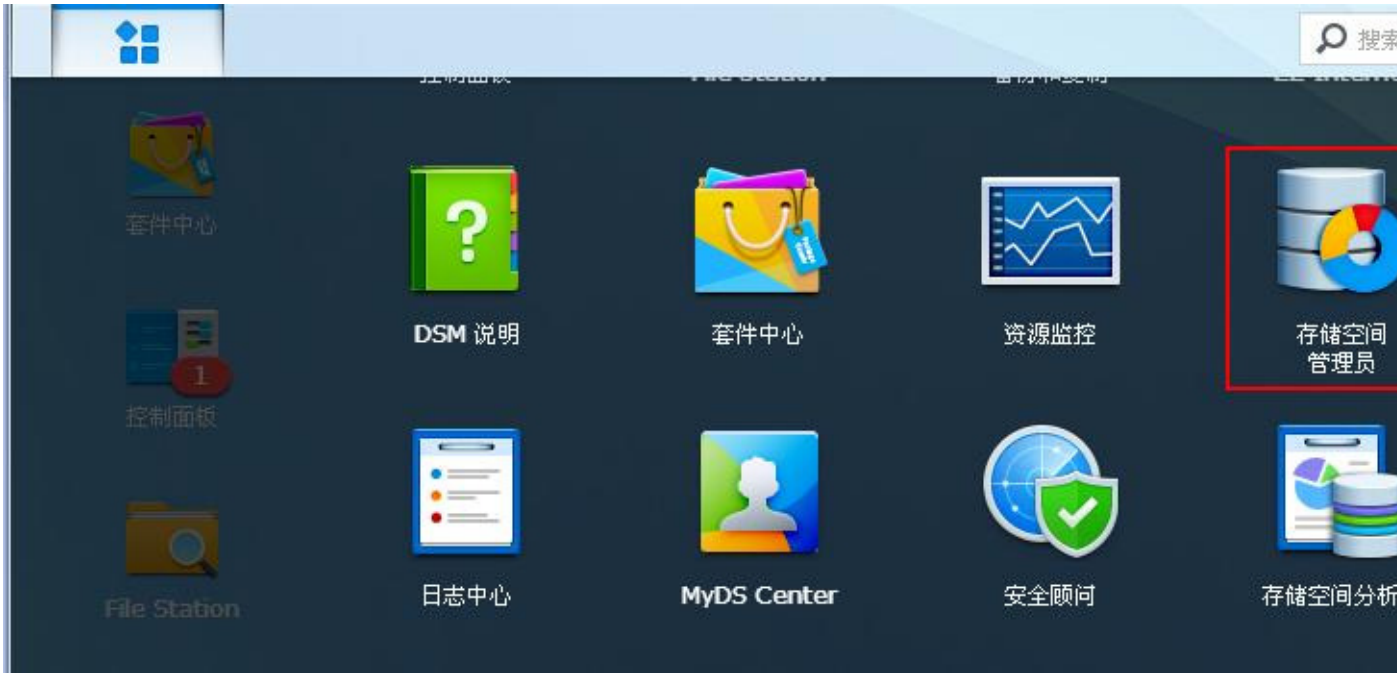
## 8.2 - 使用易锁通过iSCSI来保护NAS

背景
目前大多数NAS存储服务器都运行Linux，并不允许人们在NAS上安装软件，这意味着我们无法在NAS上安装Curtain服务器插件来保护共享文件夹。故此，我们可以通过iSCSI将其作为本地虚拟磁盘挂载到Windows服务器上来保护NAS。首先，您需要在NAS上创建iSCSI LUN（逻辑单元），然后使用Windows iSCSI Initiator在Windows服务器上创建虚拟磁盘。最后，您可以共享虚拟磁盘并通过Curtain e-locker进行保护。

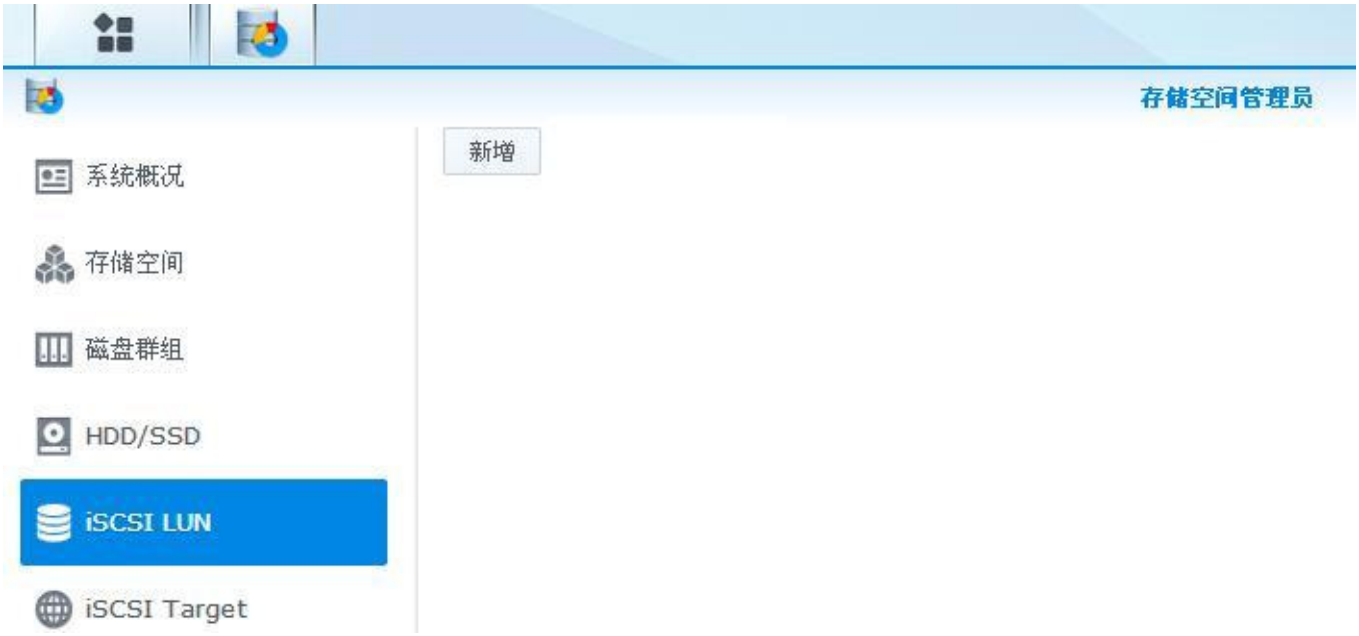
备注: 我们使用Synology DiskStation演示如何进行设定，如果使用其他NAS服务器，界面和命名将会不同。

## 创建ISCSI目标

1. 从DSM系统上进入主菜单，打开“存储空间管理员”。如图：




2. 进入“存储空间管理员”界面，选择“ISCSI LUN”。如图：



3. 单击“新增”按钮，将会弹出设置窗口，引导创建“ISCSI LUN”，选择LUN类型为“iSCSI LUN(一般文件)”，单击“下一步”。如图：

4. 设置iSCSI LUN属性，容量大小由管理员设定，以“G”为单位，其他设置保持不变，单击“下一步”。如图：

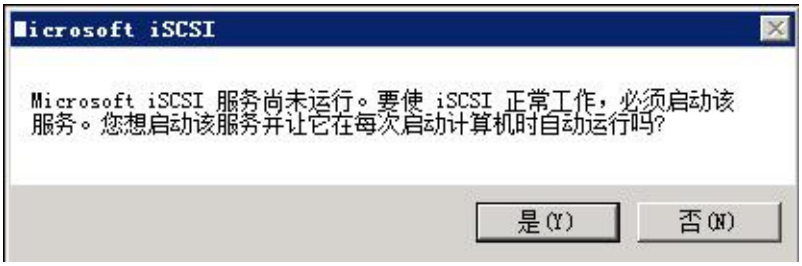
5. 勾选“启用CHAP”，并输入名称和密码，单击“下一步”。如图：

6. 再次检查设置，如果确认没有问题，单击“下一步”。如图：

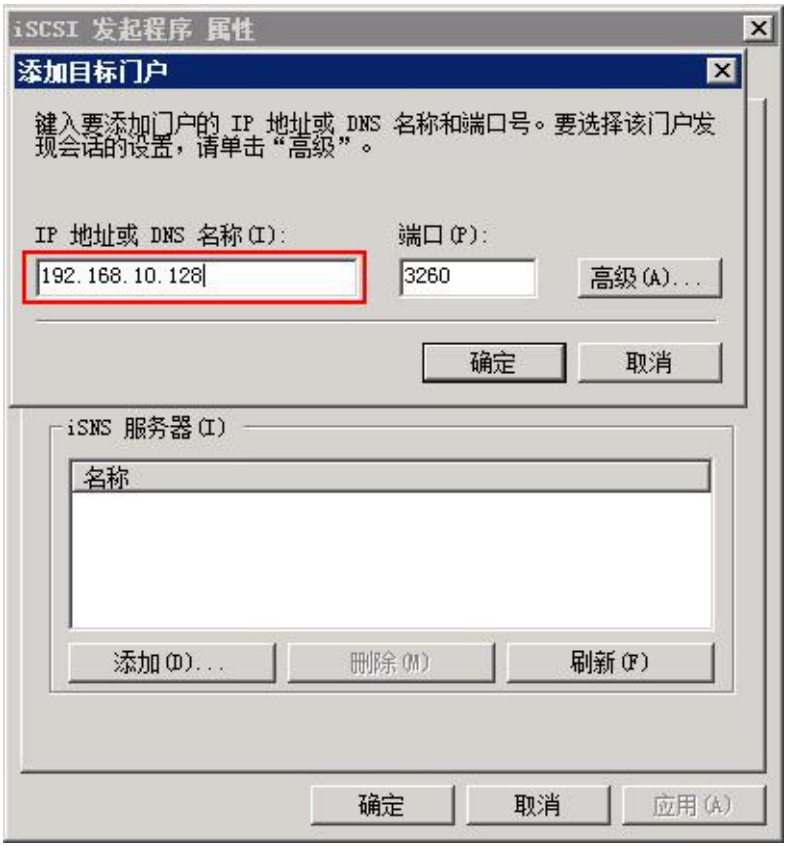

7. 在"存储空间管理员"界面上，你可以看到创建好的iSCSI LUN。如图：


映射iSCSI目标到服务器本地虚拟磁盘

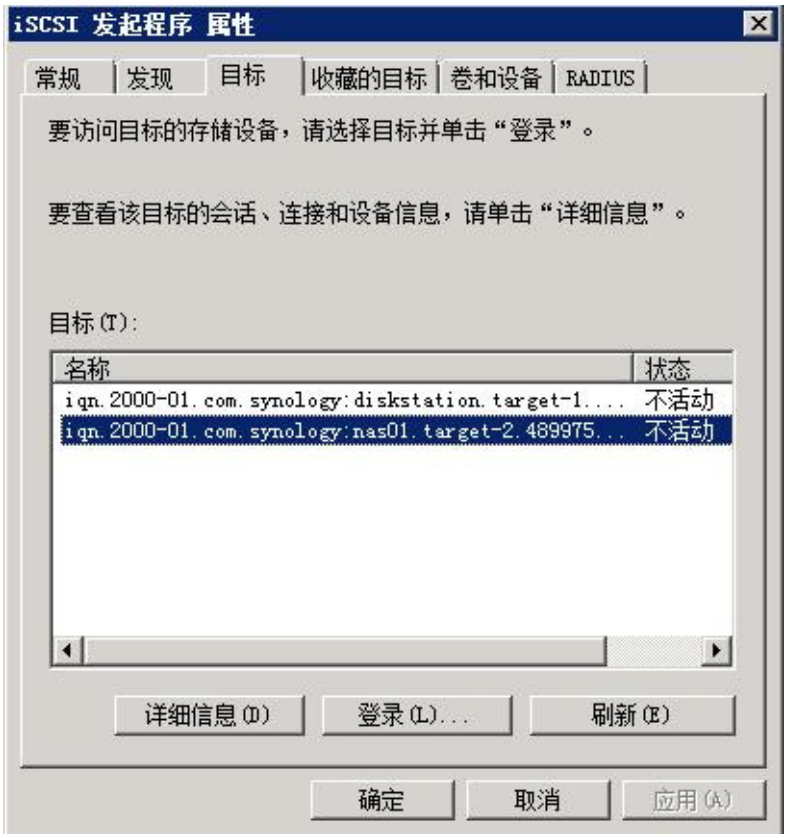
8. 在Windows服务器中，依次打开“开始菜单->管理工具->iSCSI发起程序 “，如果是第一次启用iSCSI服务，将会弹出对话框，单击“是”即可。如图：

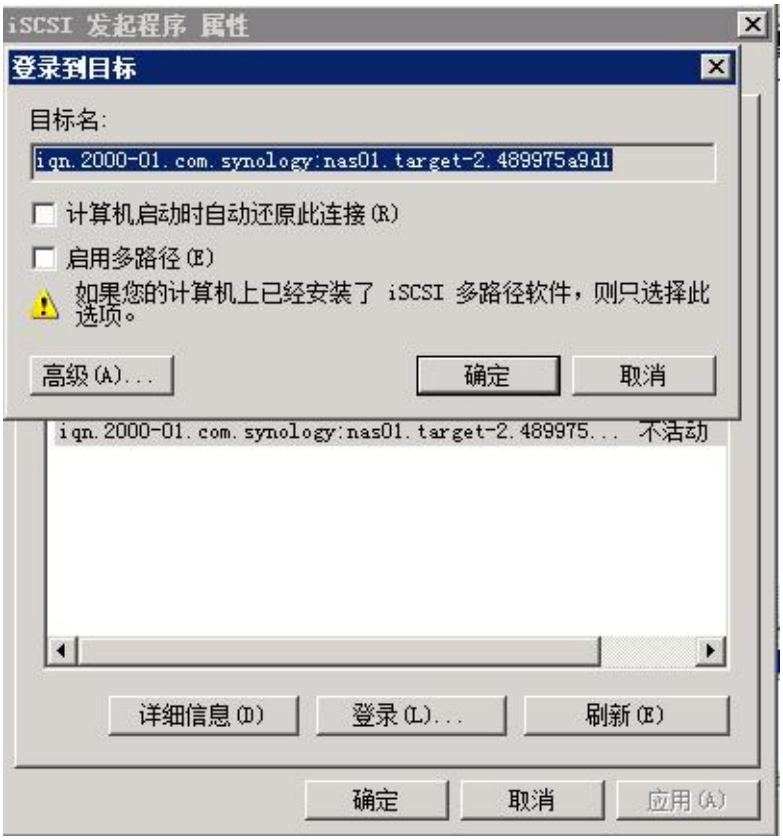


9. 在“iSCSI发起程序”属性界面，选择“发现”，并单击“添加门户”，并输入NAS的IP地址，然后单击“确定”按钮。如图：

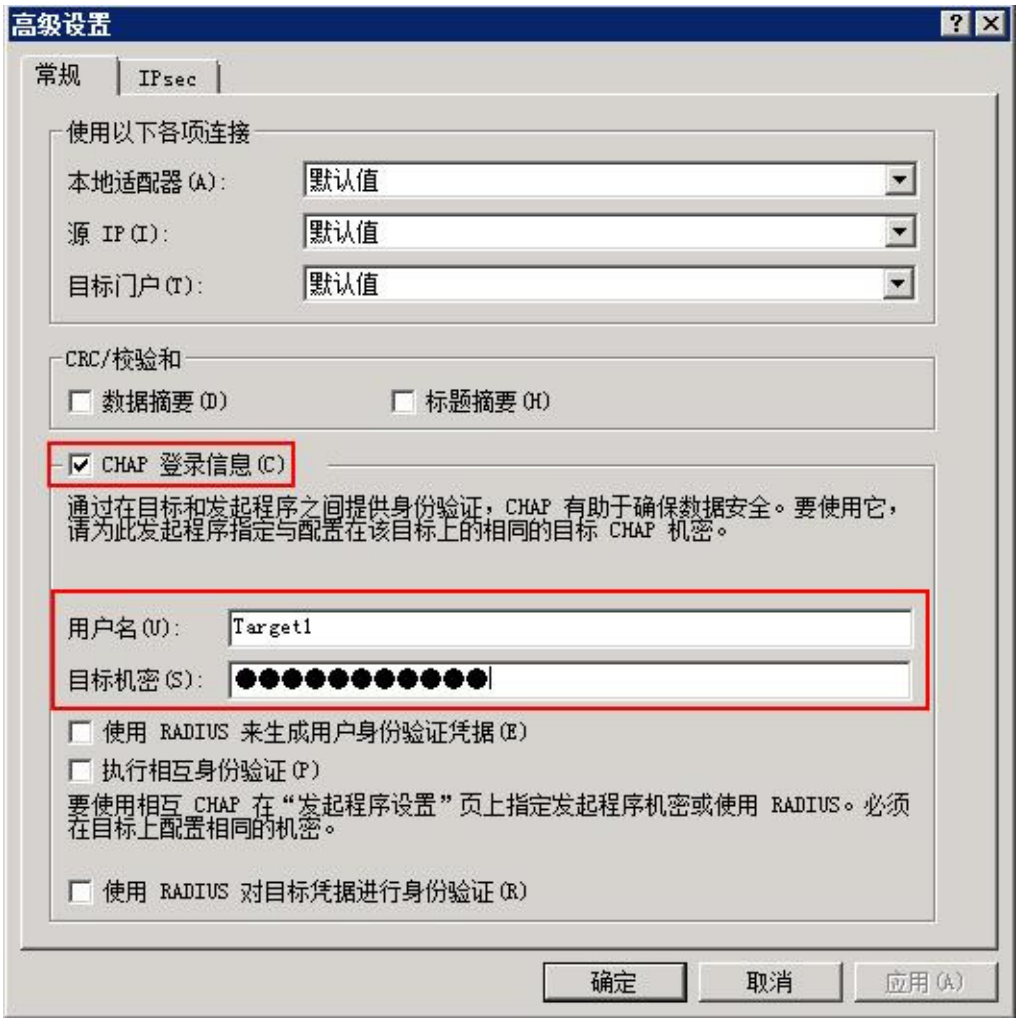
10. 在“iSCSI发起程序”属性界面，选择“目标”，将会发现目标已添加，但状态显示“不活动”，然后单击“登陆”按钮。如图：



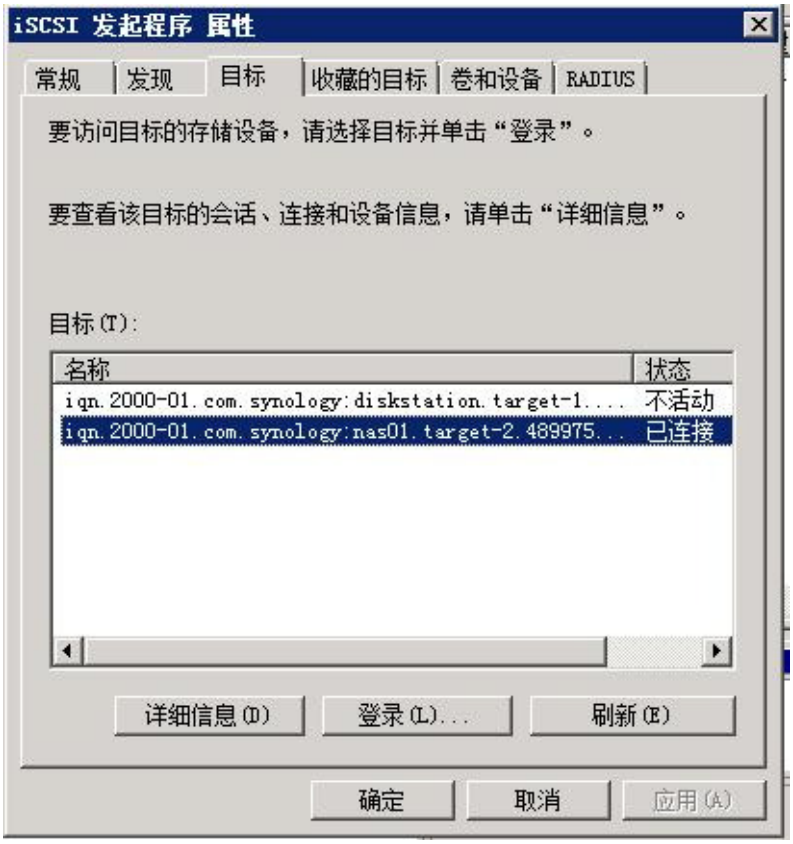



11. 继续单击“高级”按钮，勾选“CHAP登录信息”，填入用户名和密码（见步骤5），然后单击“确定”按钮。

如图：



12. 如果登录验证成功，目标状态将更改为“已连接”，单击“确定”退出。 如图：




13. 打开“计算机管理->磁盘管理”程序，新磁盘映射成功，显示还未分配。 如图：

14. 选择该磁盘并右键单击，创建“新建简单卷”，单击“下一步”直至创建完成。

如图：


共享磁盘并设置保护

15. 选中该磁盘并右键查看“属性”，将该磁盘设置为共享。

16. 打开Curtain管理员，设置该磁盘为受保护网络磁盘。(阅读FAQ 00085)

17. 重新运行Curtain客户端并映射受保护网络磁盘。

备注: 原来NAS共享文件夹权限需要重新在Windows服务器上设置。

## 8.3 - 启动或停止Curtain除错日志

请按以下步骤启动或停止Curtain除错日志:
1. 启动"命令提示符" (于 "开始菜单>程序>附件" 下)
2. 输入"regedit"启动注册表编辑器
3. 选择 \HKEY_LOCAL_MACHINE\SOFTWARE\Coworkshop\Curtain 3
4. 启动或停止Curtain除错日志:
    - 启动日志，设定DebugLog = a

5.重现问题

6.将错误日志文件复制压缩后发送给Curtain技术支援中心。

Vista以上系统除错日志的位置:
- \\installation path\Coworkshop\Curtain 3\cbin\log
- \\Users\username\CurtainLog

Vista以下系统除错日志的位置:
- \\installation path\Coworkshop\Curtain 3\cbin\log
- \\Users\username\CurtainLog

例如：
C:\Program Files\Coworkshop\Curtain 3\CBin\Log
C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\Log （64位操作系统）
C:\Users\tester\CurtainLog

备注：对于64位操作系统，请发送在 "Program Files"和"Program Files (x86)"下日志。

9.操作完成后，请记得停止除错日志：
- 停止日志，设定DebugLog = 0

备注: 请紧记在使用除错日志后将它停止，因为除错日志会占用硬盘不少空间。

## 8.4 - 针对克隆的Curtain客户端生成唯一令牌

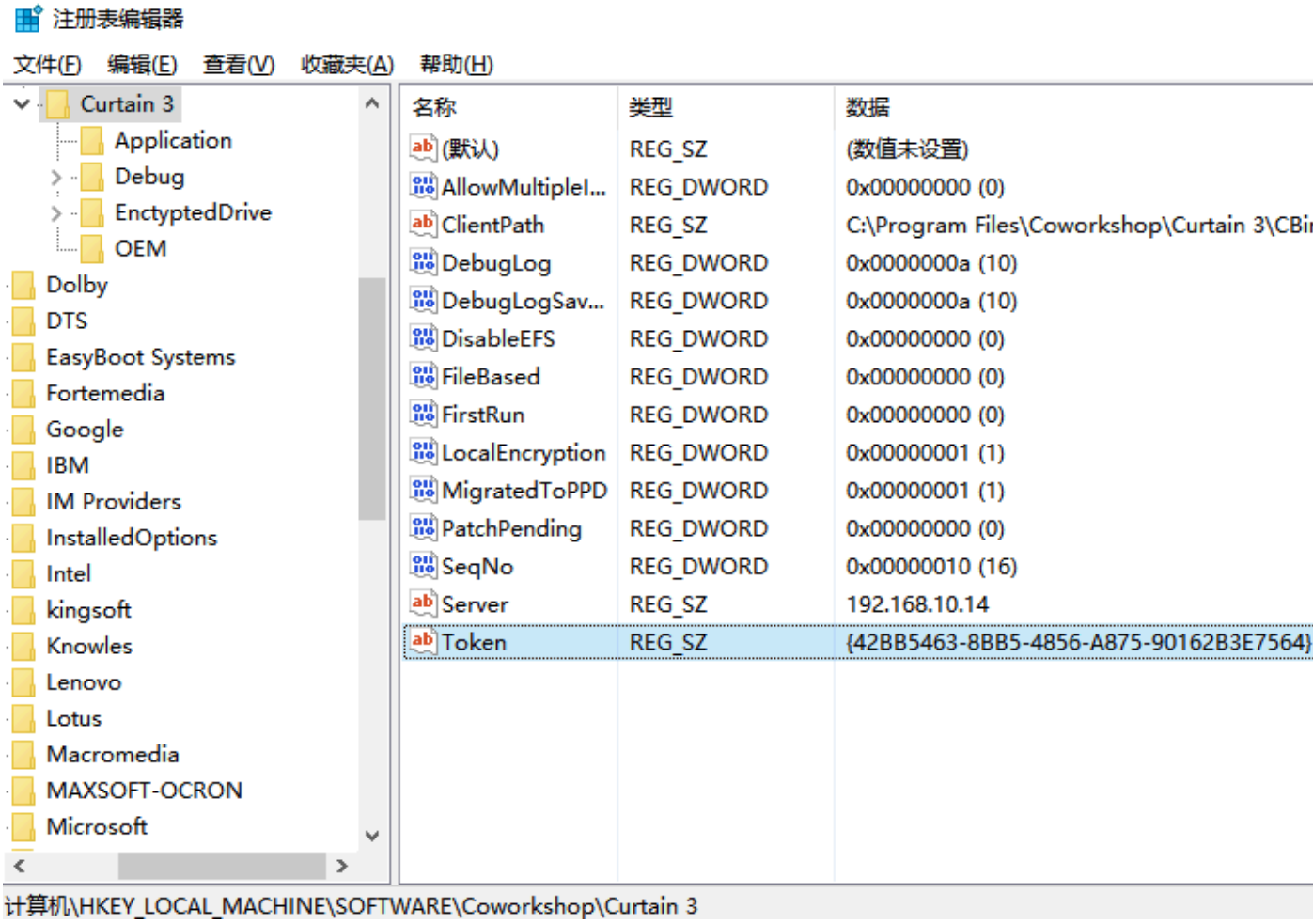
Curtain客户端安装后会生成一个独一无二的令牌（GUID全局唯一标识符），由于克隆的系统会保持令牌不变，故需使用ReGenToken.exe工具重新生成。

请按以下步骤自动生成Token:
1.在安装Curtain客户端的工作站中，双击运行ReGenToken.exe工具。

2.系统会提示 “生成令牌并设置成功” 。

3.请到Curtain客户端和Curtain管理端检查令牌是否被改变。

检查Curtain客户端：




检查Curtain管理端


备注：该工具ReGenToken.exe分为3272版本和3273版本，请根据安装的Curtain客户端版本决定。

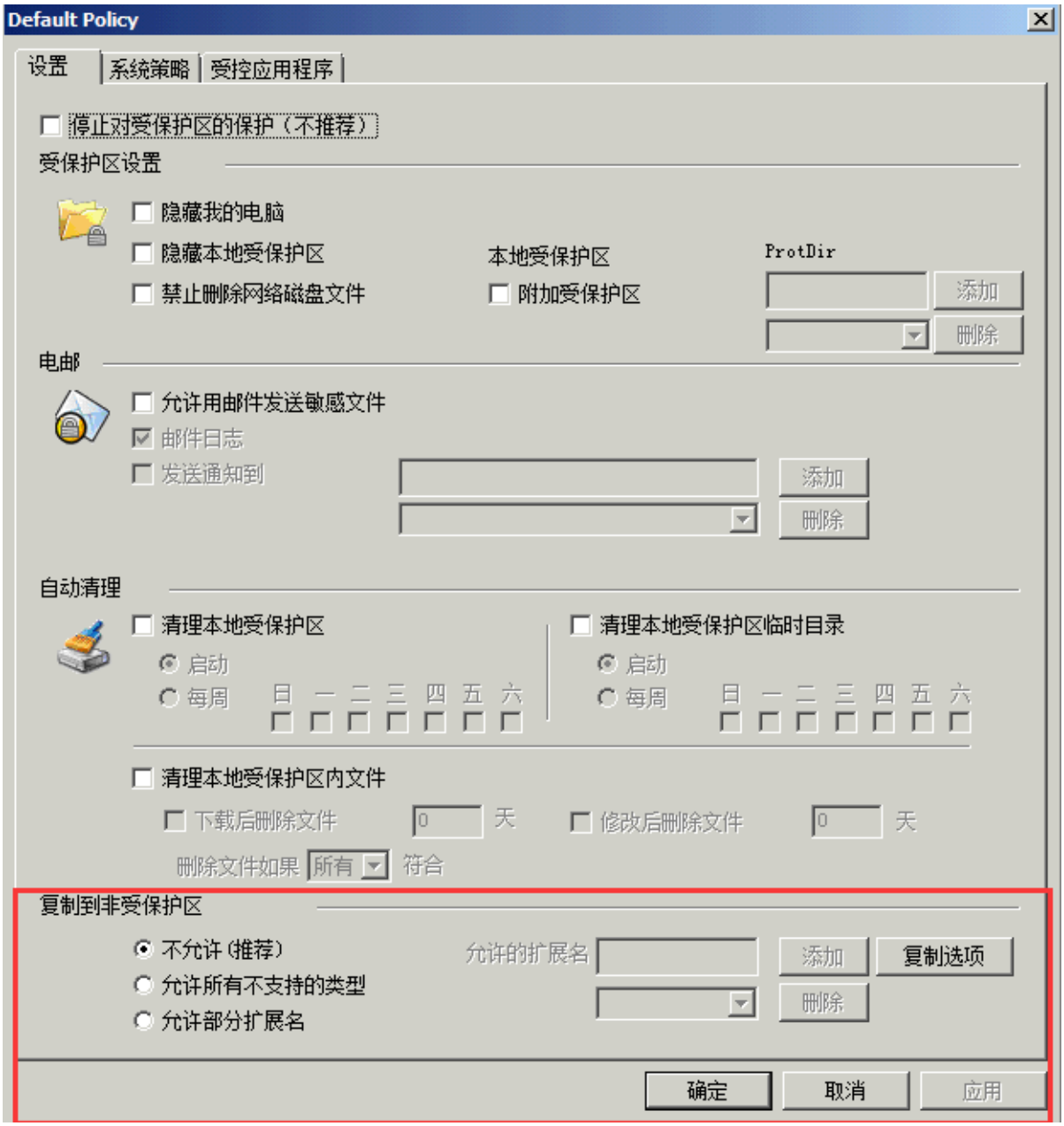
下载链接：
ReGenToken.exe tool
http://www.coworkshop.com/download/ReGenToken.zip

# 9 - 最佳实践

## 9.1 - 允许受保护文件从安全区复制/发送出去

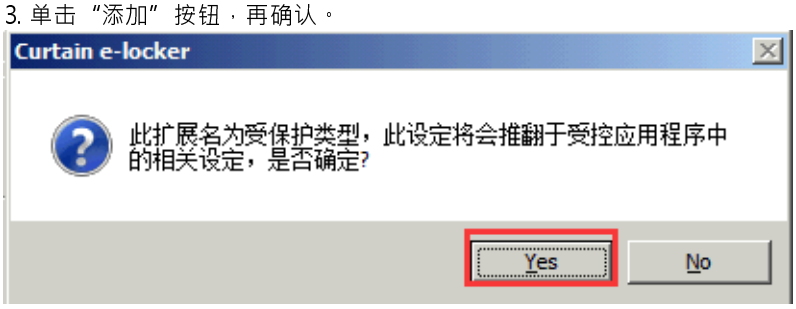
授权用户从安全区复制/发送文件到非受保护区的步骤（以txt文件为例）：

1. 在Curtain管理员，点选一个安全策略，按滑鼠右键，并选择"属性">"复制到非受保护区"。

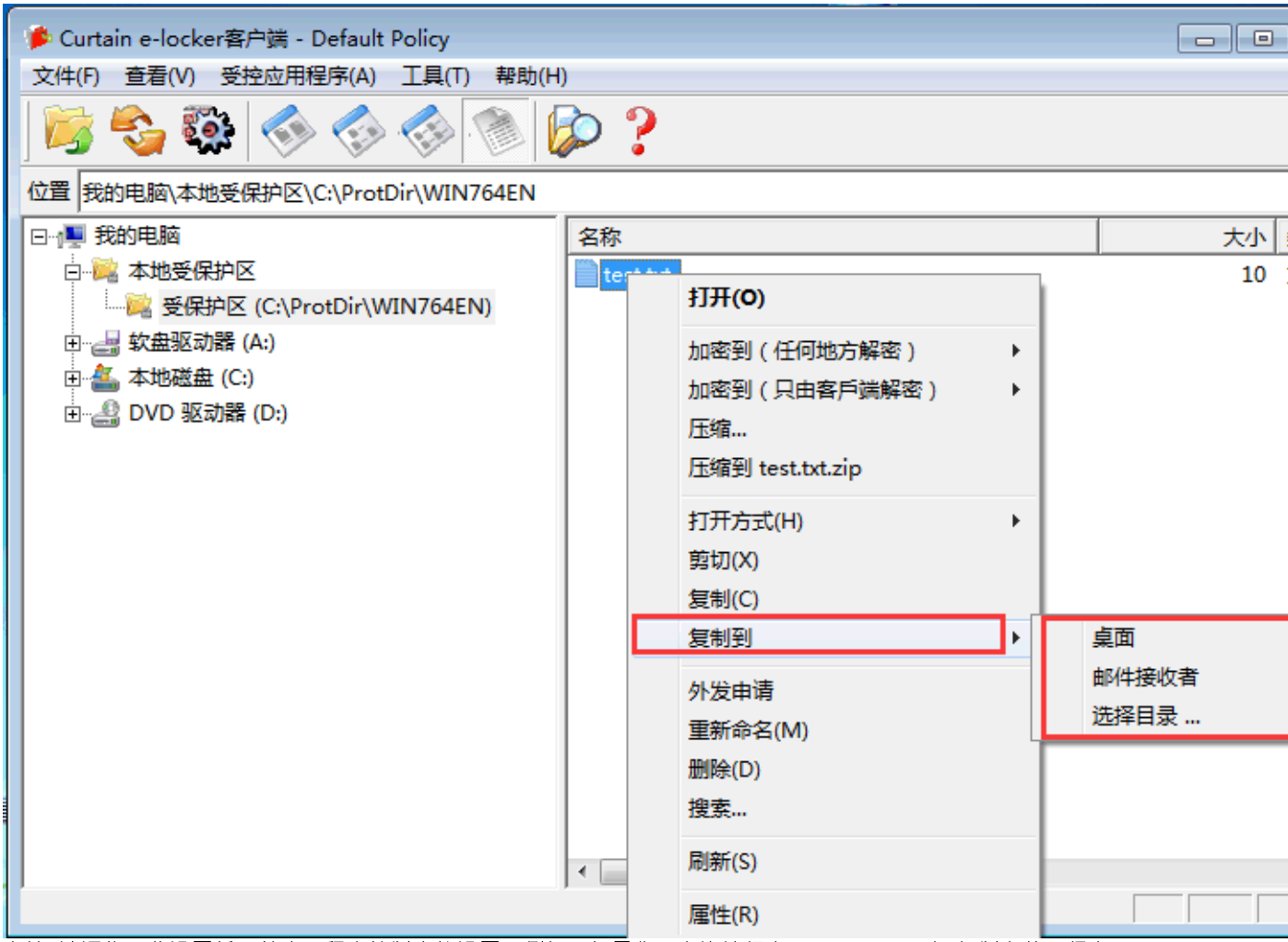


2. 选择“允许部分扩展名”（例如:TXT）。


3. 单击“添加”按钮，再确认。




4. 运行Curtain客户端，在客户端界面右键单击TXT文件 -> 复制到非受保护区。



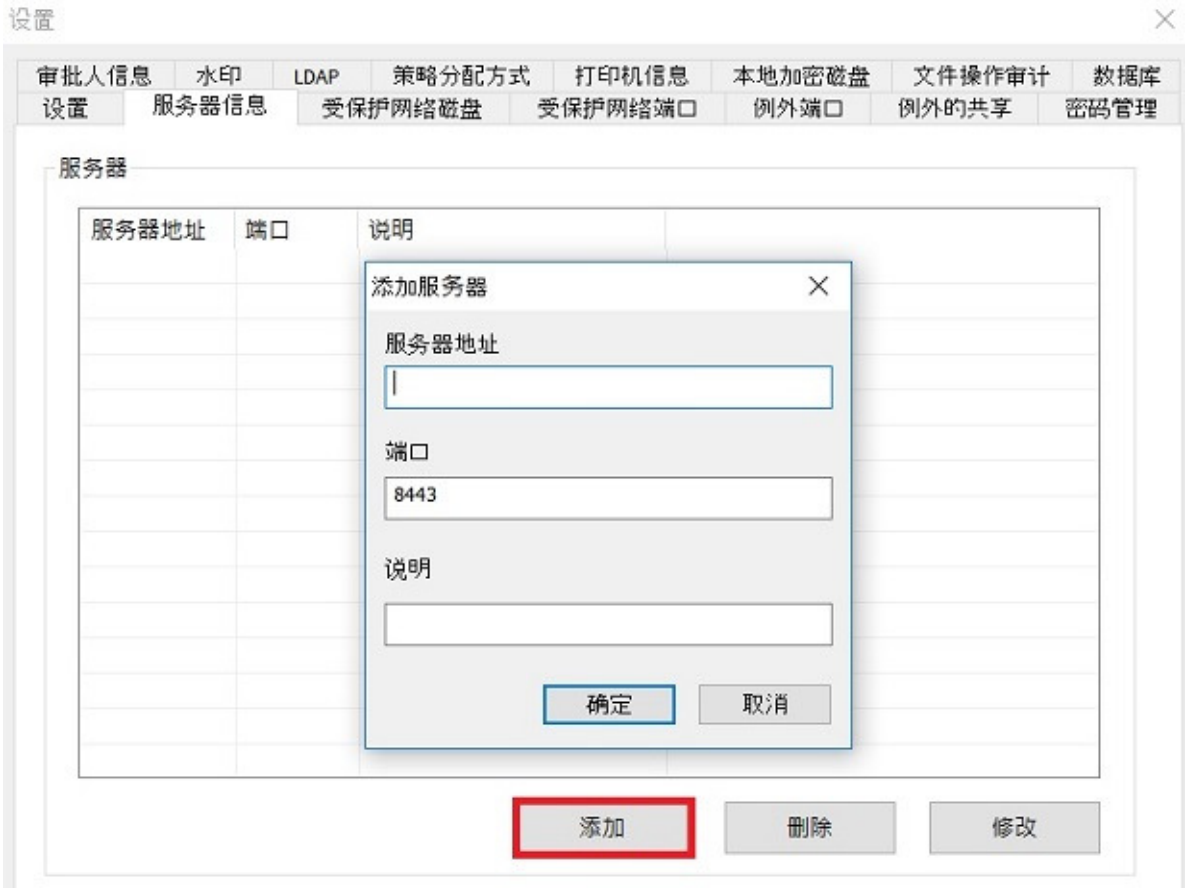

备注: 请记住，此设置将覆盖应用程序控制中的设置。例如，如果您不允许该组在MS Excel中保存/复制文件，但允许复制XLS文件，则后者设置将覆盖前者的设置。

## 9.2 - 如何设置对SolidWorks Enterprise PDM的保护？

对SolidWorks EPDM设置保护的大概步骤：
1. 于Curtain管理员，添加EPDM服务器为受保护区。
2. 于用户计算机，通过受保护的EPDM View Setup把Local File Vault位置设定到本地受保护区下的文件夹。
3. 完成

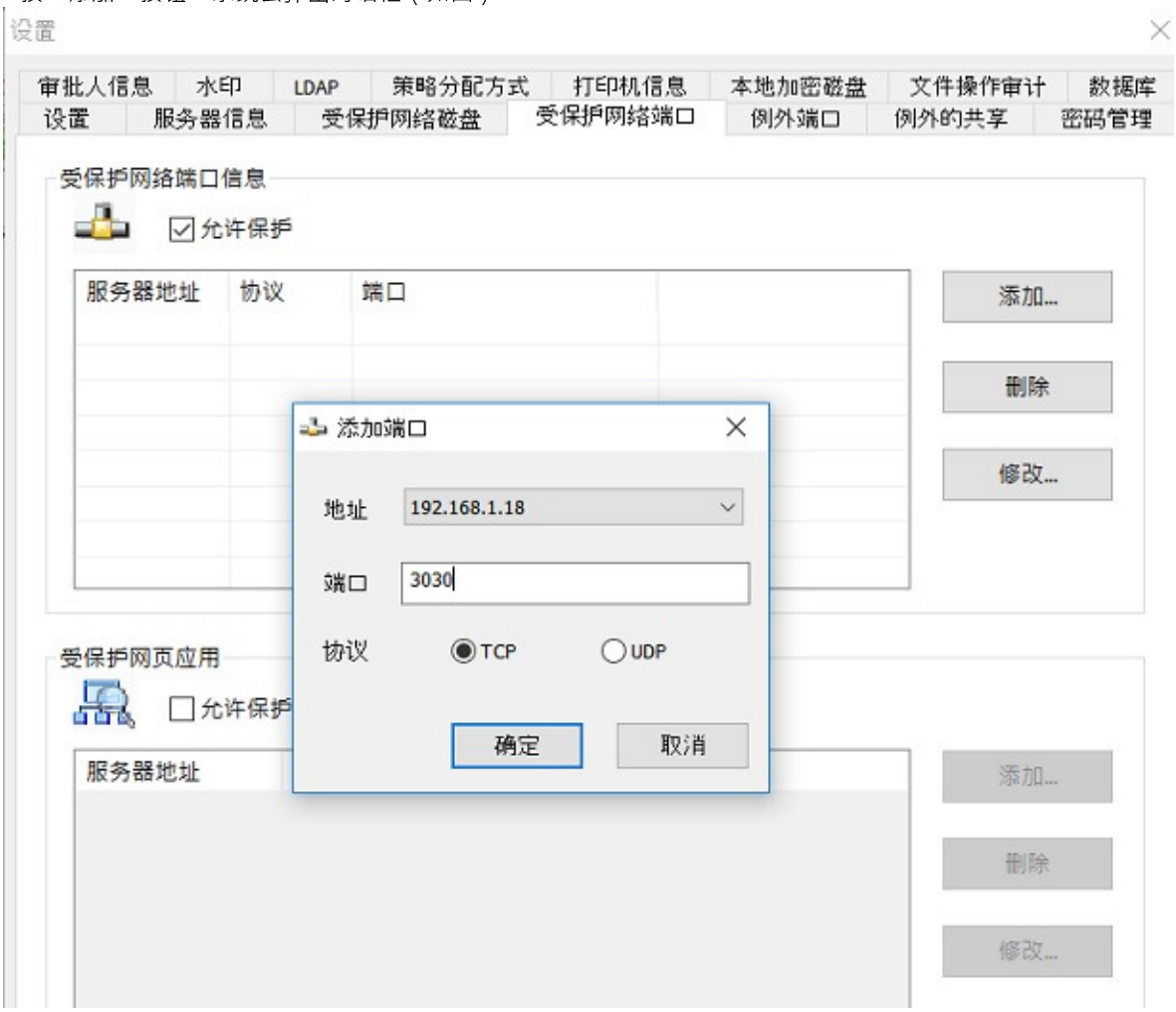
详细设置步骤：
步骤1：在Curtain管理员，添加EPDM服务器为受保护区。
1.1. 在Curtain管理员，于菜单上选择“文件>设置”。

1.2. 在“服务器信息”页，按“添加”按钮来新增EPDM伺服器。
服务器地址：EPDM 伺服器的电脑名称或 IP 位址。
端口：默认的端口是8443（用作Curtain管理员和Curtain服务器插件之间的沟通）。




1.3. 按确定键确认。

1.4. 保护EPDM服务器的网络端口。
- 于“受保护网络端口”，点选“允许保护”。
- 按“添加”按钮，系统会弹出对话框（如图）。




地址 - 选择EPDM服务器（计算机名称或IP地址）
端口 - 输入3030（EPDM的默认值是3030）
协议 - 选择TCP（EPDM的默认协议是TCP）

1.5. 按确定键确认。

步骤2. 于用户计算机，通过受保护的EPDM View Setup把Local File Vault位置设定到本地受保护区下的文件夹。
- 如果你的计算机会跟其他EPDM用户共同使用，你需要使用附加安全区，因为用户甲不能访问用户乙的本地受保护区。请继续按步骤2.1。
- 如果你的电脑不会有多个用户共同使用EPDM，请跳到步骤2.4继续。

2.1. 在Curtain管理员，点选一个安全策略，按鼠标右键，并选择“属性”。

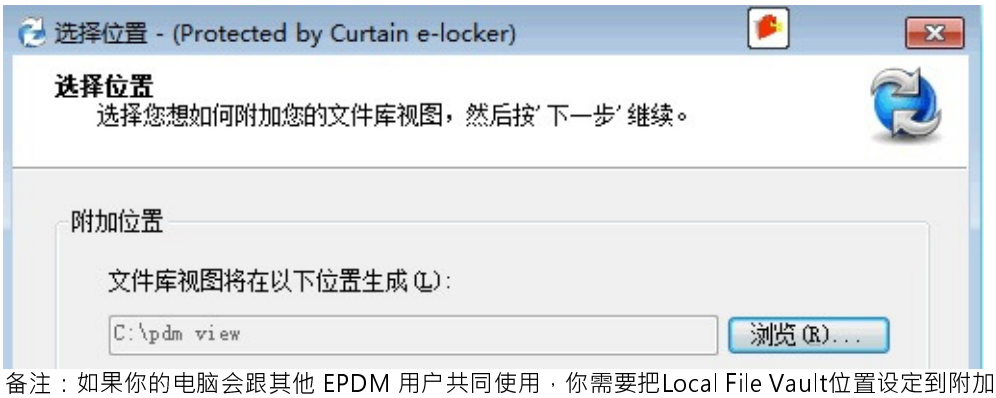
2.2. 于“设置”页:
- 选择“附加受保护区”，并输入路径。
- 按“添加”按钮确定。


2.3. Curtain管理员添加完成以后，客户端在下次启动，附加保护区就会显示在客户端内，如下图所示：


2.4. 于“开始”菜单，选择“所有程序 > Coworkshop Curtain e-locker > Secure Applications”。


2.5. 开启Secure EPDM View Setup。

2.6. 把Local File Vault位置设定到本地受保护区下的文件夹。

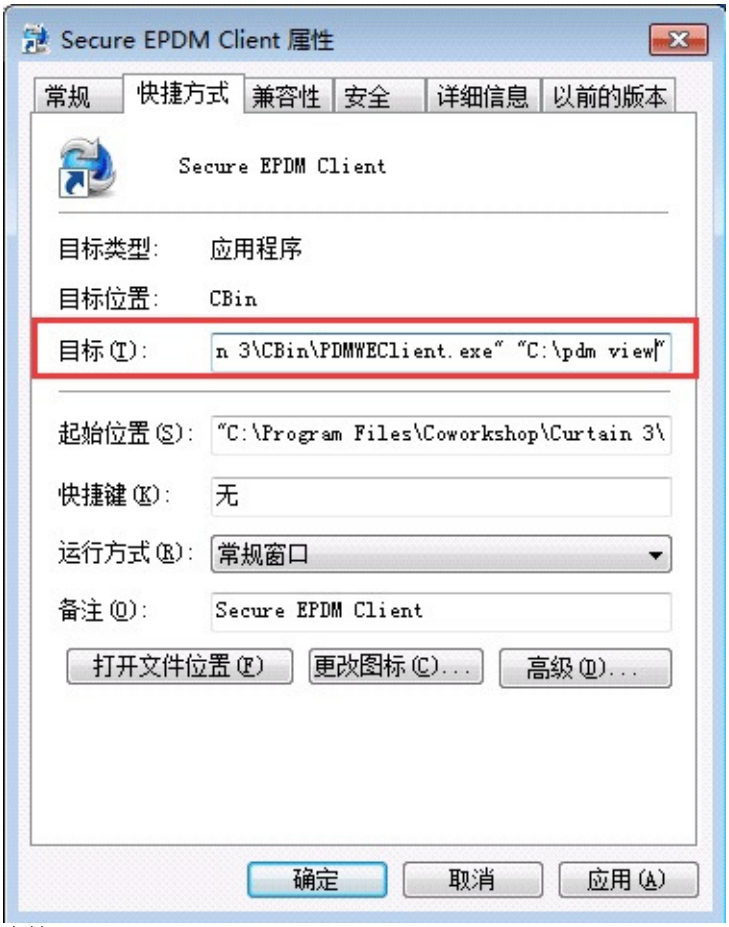



备注：如果你的电脑会跟其他 EPDM 用户共同使用，你需要把Local File Vault位置设定到附加安全区。

2.7. 于“开始”菜单，选择“所有程序 > Coworkshop Curtain e-locker > Secure Applications”。

2.8. 右键点选Secure EPDM Client快捷方式，选择“属性”。


2.9. 在目标栏中添加Local File Vault的路径。




备注：
- 请确保你已经用 Secure EPDM View Setup 把此路径设定为 Local File Vault。

2.10. 通过Secure EPDM Client来使用EPDM系统。