



Curtain™ e-locker(易鎖) 5.0

安裝說明書

若對產品或本說明書有任何疑問或查詢，歡迎聯絡我們的代理商或服務提供商。

若需要其他協助，請發電子郵件至：info@coworkshop.com。

本說明書的內容如有更改，恕不另行通知。關於使用 Curtain e-locker(易鎖)的一切條文及細則，請參閱軟件授權協議 (Curtain e-locker Software License Agreement)。

本說明書及 Curtain e-locker(易鎖)的所有版權均屬於雁飛科技有限公司 (Coworkshop Solutions Ltd.) 所有。未經雁飛科技有限公司書面許可，任何人均不得為任何目的，以任何形式或方法，複製或轉譯本說明書的任何部分。

本說明書內所提到的其他產品或商標，均屬於相關公司所擁有。

目錄

Chapter 1 - 前言

1.1 - 資料外洩的威脅	1
1.2 - Curtain e-locker(易鎖)的設計目的	1
1.3 - Backend systems(如:Windows 文件服務器)亦有權限控制，為什麼需要 Curtain e-locker?	1
1.4 - 我們公司已經禁止使用 USB 接口和互聯網，為什麼還需要 Curtain e-locker?	2
1.5 - 關於 Curtain e-locker	2
1.5.1 - Curtain e-locker 的基本控制	2
1.5.2 - Curtain e-locker 的基本結構	2
1.5.3 - Curtain e-locker 的基本組件	3
1.5.4 - Curtain 受保護區的概念	4

Chapter 2 - 安裝前的準備

2.1 - Curtain e-locker 的實施計劃	6
2.2 - 系統軟硬體的要求	6
2.2.1 - Curtain 服務器插件和 Curtain 管理員對系統軟硬體的要求	6
2.2.2 - Curtain 客戶端對系統軟硬體的要求	6
2.3 - Curtain 的基本權限控制	7
2.4 - 給 Curtain e-locker 開放端口	9
2.4.1 - 給 Curtain 管理員和服務器插件開放端口 24821 和 24822	9
2.4.2 - 給 Curtain 客戶端開放端口 24821 和 24822	16
2.4.3 - 於 Curtain 服務器插件上檢查 Tomcat 8005 端口是否已被佔用	24
2.4.4 - 為 Curtain 服務器插件更改 Tomcat 8005 端口	25

Chapter 3 - 安裝

3.1 - 安裝 Curtain 管理員	26
3.2 - 安裝 Curtain 服務器插件	29
3.3 - 安裝 Curtain 客戶端	31

Chapter 4 - 產品激活

4.1 - 產品激活	35
4.2 - 激活 Curtain e-locker	35

Chapter 5 - 設置

5.1 - 新增安全策略群組	39
5.2 - 修改安全策略群組的設定	39
5.3 - 設定默認策略	43
5.4 - 按用戶/用戶群組來配置安全策略	43
5.5 - 指派電腦/用戶到合適的安全策略	47
5.6 - 設定服務器上的受保護區	49
5.7 - 保護共享文件夾下的子文件夾	55
5.8 - 例外規則	59
5.8.1 - 例外規則	59
5.8.2 - 設置例外規則	61
5.9 - 暫時停止受保護區的保護	65
Chapter 6 - 其他功能	
6.1 - 保護文件初稿	66
6.2 - 在線/離線保護	67
6.3 - 自動清理	68
6.4 - 截屏控制	69
6.5 - 智能複製粘貼控制	69
6.6 - 安全生成 PDF 文檔	70
6.7 - 與其他人分享受保護文件	71
6.8 - 活動記錄	75
6.9 - 外發申請	77
6.10 - 附加水印	83
6.11 - 記錄打印內容	87
6.12 - 為受控應用程序創建快捷方式	88
6.13 - 本地加密磁盤	90
6.14 - 為 Curtain 管理端、服務器插件和客戶端設定登入密碼	104
6.15 - 為 Curtain 管理端、服務器插件和客戶端更改或重設登入密碼	106
Chapter 7 - 後續維護	
7.1 - 補丁的管理	108
7.2 - 管理員遷移到另一台電腦上	109
7.3 - 手動備份與恢復 Curtain 管理員的安全策略和活動記錄	111
7.4 - 自動備份 Curtain 管理員的安全策略	111
Chapter 8 - 常見問題	
8.1 - 如何避免和殺軟沖突？	114
8.2 - 使用易鎖通過 iSCSI 來保護 NAS	114
8.3 - 啟動或停止 Curtain 除錯日志	126

8.4 - 針對克隆的 Curtain 客戶端生成唯一令牌 126

Chapter 9 - 最佳實踐

9.1 - 允許受保護文件從安全區復制/發送出去 128

9.2 - 如何設置對 SolidWorks Enterprise PDM 的保護？ 130

1 - 前言

1.1 - 資料外洩的威脅

在每天的工作中，有些敏感資料又必需要給員工去用(如:業務會接觸到客戶資料;工程師會接觸到圖檔等)，但公司又很困難去控制員工如何使用這些敏感資料。當員工有權去使用這些資料時(如:讀取、修改等)，就如同可以擁有它，員工可以很容易通過不同渠道將資料帶走(如:打印、移動硬盤、Internet、電郵、甚至截屏等)。對公司來說，可以全面控制敏感資料的使用，是十分困難的。

1.2 - Curtain e-locker(易鎖)的設計目的

Curtain e-locker(易鎖)是一套完善的防止資料外洩解決方案，它可以有效防止不授權員工用任何渠道將資料帶走。實施Curtain e-locker後，公司可以容許授權員工正常使用敏感資料，同時，公司可以完全防止員工在使用資料時將資料帶走。

1.3 - Backend systems(如:Windows文件服務器)亦有權限控制，為什麼需要Curtain e-locker?

是的，backend systems也有權限控制，但是，backend systems只可以控制"讀取"、"修改"、"刪除"等權限。如果管理員容許用戶訪問服務器資料(如:共享文件夾)，backend systems就不能阻止用戶將文檔保存至本地磁盤、USB硬碟或透過電郵將文檔外發，這方面正正是Curtain e-locker的功用，因此，Curtain e-locker並不是取代backend systems，而是與backend systems緊密合作。當一個用戶授權使用服務器上的資源時，管理員可以使用Curtain e-locker來防止資料外洩。

舉例: 下圖是Windows文件夾的權限設定，圖中可見，它並沒有"打印"或"保存"等控制。



1.4 - 我們公司已經禁止使用USB接口和互聯網，為什麼還需要Curtain e-locker?

是的，禁止使用USB接口和互聯網是可以減低資料外洩的風險。但是，還有很多渠道可以將資料帶走。例如：

- 打印
- 截屏、截屏軟件
- 複製粘貼
- 電郵
- Wi-Fi、藍芽 (用手機作為熱點)
- Skype, Whatsapp, QQ
- 更多...

有些公司嘗試把所有接口或渠道堵住，但是對管理員來說，這是十分困難去實施和維護形形色色不同的控制。而且，在現今資訊發達的社會，不容許員工在工作時使用電郵、Skype、USB等工具是十分不方便。Curtain e-locker既不影響正常操作，亦可以確保資料的安全，Curtain e-locker在方便性和資料保安之間取得很好的平衡。

1.5 - 關於Curtain e-locker

1.5.1 - Curtain e-locker的基本控制

Curtain e-locker可以控制：

- 存儲到任何地方
- 發送
- 列印
- 列印螢幕
- 複製內容到任何地方
- 複製文檔到任何地方

Curtain e-locker只控制受保護區內的文檔，員工可以如常使用受保護區內的文檔，只是一切非授權的功能都會被Curtain e-locker堵住。比如：如果用戶不容許存儲受控文檔到別的地方或打印受控文檔，這些功能都會被Curtain堵住，但用戶依然可以使用電郵、USB移動硬盤或互聯網，只時受保護區內的文檔受到Curtain的控制。

系統管理員可以針對不同用戶或電腦來設定不同的安全策略群組，請參考相關文件。

1.5.2 - Curtain e-locker的基本結構

員工在日常工作中，很多時需要接觸到一些機密資料(如：銷售人員會接觸到客戶資料、工程師需要接觸圖檔等等)。當他們授權訪問Windows文件服務器上的共享文件夾時，公司是十分困難防止他們將這些機密資料帶走。

實施Curtain e-locker後，管理員可以設定那些服務器上的共享文件夾需要Curtain的保護。如果員工需要使用這些受保護資料，他們的電腦必需要安裝了Curtain客戶端，在安裝Curtain客戶端時，系統會自動在員工電腦上建立一個安全文件夾(稱為本地受保護區)。

管理員於Curtain管理端上建立及設定不同的安全策略群組，設定後指派用戶電腦到不同的群組當中。Curtain e-locker有一個獨有的設計，稱為受保護區(受保護區是由服務器上的受保護資料和客戶端上的本地受保護區組成的)，員工可以在受保護區內如常使用機密資料(如：讀取、修改等)，但是在沒有授權情況下就不能將資料帶到受保護區之外。同時，員工依然可以使用互聯網、電郵等設備。



結構



1.5.3 - Curtain e-locker的基本組件

Curtain e-locker有三個基本的組件:

- Curtain客戶端
- Curtain管理員(我們亦會把安裝了Curtain管理員的電腦稱呼為Curtain安全策略服務器)
- Curtain服務器插件

Curtain客戶端:

當用戶使用服務器上的受保護資料時(如:文件服務器上的受保護共享文件夾、受保護網站等)，用戶的電腦必需要已經安裝了Curtain客戶端。在安裝Curtain客戶端時，系統會自動建立一個安全的文件夾(那就是Curtain本地受保護區)。

Curtain管理員:

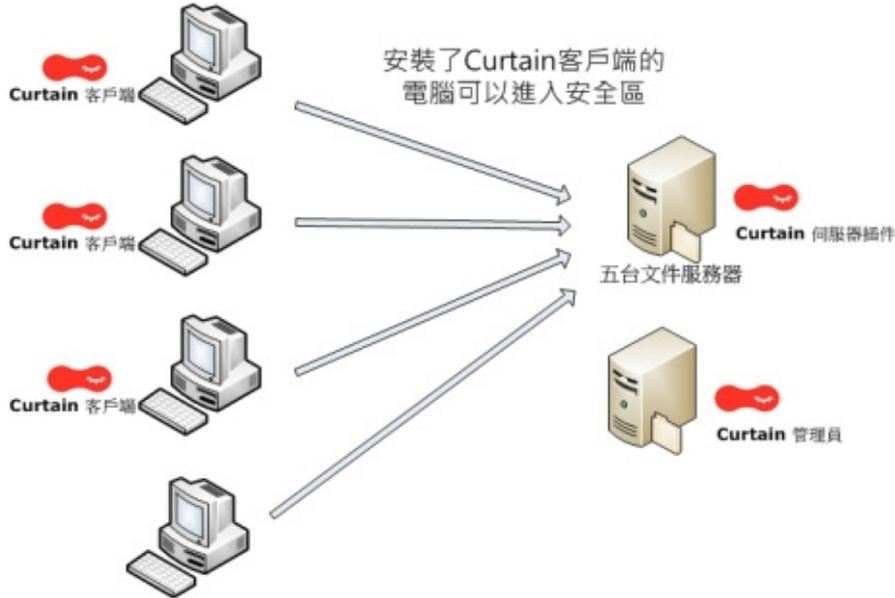
系統管理員可以用Curtain管理員來集中地為所有Curtain客戶端設定安全策略。同時，Curtain客戶端會儲存用戶活動記錄以供授權人員查閱。一般而言，一家公司只需要安裝一台Curtain管理員。

Curtain服務器插件:

Curtain服務器插件需要安裝在所有需要Curtain e-locker保護的服務器上。Curtain服務器插件會定時與Curtain管理員溝通，用最新的安全策略來保護服務器上的資料。

舉例:這家公司想用Curtain e-locker來保護它們五台服務器上的共享文件夾，那麼他們需要於這五台服務器上都安裝Curtain服務器插件。

以下是Curtain e-locker基本的架構:



沒有安裝Curtain客戶端的電腦只可以使用非機密資料

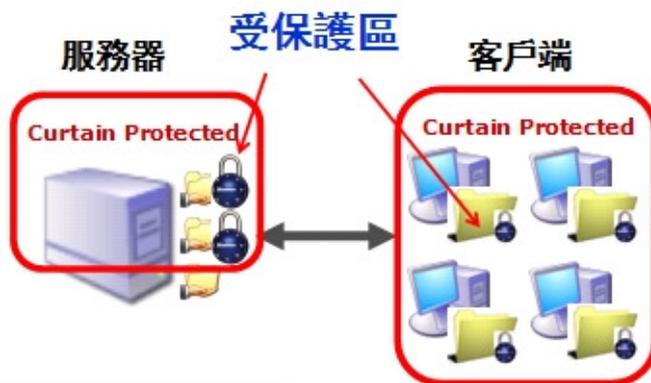
備註:

- Curtain管理員可以安裝在一台獨立的服務器上或是安裝在其中一台文件服務器上。
- 系統管理員可以通過"例外"這個功能來容許沒有安裝Curtain客戶端的電腦訪問受保護的服務器資源。

1.5.4 - Curtain受保護區的概念

受保護區是由(1)服務器上的受保護資料和(2)客戶端上的本地受保護區組成的。服務器上的受保護資料可以是文件服務器上的共享文件夾、SharePoint、ERP、自行開發的系統等。而在用戶電腦上，本地受保護區會在安裝Curtain客戶端時自動生成，文件夾名稱是"ProtDir"，它會被建立於所有本地的硬盤上。

受保護區:



客戶端上的本地受保護區:



以上例子，本地硬盤上有兩個分區(C和D)，所以"ProtDir"會建立於C和D這兩個分區之下。而且，本地受保護區是個人化的，即使在同一台電腦上，用戶也不能訪問另一位用戶的本地受保護區。

備註:

- 於安全策略群組，有一個"隱藏本地受保護區"的設定，管理員可以透過啟動這功能，來達到強制用戶直接使用文件服務器上受控文檔的效果。
- 軟件有一個"本地加密磁盤"的功能，管理員可以透過這功能來加密本地受保護區，來提升資料安全性。
- 如有需要，管理員可以添加"附加本地受保護區"。

2 - 安裝前的準備

2.1 - Curtain e-locker的實施計劃

安裝前的準備:

- 那些服務器上的資料需要受Curtain e-locker保護(如:文件服務器上的共享文件夾、SharePoint、ERP、自行開發的系統等)?
- 那些用戶需要使用這些受保護的資料?
- 公司想如何控制用戶使用這些受保護的資料(如:禁止保存到受保護區以外)?
- 那台服務器會安裝Curtain管理員?
- 是否想將Curtain e-locker與Active Directory整合(以便使用AD用戶/用戶群組來配置安全策略)?
- 是否想將用戶電腦上的本地受保護區加密?

實施次序:

1. 安裝Curtain管理員
2. 在所有需要Curtain e-locker保護的服務器上安裝Curtain服務器插件
3. 在用戶的電腦上安裝Curtain客戶端
4. 激活Curtain e-locker
5. 於Curtain管理員上建立及設定安全策略群組
6. 從Active Directory導入用戶資料(如果需要按AD用戶/用戶群組來配置安全策略)
7. 指派電腦/用戶到不同的安全策略群組
8. 設定服務器上的受保護區(那些服務器上的資料需要保護)
9. 完成

備註: 不應該將Curtain服務器插件和Curtain客戶端安裝在同一台電腦上。

2.2 - 系統軟硬體的要求

2.2.1 - Curtain服務器插件和Curtain管理員對系統軟硬體的要求

Curtain服務器插件和Curtain管理員對系統軟硬體的要求:

- Intel Pentium或更好的處理器
- Windows XP、服務器2003、2008、2012、2012R2、2016、Vista、Win 7、Win 8、Win 8.1或Win 10操作系統
- 128MB記憶體 (建議256MB記憶體)
- 200MB硬碟空間 (NTFS格式)
- TCP/IP網路協定
- TCP通信埠8443 (默認開放)
- TCP通信埠24821與24822必需開放 (注意: 如果網路存在防火牆, 請確認這兩個通信埠未被遮罩)
- 對於64位元操作系統, MSXML 4或6是必需的 (在微軟官方網站上可以下載到)

2.2.2 - Curtain客戶端對系統軟硬體的要求

Curtain客戶端對系統軟硬體的要求:

- Intel Pentium或更好的處理器
- Windows XP、服務器2003、2008、2012、2012R2、2016、Vista、Win 7、Win 8、Win 8.1或Win 10操作系統
- 128MB記憶體 (建議256MB記憶體)
- 200MB硬碟空間 (NTFS格式)
- TCP/IP網路協定
- TCP通信埠24821與24822必需開放 (注意: 如果網路存在防火牆, 請確認這兩個通信埠未被遮罩)
- 對於64位元操作系統, MSXML 4或6是必需的 (在微軟官方網站上可以下載到)

2.3 - Curtain的基本權限控制

Curtain的基本權限控制可以針對個別安全策略群組和應用軟件來設置的，以下是默認的權限控制。



"強制儲存到受保護區內" - 此選項被選取時，用戶不能於應用軟件中(如:Word)將受控文檔保存到受保護區之外。

"禁止複製出去" - 此選項被選取時，用戶不能於Curtain客戶端中將受控文檔複製到受保護區之外。"

"禁止列印" - 此選項被選取時，於應用軟件中所有有關打印的功能都會被禁止。

"附加水印" - 此選項被選取時，打印出來的文件上會加上水印(詳細資料請參考相關文檔)。

"記錄打印內容" - 此選項被選取時，系統會為打印出來的文件拍快照，快照會儲存在Curtain管理員的活動記錄內(詳細資料請參考相關文檔)。

"禁止列印屏幕" - 此選項被選取時，當用戶使用截屏鍵或截屏軟件時，顯示敏感資料的窗口都會變成灰色。

"禁止剪貼板" - 此選項被選取時，將文檔內容複製粘貼到受保護區之外都會被禁止(如:複製粘貼內容到Gmail)。

"禁止傳送(如:電郵、互聯網等)" - 此選項被選取時，於應用軟件中所有有關發送的功能都會被禁止。

設置Curtain權限控制的例子

情況1 - 針對MS Word，啟動"強制儲存到受保護區內":

- 當用戶嘗試於MS Word內通過選擇"文件>另存"將受控文檔保存到受保護區之外時，Curtain e-locker會禁止有關操作並提示用戶。



情況2 - 針對MS Word，停用"禁止複製出去":

- 於Curtain客戶端，點選一個Word文檔，按滑鼠右鍵，你可以於子菜單中看見"複製到"選項。你可以使用此功能將文檔複製到受保護區之外。

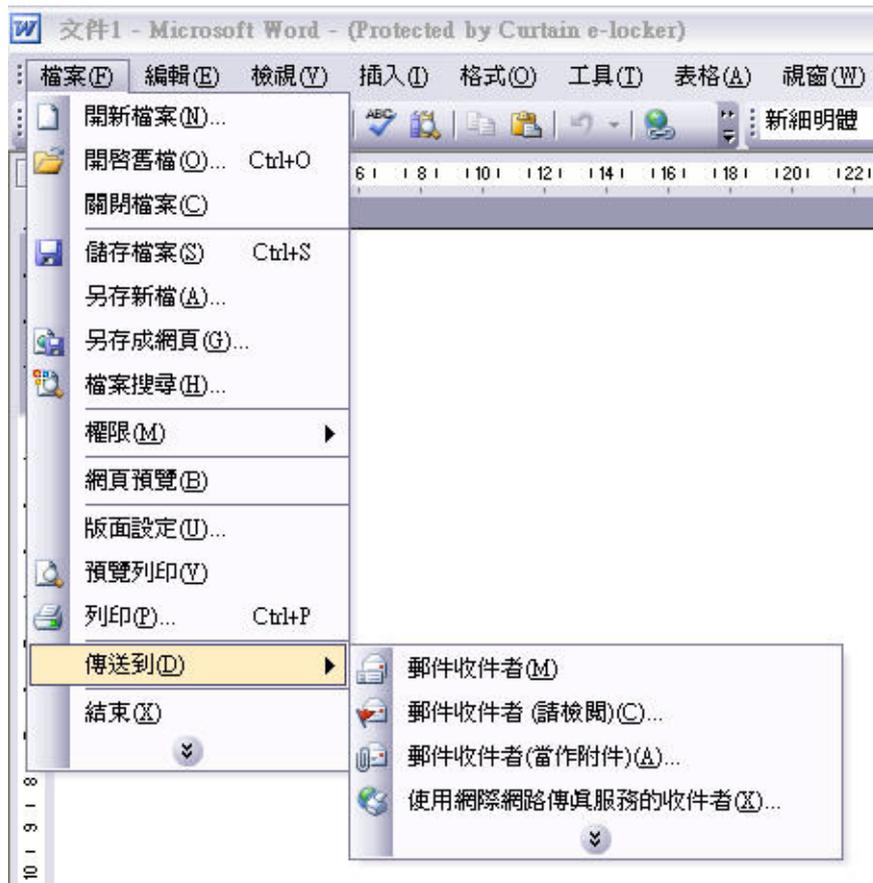
文檔被複製到受保護區之外後:

- Curtain e-locker再不會控制此文檔。

- Curtain e-locker會將此"移出複製"操作記錄在活動記錄中。



情況3 - 針對MS Word，啟動"禁止傳送(如:電郵、互聯網等)":
 - 當用戶嘗試於MS Word內通過選擇"檔案>傳送到"將受控文檔以電郵方式傳送到受保護區之外時，Curtain e-locker會禁止有關操作並提示用戶。



2.4 - 給Curtain e-locker開放端口

2.4.1 - 給Curtain管理員和服務器插件開放端口24821和24822

如果啟用了Windows防火牆，請給Curtain管理員和服務器插件開放端口24821和24822。

於Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10操作系統下，添加以下規則：

- 24821的TCP的入站規則
- 24821的UDP的入站規則
- 24822的TCP的出站規則
- 24822的UDP的出站規則

於Windows 2003和XP，把以下端口設定為例外：

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

於Windows 2008/2012/Vista/Win 7/Win 8/Win10操作系統下，添加規則的步驟：

舉例設置24821的TCP的入站規則

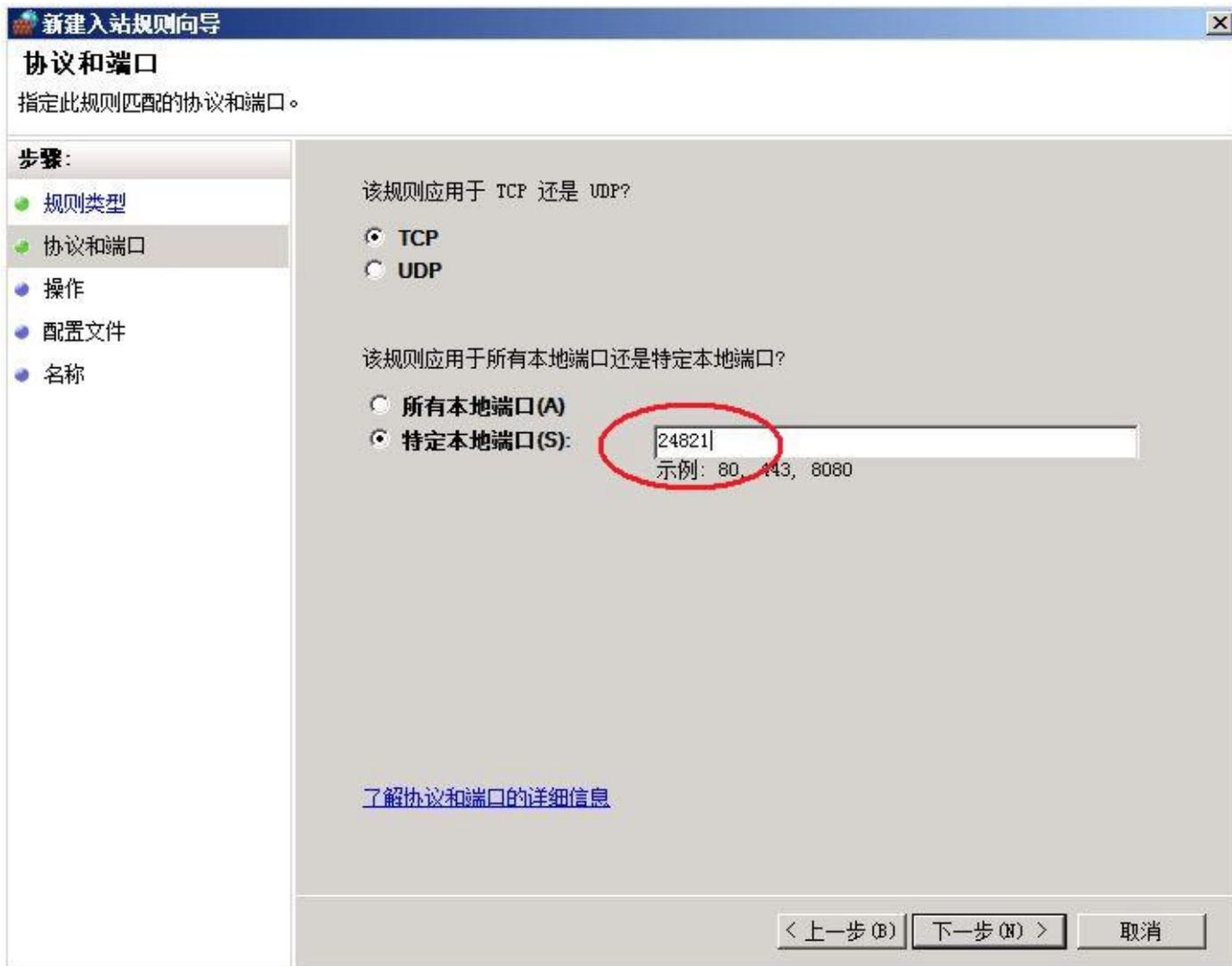
1. 右鍵選擇【我的電腦】>【管理】，彈出"服務器管理器"界面，選擇"配置>高級安全Windows防火牆>入站規則"，右鍵選擇"入站規則"，選擇"新規則"。



2. 彈出"新建入站規則向導"，如下圖所示，選擇"端口"，點擊【下一步】。



3. 在"特定本地端口"內輸入 "24821"，點擊【下一步】。



4. 選擇"允許連接"，點擊【下一步】。



5. 如圖所示默認勾選上"域"，"專用"，"公用"，點擊【下一步】。



6. 在名稱內輸入"Curtain"，點擊【完成】。

新建入站规则向导

名称
指定此规则的名称和描述。

步骤:

- 规则类型
- 协议和端口
- 操作
- 配置文件
- **名称**

名称 (N):
Curtain

描述 (可选) (D):

< 上一步 (B) 完成 (F) 取消

7. 查看右方入站規則的列表，在列表中會多出一項"Curtain"，如下圖所示，添加例外端口操作成功。



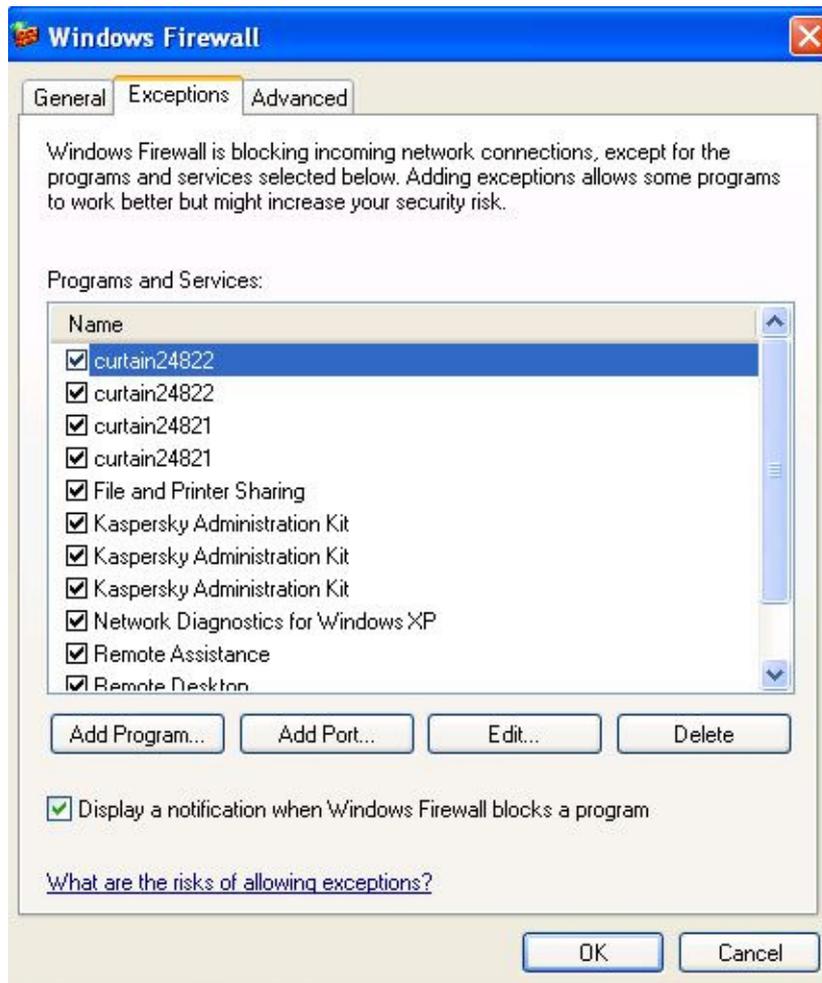
同理，按上面步驟設置 24821的UDP的入站規則，24822的TCP的出站規則，24822的UDP的出站規則即可。

備註：

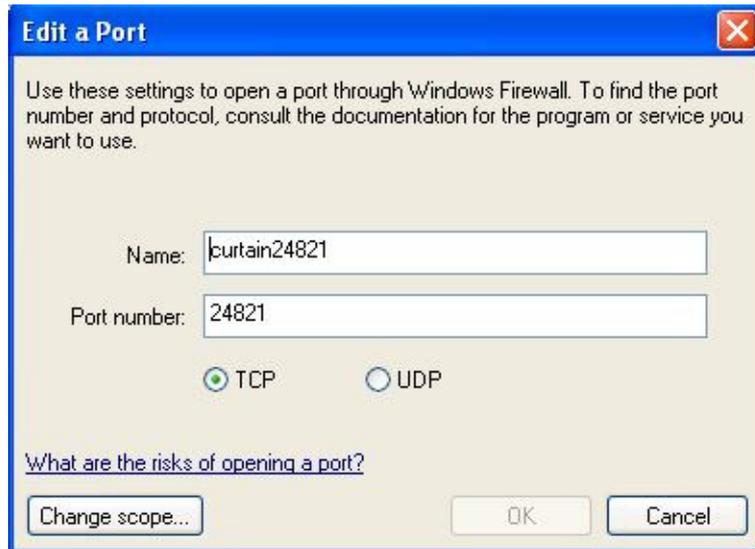
- 設置出站規則時，右鍵選擇"出站規則"，選擇"新規則"。

於Windows 2003和XP，設置例外端口的步驟

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



2. 給此例外輸入名稱、端口為TCP的24821，並按OK確定。



同理，按上面步驟設置UDP的24821，TCP的24822，UDP的24822即可。

2.4.2 - 給Curtain客戶端開放端口24821和24822

如果啟用了Windows防火牆，請給Curtain客戶端開放端口24821和24822。

於Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10操作系統下，添加以下規則：

1. 24822的TCP的入站規則
2. 24822的UDP的入站規則
3. 24821的TCP的出站規則
4. 24821的UDP的出站規則

於Windows 2003和XP，把以下端口設定為例外：

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

於Windows 2008/2012/2016/Vista/Win 7/Win 8/Win10操作系統下，添加規則的步驟：

舉例設置24822的TCP的入站規則

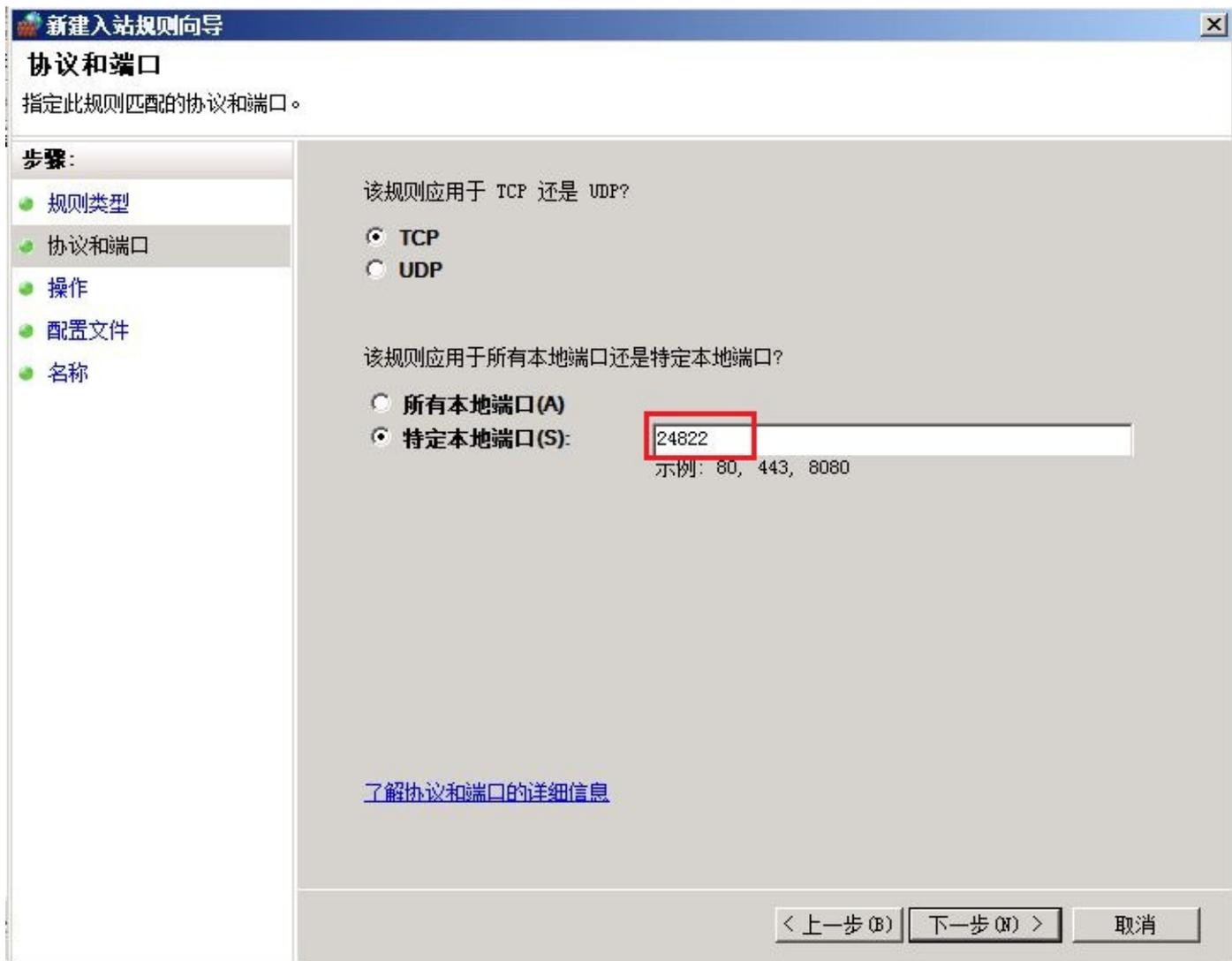
1. 右鍵選擇【我的電腦】>【管理】，彈出"服務器管理器"界面，選擇"配置>高級安全Windows防火牆>入站規則"，右鍵選擇"入站規則"，選擇"新規則"。



2. 彈出"新建入站規則向導"，如下圖所示，選擇"端口"，點擊【下一步】。



3. 在"特定本地端口"內輸入 "24822"，點擊【下一步】。



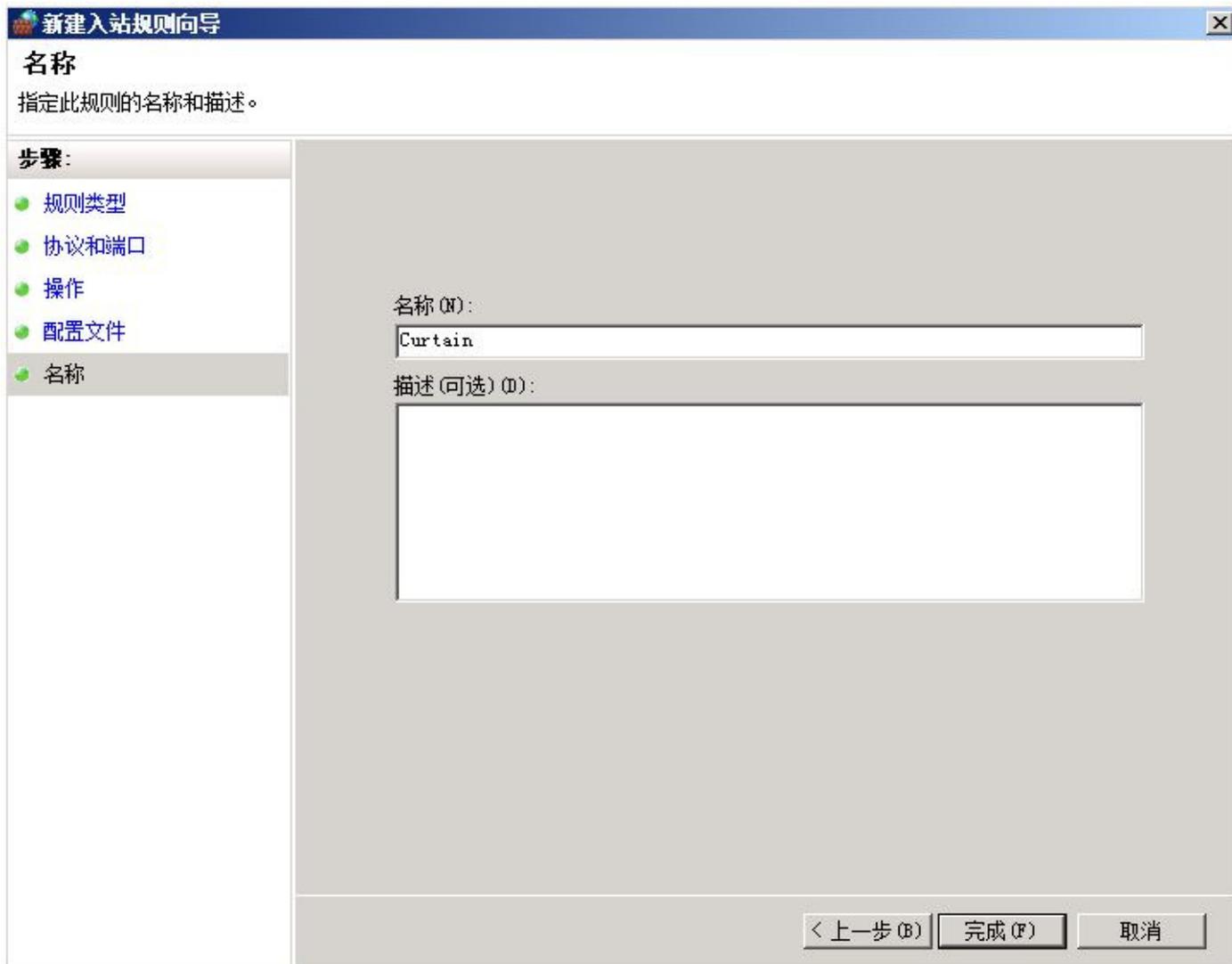
4. 選擇"允許連接"，點擊【下一步】。



5. 如圖所示默認勾選上"域"，"專用"，"公用"，點擊【下一步】。



6. 在名稱內輸入"Curtain"，點擊【完成】。



7. 查看右方入站規則的列表，在列表中會多出一項"Curtain"，如下圖所示，添加例外端口插件成功。



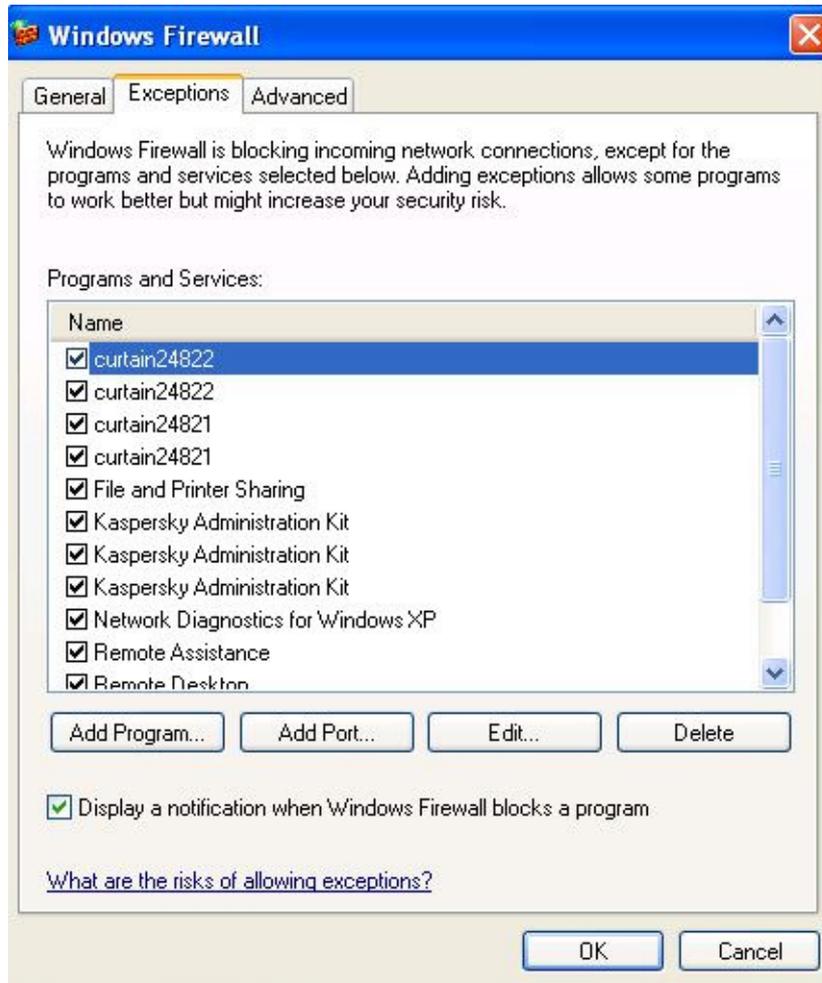
同理，按上面步驟設置24822的UDP入站規則，24821的TCP的出站規則，24821的UDP的出站規則即可。

備註：

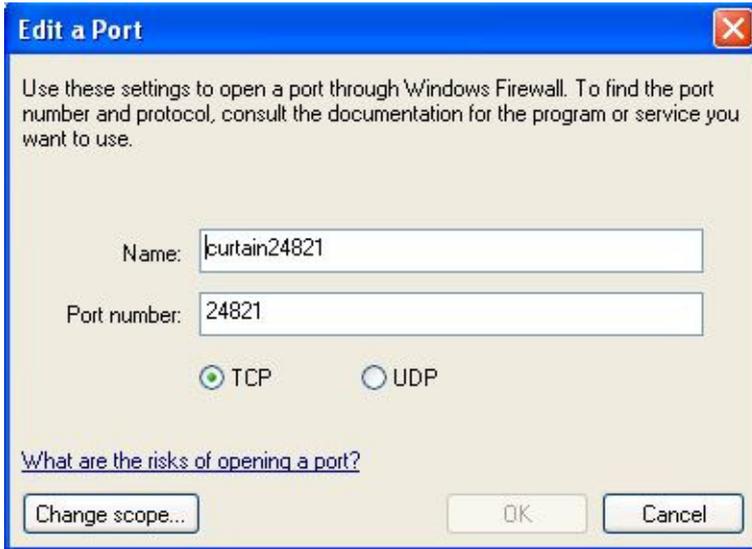
- 設置出站規則時，右鍵選擇"出站規則"，選擇"新規則"。
- 請注意，在Curtain客戶端上入站規則是開放端口24822，而在Curtain管理員和服務器插件上入站規則是開放端口24821，很容易混亂。

於Windows 2003和XP，設置例外端口的步驟

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



2. 給此例外輸入名稱、端口為TCP的24821，並按OK確定。



同理，按上面步驟設置UDP的24821，TCP的24822，UDP的24822即可。

2.4.3 - 於Curtain服務器插件上檢查Tomcat 8005端口是否已被佔用

在安裝Curtain服務器插件過程中，會同時安裝Tomcat，為了避免Tomcat端口8005衝突，請在安裝Curtain服務器插件之前先檢查端口是否已被佔用。如果端口8005已被佔用，請在安裝Curtain服務器插件後不要重啟電腦，先為Curtain服務器插件更改Tomcat端口（更改端口步驟，請參考FAQ 00193）。

查看Tomcat端口8005的步驟：

1. 在Command Prompt下，輸入netstat -ano|findstr "8005"，然後按“輸入”。
2. 如果該端口沒有被佔用，查找為空（如下圖）。

```

C:\Windows\system32>netstat -ano|findstr "8005"

C:\Windows\system32>
  
```

3. 如果端口已被佔用，就會列出佔用程序的信息。

```

Administrator: Command Prompt

Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>netstat -ano|findstr "8005"
TCP    127.0.0.1:8005          0.0.0.0:0             LISTENING      3956

C:\Windows\system32>tasklist|findstr "3956"
Tomcat8.exe                3956 Services                0             40,760 K

C:\Windows\system32>
  
```

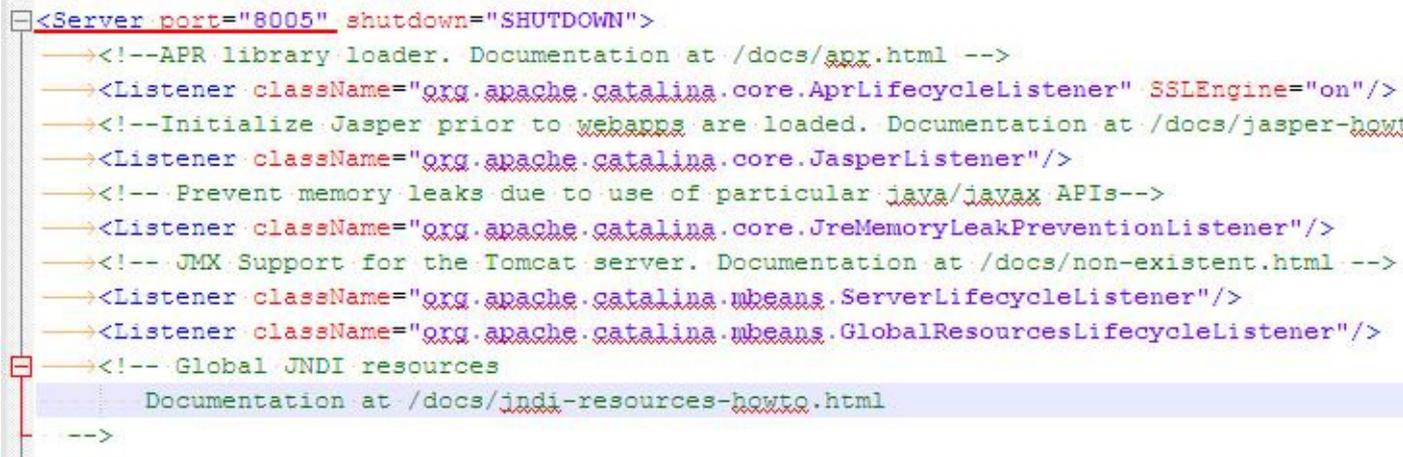
4. 使用PID來查詢程式信息，於Command Prompt，輸入tasklist|findstr "3856"，然後按“輸入”（上圖例子PID為3956）。
5. 手動修改server.xml文檔（請參考FAQ 00193）。

2.4.4 - 為Curtain服務器插件更改Tomcat 8005端口

如果Tomcat端口8005已被其他程式佔用，請在安裝Curtain服務器插件後不要重啟電腦，先為Curtain服務器插件更改Tomcat端口。

為Curtain服務器插件更改Tomcat端口的步驟：

1. 於電腦管理，將“Curtain web service”服務停止。
2. 到文件夾 C:\Program Files\CoworkShop\Curtain 3\Runtime\tomcat6.0.26\conf\。
3. 用Notepad打開server.xml文件（或其他編輯工具）。
4. 找到port 8005（如圖所示位置），並將“8005”改為其他空間的端口，然後保存。



```

<Server port="8005" shutdown="SHUTDOWN">
  <!-- APR library loader. Documentation at /docs/apr.html -->
  <Listener className="org.apache.catalina.core.AprLifecycleListener" SSLEngine="on"/>
  <!-- Initialize Jasper prior to webapps are loaded. Documentation at /docs/jasper-howto -->
  <Listener className="org.apache.catalina.core.JasperListener"/>
  <!-- Prevent memory leaks due to use of particular java/javax APIs-->
  <Listener className="org.apache.catalina.core.JreMemoryLeakPreventionListener"/>
  <!-- JMX Support for the Tomcat server. Documentation at /docs/non-existent.html -->
  <Listener className="org.apache.catalina.mbeans.ServerLifecycleListener"/>
  <Listener className="org.apache.catalina.mbeans.GlobalResourcesLifecycleListener"/>
  <!-- Global JNDI resources
  Documentation at /docs/jndi-resources-howto.html
  -->

```

5. 於電腦管理，將“Curtain web service”服務啟動（安裝Curtain服務器插件後需要重啟電腦）。
6. 完成。

3 - 安裝

3.1 - 安裝Curtain管理員

當決定好在那一台服務器上安裝Curtain管理員後，請按以下步驟進行安裝。

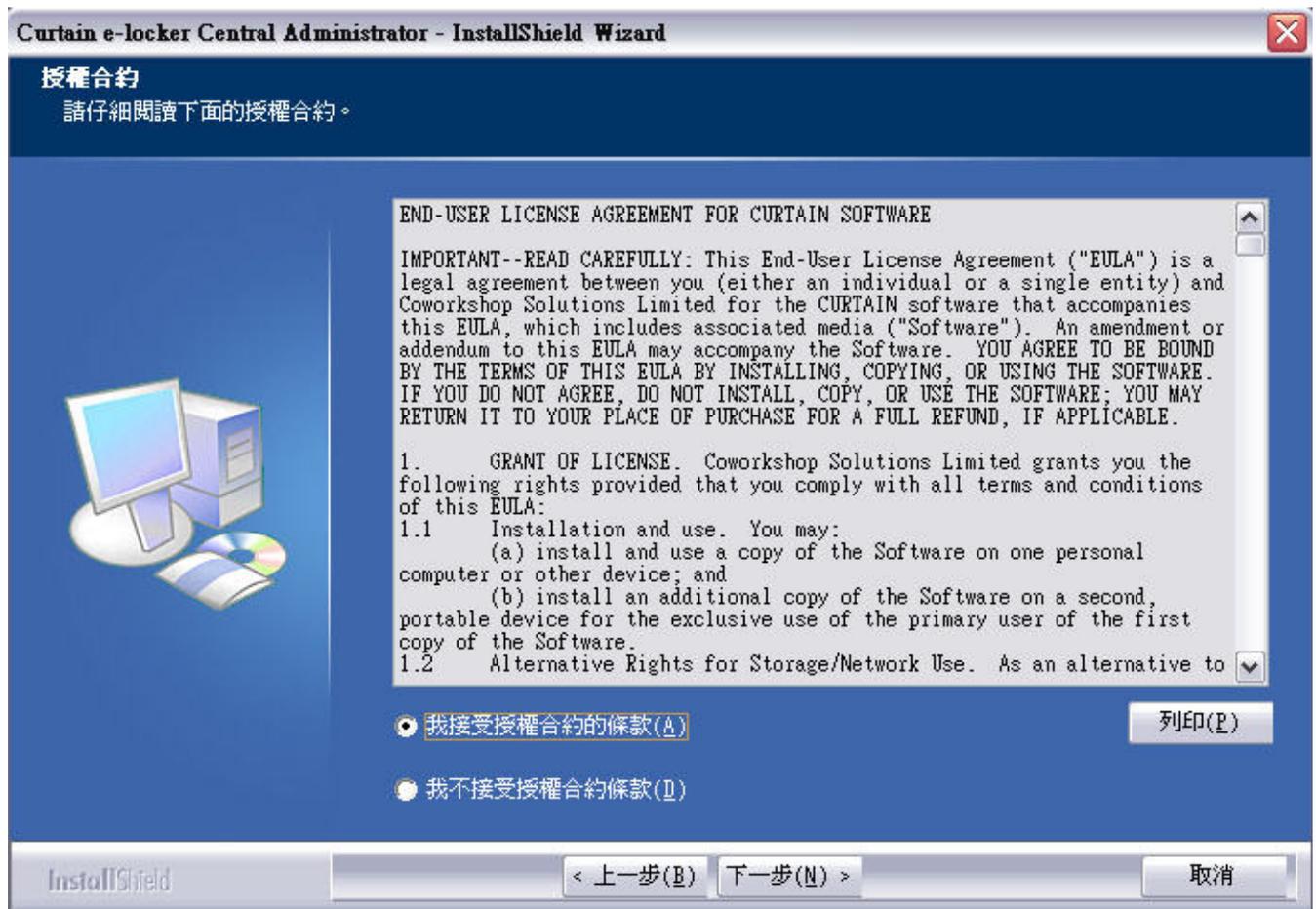
[安裝Curtain管理員的步驟:](#)

1. 複製適合的Curtain服務器安裝包(如:CurtainAdmin_Win32(327304).zip 或 CurtainAdmin_X64(327304).zip)到服務器的硬盤上。
2. 解壓安裝包。
3. 執行Curtain服務器安裝程序。請確保以Windows管理員身份登入。接著，請選擇安裝程序的語言。

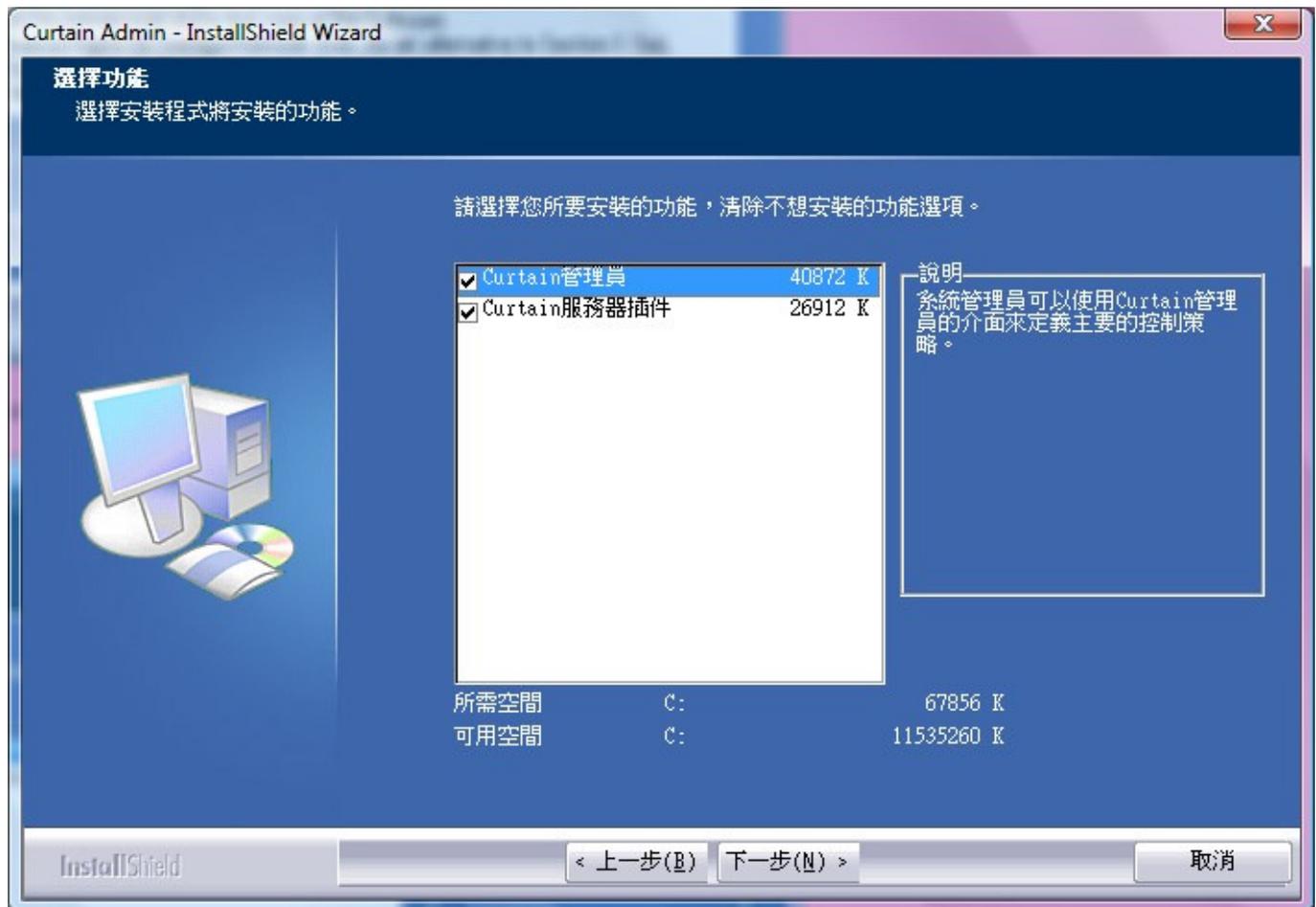


4. 選擇安裝程序的語言，並按確定。

5. 閱讀軟件使用証協議。如同意協議內容，選擇"我接受軟件使用証協議"，並按下一步繼續安裝。



接著，請選擇模塊進行安裝。



6. 有以下兩個情況:

(a) 如果只是在這台服務器上安裝Curtain管理員，
- 只需要點選"Curtain管理員"

(b) 如果需要保護這台服務器上的資料(如:文件伺服器上的受保護共享文件夾、受保護網站等)，
- 點選"Curtain管理員"以安裝Curtain管理員，和
- 點選"Curtain服務器插件"以安裝Curtain服務器插件。
並按下一步繼續安裝。

7. 選擇安裝程序的文件夾，並按下一步繼續安裝。

8. 按安裝按鈕，開始安裝程序。

9. 如果在此台服務器上安裝了Curtain服務器插件，在完成安裝後，請重啓電腦。

3.2 - 安裝Curtain服務器插件

如果需要保護一台服務器上的資料(如:文件服務器上的受保護共享文件夾、受保護網站等)，你需要在該服務器上安裝Curtain服務器插件。請按以下步驟進行安裝。

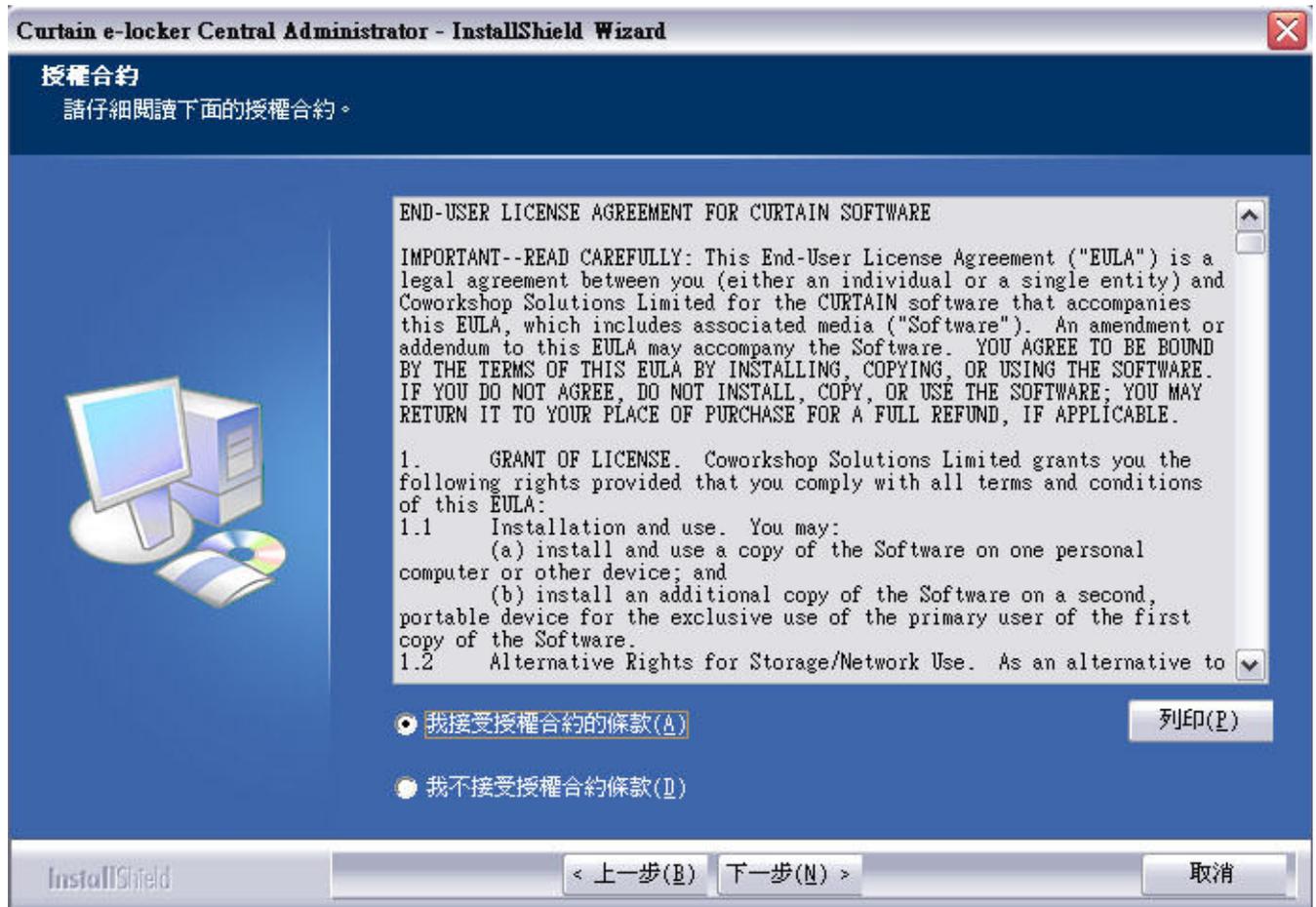
安裝Curtain服務器插件的步驟:

1. 複製適合的Curtain服務器安裝包(如:CurtainAdmin_Win32(327304).zip 或 CurtainAdmin_X64(327304).zip)到服務器的硬盤上。
2. 解壓安裝包。
3. 執行Curtain服務器安裝程序。請確保以Windows管理員身份登入。接著，請選擇安裝程序的語言。

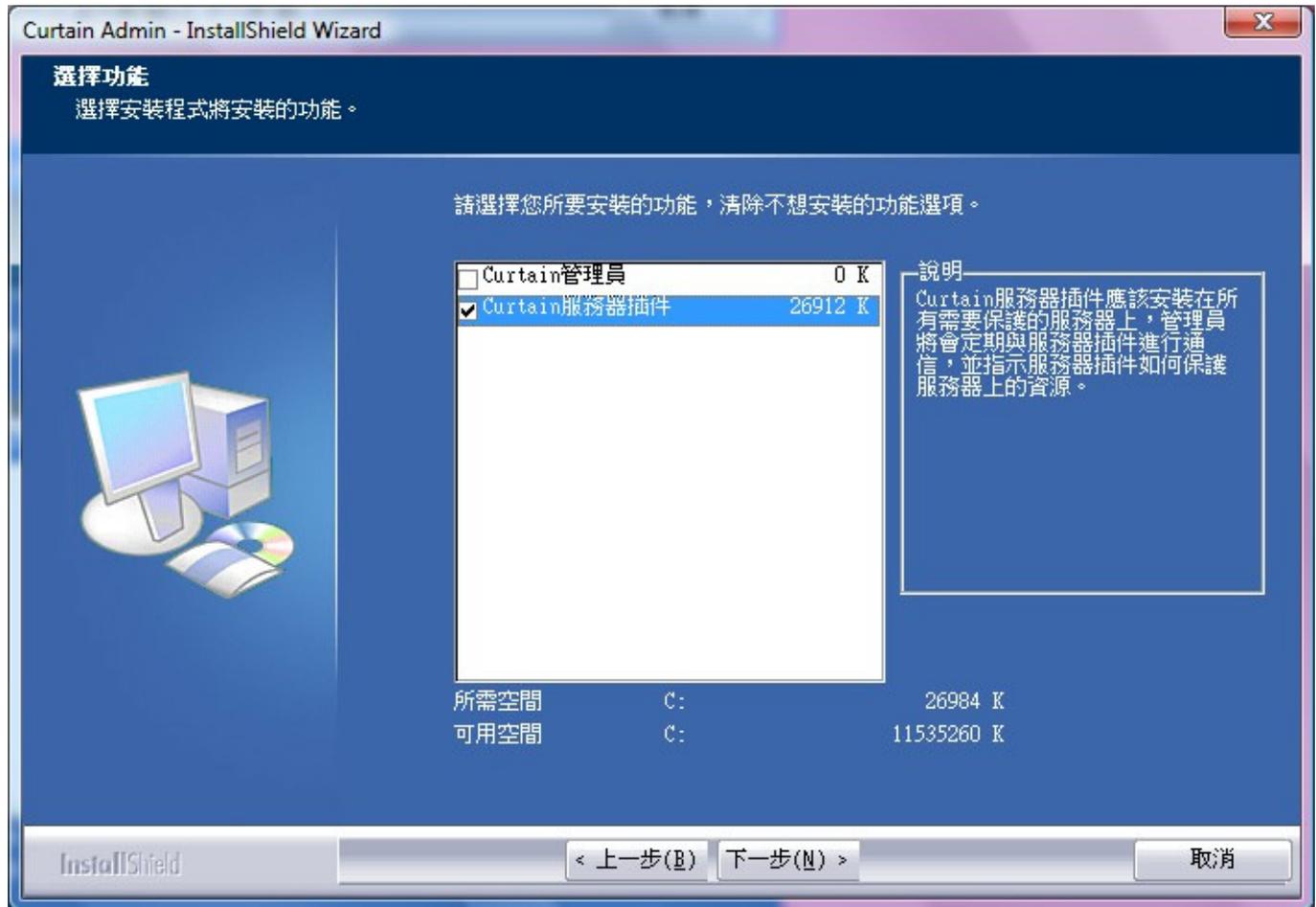


4. 選擇安裝程序的語言，並按確定。

5. 閱讀軟件使用証協議。如同意協議內容，選擇"我接受軟件使用証協議"，並按下一步繼續安裝。



接著，請選擇模塊進行安裝。



6. 只需要點選"Curtain服務器插件"，並按下一步繼續安裝。
7. 選擇安裝程序的文件夾，並按下一步繼續安裝。
8. 按安裝按鈕，開始安裝程序。
9. 在完成安裝後，請重啓電腦。

3.3 - 安裝Curtain客戶端

如果用戶需要使用服務器上的受保護資料時(如:文件服務器上的受保護共享文件夾、受保護網站等)，用戶的電腦必需要安裝Curtain客戶端。請按以下步驟進作安裝。

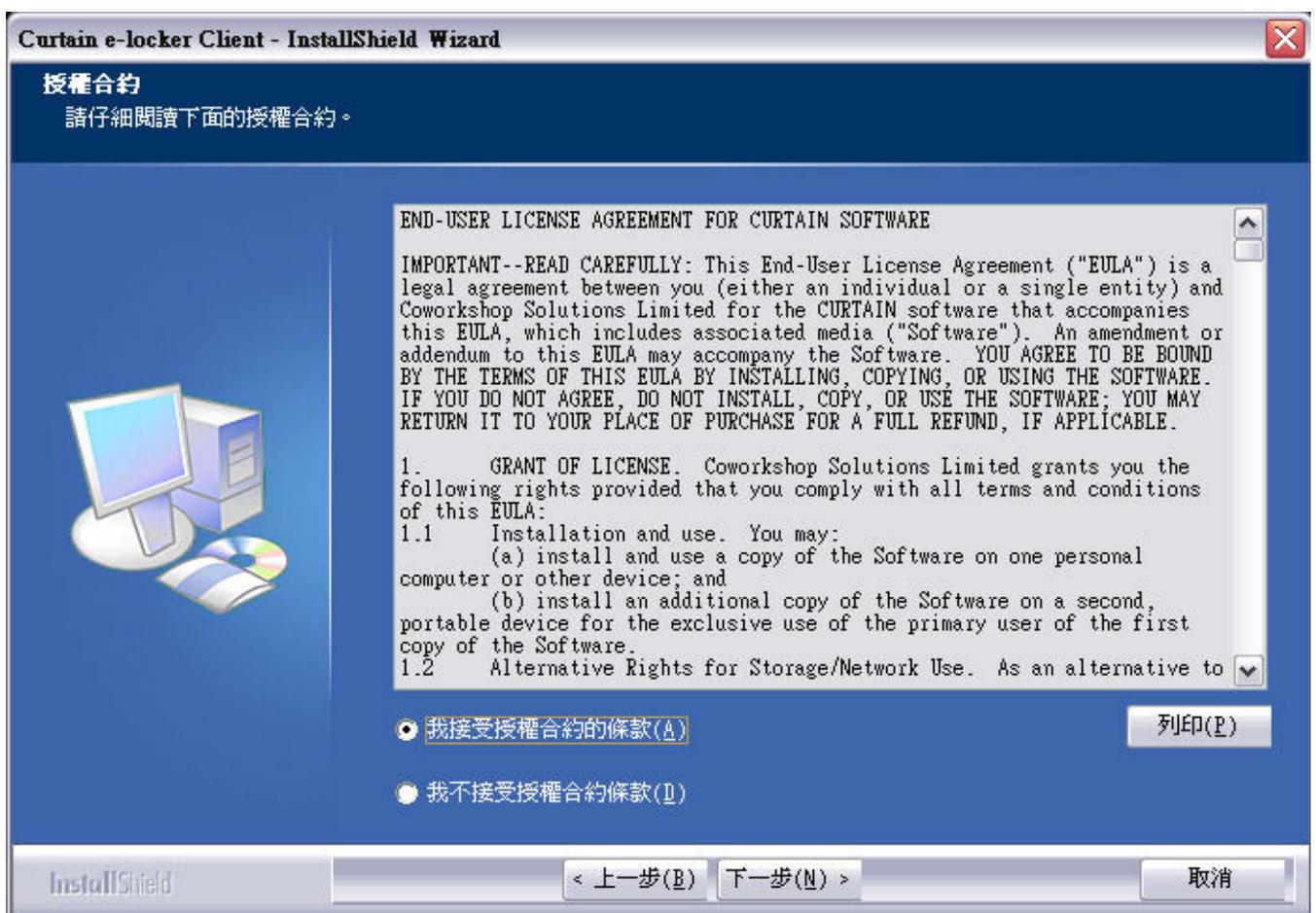
安裝Curtain客戶端的步驟:

1. 複製適合的Curtain客戶端安裝包(如:CurtainClient_Win32(327304).zip 或 CurtainClient_X64(327304).zip)到用戶電腦的硬盤上。
2. 解壓安裝包。

3. 執行Curtain客戶端安裝程序。請確保以Windows管理員身份登入。接著，請選擇安裝程序的語言。



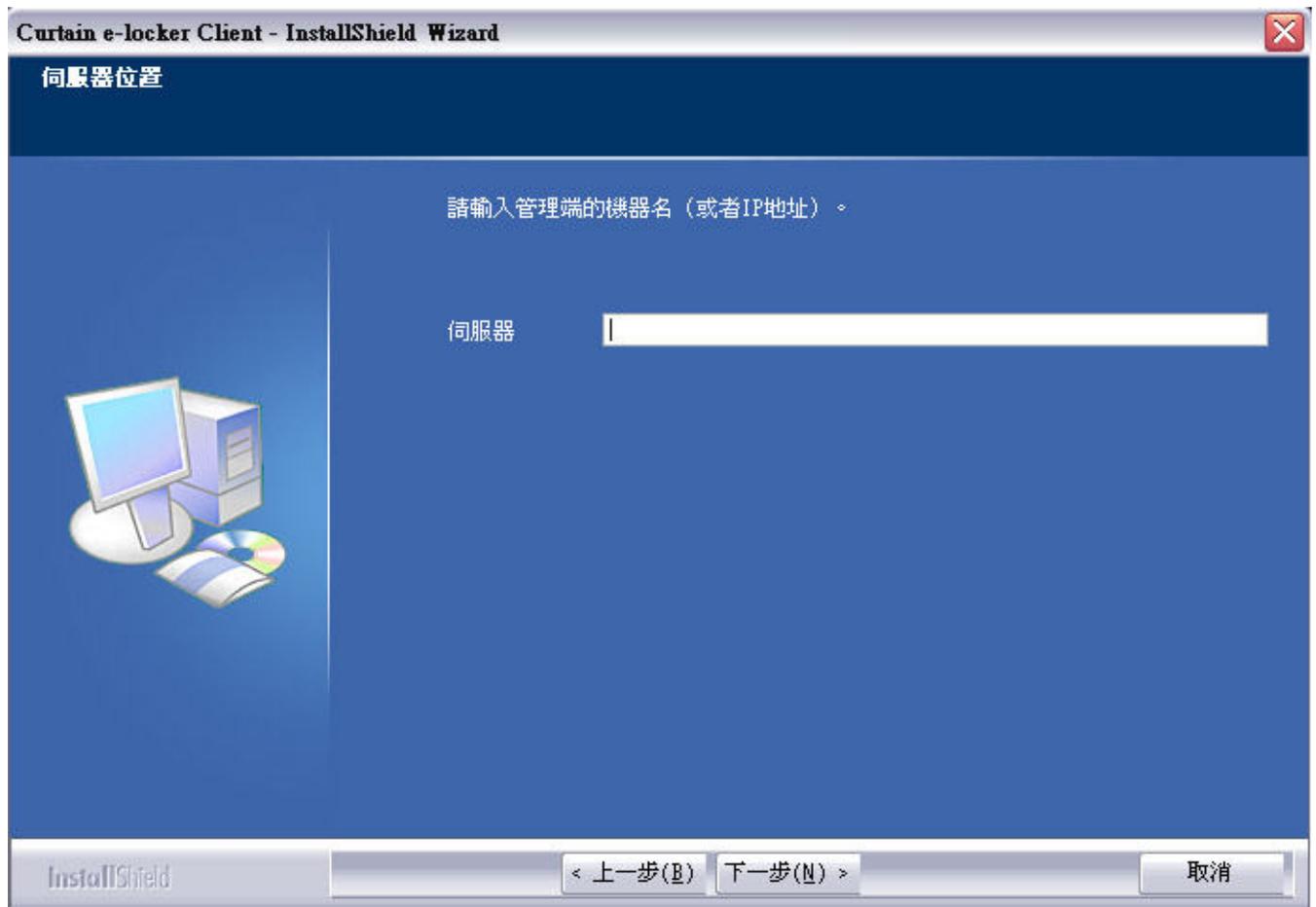
4. 選擇安裝程序的語言，並按確定。
5. 閱讀軟件使用証協議。如同意協議內容，選擇"我接受軟件使用証協議"，並按下一步繼續安裝。



接著，安裝程序會檢測系統環境是否滿足安裝要求，請按下一步繼續安裝。



6. 輸入Curtain管理員的IP地址或電腦名稱(請確保輸入正確。如不太肯定，請聯絡系統管理員)，並按下一步繼續安裝。



7. 選擇安裝程序的文件夾，並按下一步繼續安裝。

8. 按安裝按鈕，開始安裝程序。

9. 完成安裝後，請重啓電腦。

備註：如果想通過Group Policy(群組原則)遠程安裝Curtain客戶端，請參考FAQ 00201。

4 - 產品激活

4.1 - 產品激活

Curtain e-locker應用了產品激活技術來控制軟件的使用証。如果沒有進行產品激活，客戶只可以使用Curtain e-locker三十天。期間，客戶可以隨意使用軟件，以達至評估軟件功能的目的。在三十天後，如果客戶想延長測試期限，客戶可以向我們或我們的代理商作出申請。

對於已經是Curtain e-locker的客戶，客戶應該於安裝系統時進行產品激活。並且需要每年進行一次產品重新激活，以控制軟件的使用証。我們會協助客戶進行每年的重新激活而不收取任何費用(包括沒有購買軟件維護的客戶)。關於產品激活的步驟，請參考相關文件。

當需要進行產品激活時，每當用戶開啟Curtain客戶端或Curtain管理員時，系統會彈出提示信息。以下是相關提示信息。



於激活限期前三十天，系統會開始彈出提示信息。如果到激活限期時還未進行激活，用戶將不能開啟Curtain客戶端和Curtain管理員，直至產品重新激活。

備註：管理員只需要在Curtain管理員上進行產品激活，當Curtain管理員被成功激活後，所有Curtain客戶端也會自動被激活。

4.2 - 激活Curtain e-locker

當需要進行產品激活時，每當用戶開啟Curtain客戶端或Curtain管理員時，系統會彈出提示信息。請按以下步驟進行產品激活。

激活Curtain e-locker的步驟:

1. 開啟Curtain管理員。接著，系統會要求進行產品激活。



2. 按"是"開始產品激活(或按"否"跳過激活)。
 如果你是初次進行產品激活，請輸入25個位的產品鑰匙。
 如果這是每年的產品重新激活，請跳到步驟4繼續。

3. 輸入產品鑰匙(請注意大小寫)和公司資料，完成輸入後按確定繼續。
 接著，系統會顯示以下對話框。

4. 按"生成激活請求文件"按鈕將"要求激活文檔"保存，並將該文檔發送給我們(registration@coworkshop.com)。
 我們收到要求激活文檔後，我們會把以下文檔發送回給你。
 如果這是初次產品激活，你將會收到兩個文檔(確認碼和授權字符串)
 如果這是每年的產品重新激活，你將會收到一個文檔(確認碼)

5. 當收到確認碼後，請按"導入確認激活文件"，並選擇確認碼文檔。按確定按鈕後，系統會顯示以下信息。

- 如果這是初次產品激活，請跳到下一個步驟繼續。
 如果這是每年的產品重新激活，你已經成功完成了重新激活。

6. 在Curtain管理員，於菜單上選擇"檔案>設定"。接著，系統會顯示"設定"對話框。請輸入授權字符串，並按確定。

設定

設定 伺服器信息 受保護網路磁碟機 受保護網路埠 密碼管理

授權

授權字符串 *****

指定新的管理員

伺服器選項

請求狀態報告 30 分鐘

請求取得設定 10 分鐘

客戶端選項

狀態報告及查詢設定 10 分鐘

狀態報告 10 分鐘

查詢配置 10 分鐘

查詢升級檔 30 分鐘

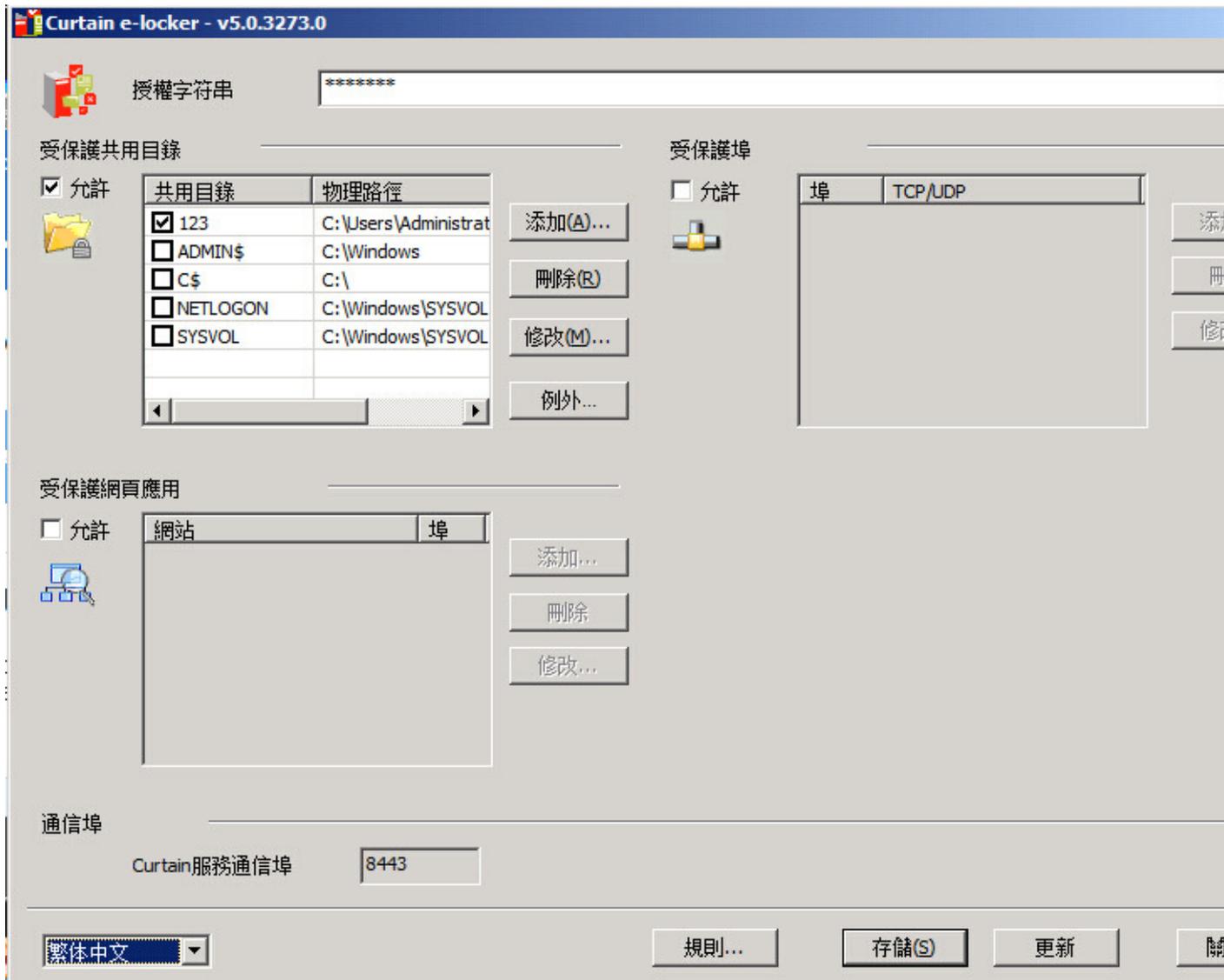
電郵設定

SMTP伺服器 埠： 25

確定 取消 應用

如果你為了保護服務器上的資料(如:共享文件夾等)，在服務器上只單獨安裝了Curtain服務器插件，請按步驟7至10把授權字符串輸入到Curtain服務器插件上。

7. 啟動"安全網絡管理" (於"開始 > 程式 > Coworkshop Curtain e-locker"下)。



8. 輸入授權字符串，並按"存儲"。

9. 按"更新"來應用新的設定。

10. 按"關閉"離開。

恭喜! 你已經成功完成了產品激活。

5 - 設置

5.1 - 新增安全策略群組

管理員可以建立多個安全策略群組來管理不同的電腦或用戶，我們建議用Default Policy安全策略群組來保護大部份的電腦或用戶，以下是安全策略群組例子以供參考。

- Default Policy: 用於一般用戶，不容許列印和保存受保護文檔到受保護區以外。
- Managers: 用於管理人員，容許列印和保存受保護文檔到受保護區以外。
- Notebooks: 用於手提電腦: 對於手提電腦，不容許列印和保存受保護文檔到受保護區以外，並且電腦必需每72小時連接Curtain管理端才能繼續使用本地受保護區內的文檔。

以下是新增安全策略群組的步驟:

1. 在Curtain管理員菜單，選擇"文件>新建安全策略"。接著，系統會要求你輸入新建的安全策略名稱。



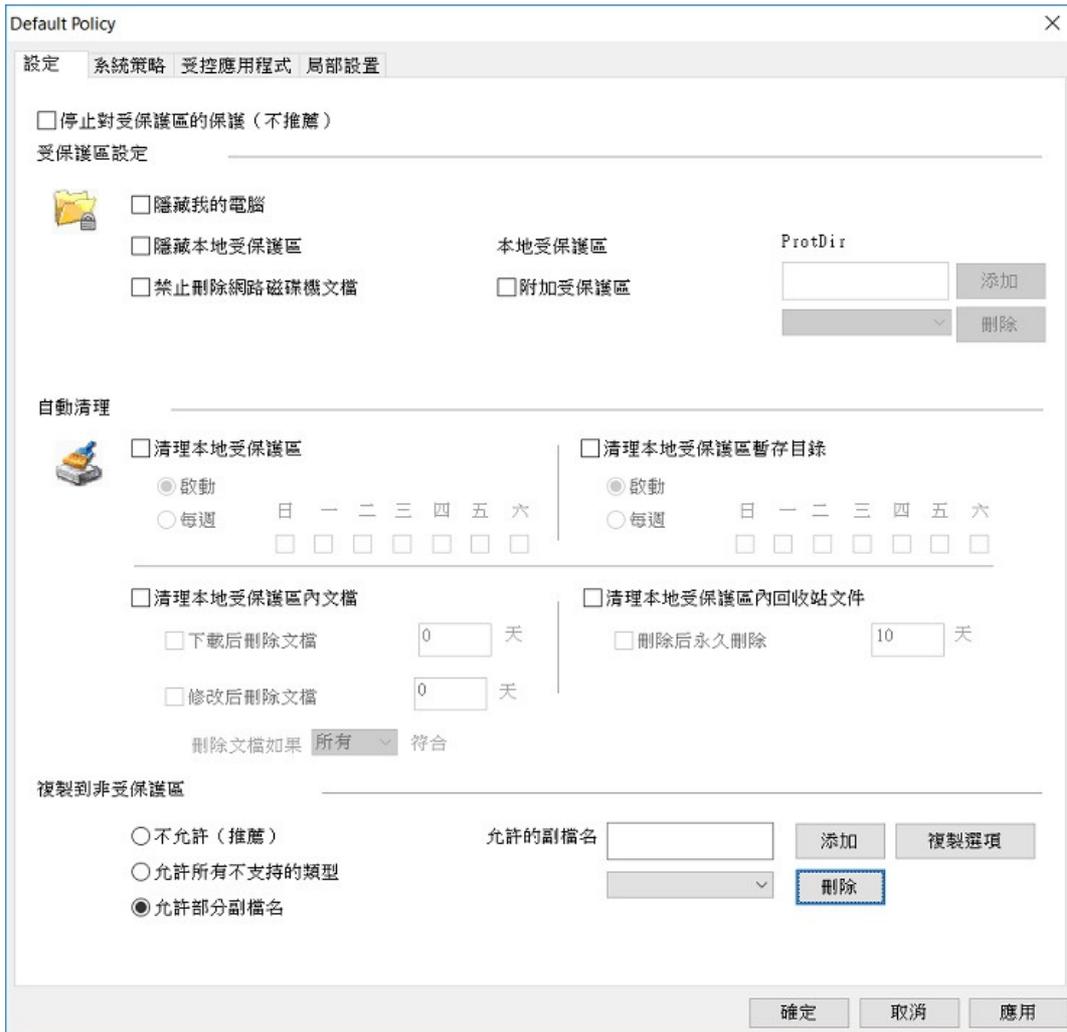
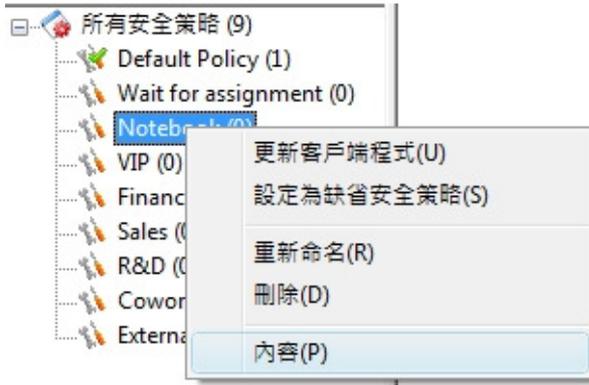
2. 輸入新建的安全策略名稱，並按確定。



5.2 - 修改安全策略群組的設定

修改安全策略群組設定的步驟:

1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵，並選擇"內容"。



以下是一個安全策略群組的設置簡介:

於"設定"頁

- 停止對受保護區的保護
- 附加本地受保護區
- 本地受保護區的自動清理
- 用副檔名設定"複製出去"策略
- "加密出去"策略

於"系統策略"頁

- 在線/離線控制

於"受控應用程式"頁

- 設定如何控制應用程式使用受保護文檔 (如:不容許列印和保存受保護文檔到受保護區以外)

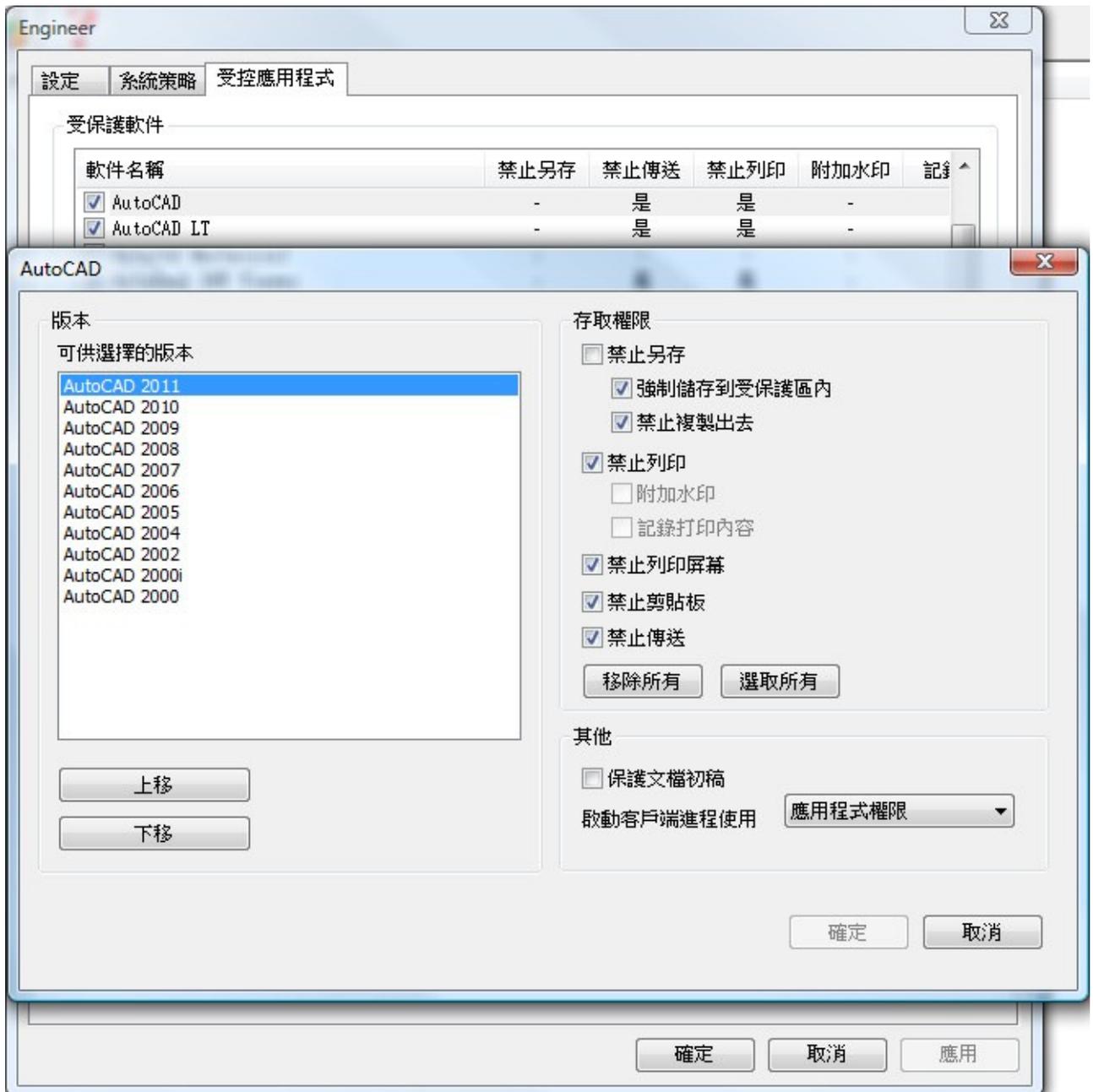
於"局部設置"頁

- 設定此安全策略群組外發申請的審批人
- 設定此安全策略群組所包括的打印機

這裡我們集中於"受控應用程式"頁面的設定，其他的功能，請參考第六章。

2. 於"受控應用程式"頁，雙擊你想修改設定的應用軟件。

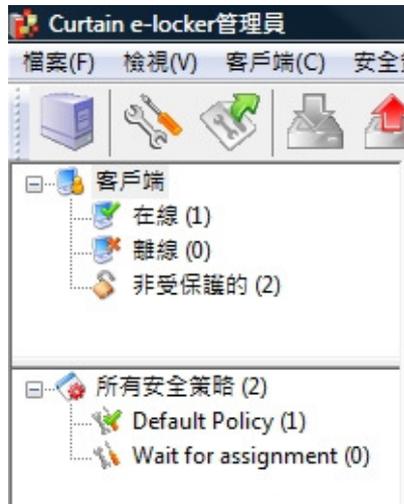
3. 修改Curtain權限控制，並按確定鍵確認。



4. 重覆步驟2至步驟3去修改其他應用軟件的設定。

5.3 - 設定默認策略

當一個安全策略群組被設定為默認策略時，所有新安裝的Curtain客戶端會自動被指派到該安全策略。系統會在默認策略上加上綠色勾號以作識別。當在剛剛完成安裝後第一次開啟Curtain管理員，默認策略是"Default Policy"。



系統有兩個預設的安全策略群組。

- Default Policy: 這個策略群組的預設控制是比較嚴謹的。用戶可以如常使用受保護區內的機密文檔，但是他們不能將文檔帶出受保護區。
- Wait for Assignment: 這個策略群組的預設控制是完全不容許用戶閱讀或修改受保護區內的機密文檔。

所有新安裝的Curtain客戶端都會先連接到Curtain管理員，並自動被指派到默認安全策略。如果管理員想先確認Curtain客戶端然後才容許它們閱讀或修改受保護區內的機密文檔，管理員可以將"Wait for Assignment"設定為默認策略。設置後，所有新安裝的客戶端都需要管理員指派它們到合適的安全策略才能使用機密文檔。

將一個安全策略群組設定為默認策略的步驟:

1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵。

2. 選擇"設定為預設安全策略"



3. 完成

5.4 - 按用戶/用戶群組來配置安全策略

Curtain e-locker的安全策略可應用於電腦或用戶/用戶組。如果您希望通過AD用戶/用戶組授予安全策略，則需要連接AD以將用戶信息導入Curtain管理員。當第一次Curtain管理員獲取用戶信息時，系統將使用默認安全策略來控制該用戶/用戶組。管理員需要手動將用戶/用戶組分配給適當的安全策略組。

要按用戶/用戶組授予安全策略，請按照以下步驟在Curtain管理員中啟用“按用戶分配”。

在Curtain管理員中啟用“按用戶分配”的步驟：

1. 運行Curtain管理員，打開文件 -> 設定 -> 策略分配方式。
2. 選擇“按用戶分配”，單擊“確定”按鈕。



然後“用戶和組”將顯示在Curtain管理員中。



3. 完成。

從AD域導入用戶和用戶組的步驟：

1. 運行Curtain管理員，打開文件 -> 設定 -> LDAP。
2. 選“啟用LDAP”按鈕。
3. 在“LDAP服務器地址”上輸入LDAP服務器地址，DNS或IP地址。
4. “LDAP服務器端口”，默認端口為389。
5. 建議啟用“使用安全LDAP連接”，表示使用安全的LDAP連接到AD（默認為不啟用）。

6. 在“LDAP用戶名”下輸入用戶名，以連接LDAP服務器。
7. 在“LDAP密碼”中輸入密碼。
8. “LDAP搜索庫”，輸入用戶或用戶組的根，可輸入CN、OU和DC。
 - 例如搜索整個域，可以輸入“dc=域名，dc=域後綴”（例如：“dc=test，dc=com”）。
 - 例如搜索整個組，可以輸入“ou=組織單元名稱，dc=域名，dc=域後綴”（例如：“ou=it，dc=test，dc=com”）。
 - 例如搜索某用戶，可以輸入“cn=用戶名，ou=組織單元名稱，dc=域名，dc=域後綴”（例如：“cn=tester，ou=it，dc=test，dc=com”）。
9. “LDAP信息緩存”，用於AD的設置緩存信息（默認為15分鐘）。
10. 設置完成後，單擊“測試連接”按鈕查看是否成功連接到AD。



11. 如果AD用戶/用戶組已成功導入Curtain管理員，則它們將顯示在Curtain管理員中的“用戶和組”，如下圖。



12. 完成。

備註：對於本地/工作組用戶，一旦他們打開Curtain客戶端，它們將被列在“用戶和組”下。

指派用戶/用戶組到合適的安全策略的步驟：

1. 在Curtain管理員中，左面控制板中選擇用戶/用戶組。然後，用戶/用戶組將在右面控制板中列出。



2. 選擇用戶/用戶組（按Ctrl按鈕可選擇多個用戶/用戶組）。

3. 右鍵單擊並選擇“改變安全策略”以將用戶/用戶組分配給適當的安全策略組。



4. 重複步驟2-3，將其他用戶/用戶組分配給適當的安全策略組。

5. 完成。

5.5 - 指派電腦/用戶到合適的安全策略

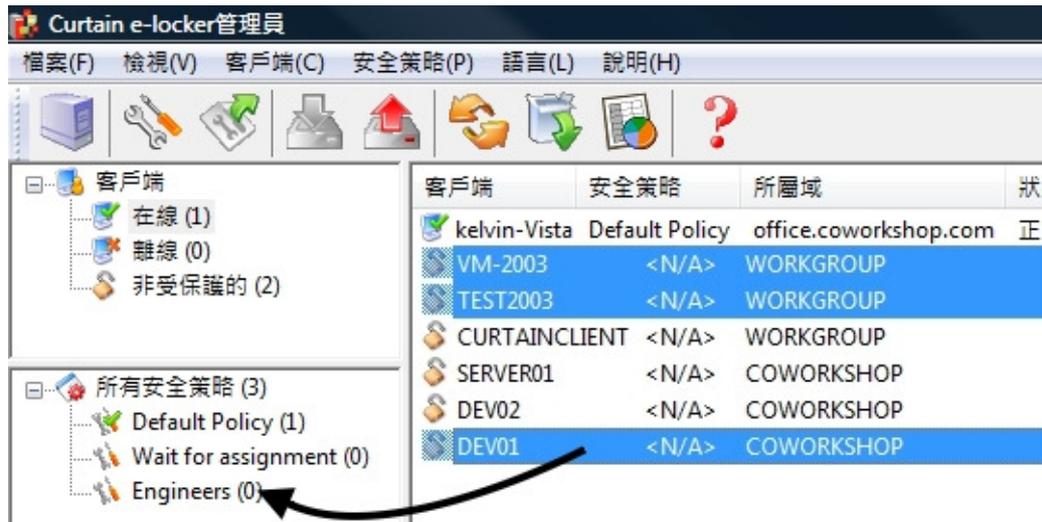
指派Curtain客戶端到合適的安全策略的步驟:

1. 在Curtain管理員左手面的控制板，點選“在線”或“離線”。



2. 選擇用戶電腦(按Ctrl鍵可選擇多台電腦)。

3. 將選擇好的用戶電腦拖放到合適的安全策略。

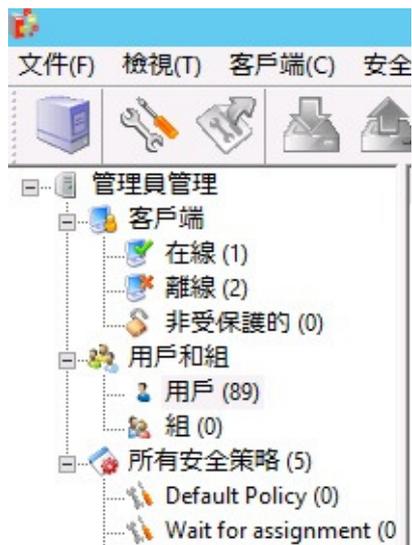


4. 重覆步驟2至步驟3，將其他Curtain客戶端指派到合適的安全策略。

5. 完成

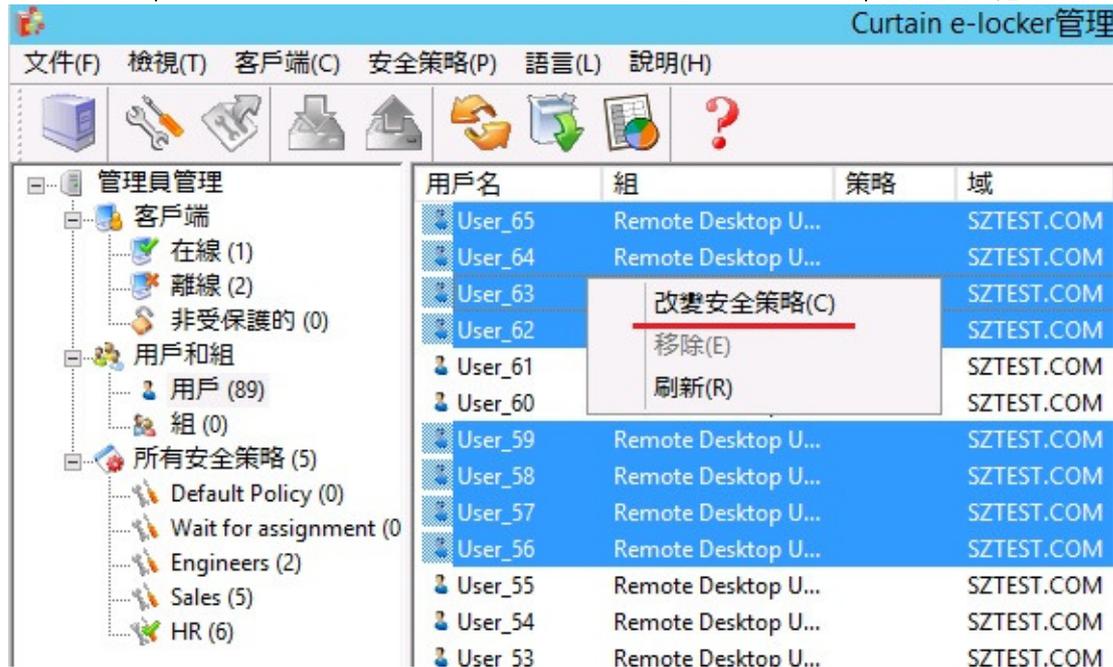
指派用戶到合適的安全策略的步驟：

1. 在Curtain管理端左手面的控制板，點選“用戶/組”。



2. 選擇用戶/組(按Ctrl键可選擇多個用戶)。

3. 選擇好用戶/組後，點擊鼠標右鍵，彈出面板中選擇“改變安全策略”，將用戶/組選擇到合適的安全策略。



4. 重複步驟2至步驟3，將其他的用戶/組指派到合適的安全策略。

5. 完成。

5.6 - 設定服務器上的受保護區

Curtain e-locker可以用來保護不同服務器上的資源(如:Windows文件服務器上的共享文件夾、網站、甚至自己開發的應用或後台系統)。請按以下的步驟來設定服務器上的受保護區。

設定服務器上受保護區的步驟:

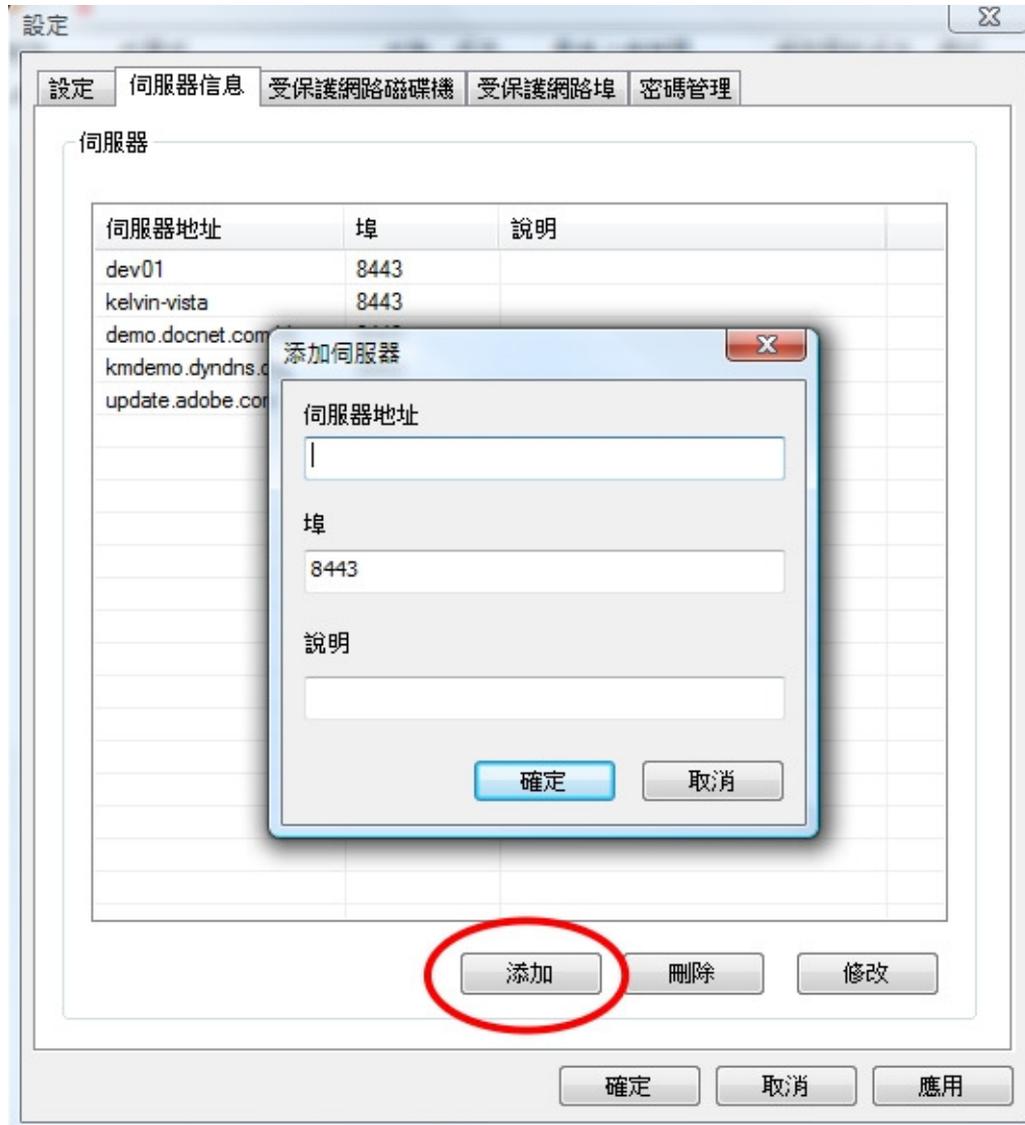
1. 在Curtain管理員，於菜單上選擇"文件> 設定"。



2. 於"伺服器信息"頁，按"添加"按鈕來新增伺服器。舉例:如果你想保護兩台Windows文件伺服器上的共享文件夾和一個應用網站，你需要將那三台伺服器添加在此頁。

伺服器地址: 服務器的電腦名稱或IP地址。

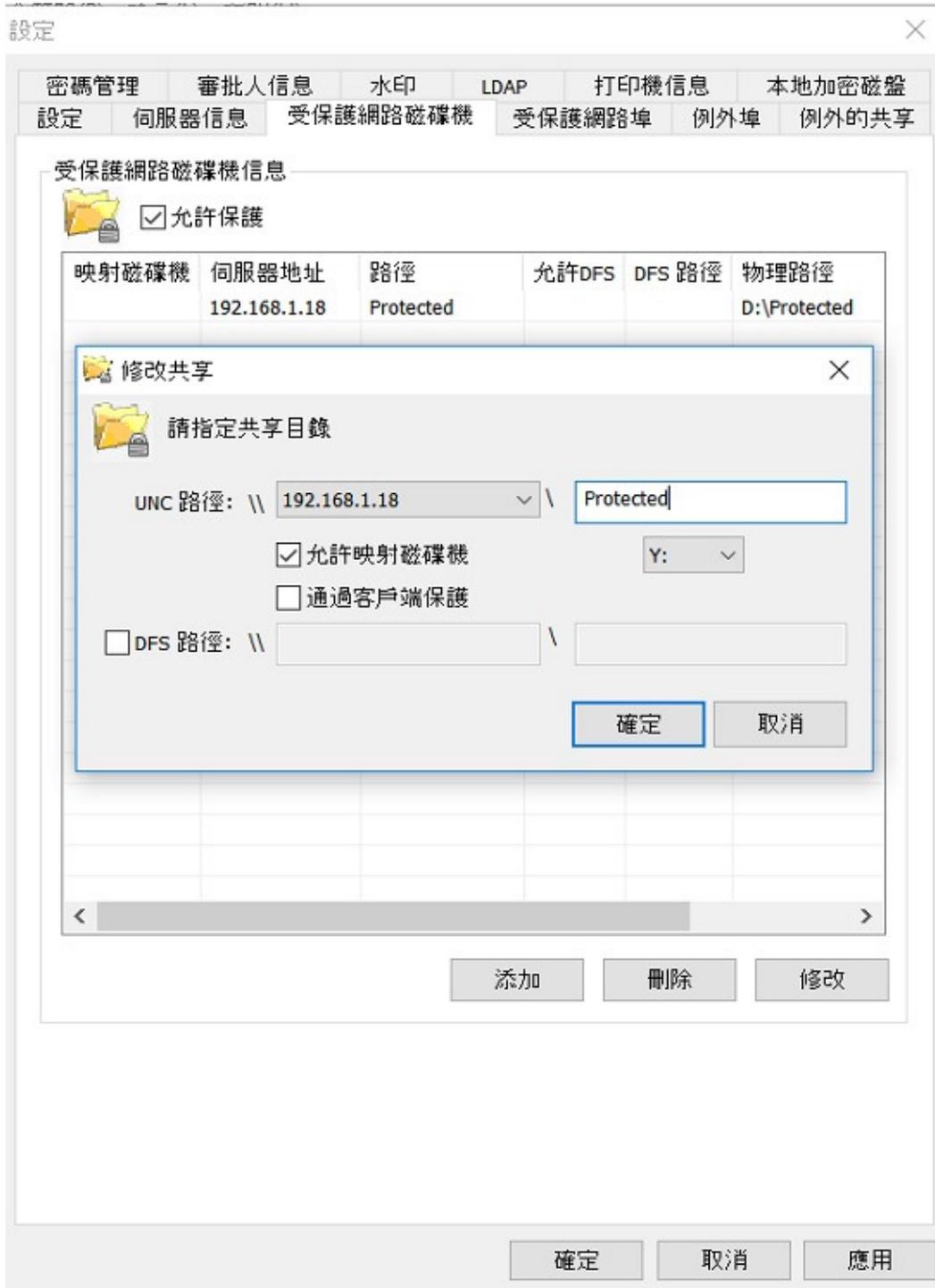
埠: 默認的埠是8443(用作Curtain管理員和Curtain伺服器插件之間的溝通)。



3. 新增服務器上受保護區。

情況1 - 保護Windows文件伺服器上的共享文件夾

- 於"受保護網路磁碟機"頁，點選"允許保護"。
- 按"添加"按鈕，系統會彈出對話框。



UNC 路徑: \\ 伺服器\分享名稱

- 伺服器 - 選擇伺服器(電腦名稱或IP地址)
- 分享名稱 - 輸入分享名稱(不是文件夾名稱, 除非你使用文件夾名稱來命名分享)

允許映射磁碟機: 如果你想Curtain客戶端於啟動時自動映射到指定的磁碟機, 請點選此選項並選擇磁碟機。要不然, 用戶需要手動進行磁碟機映射。

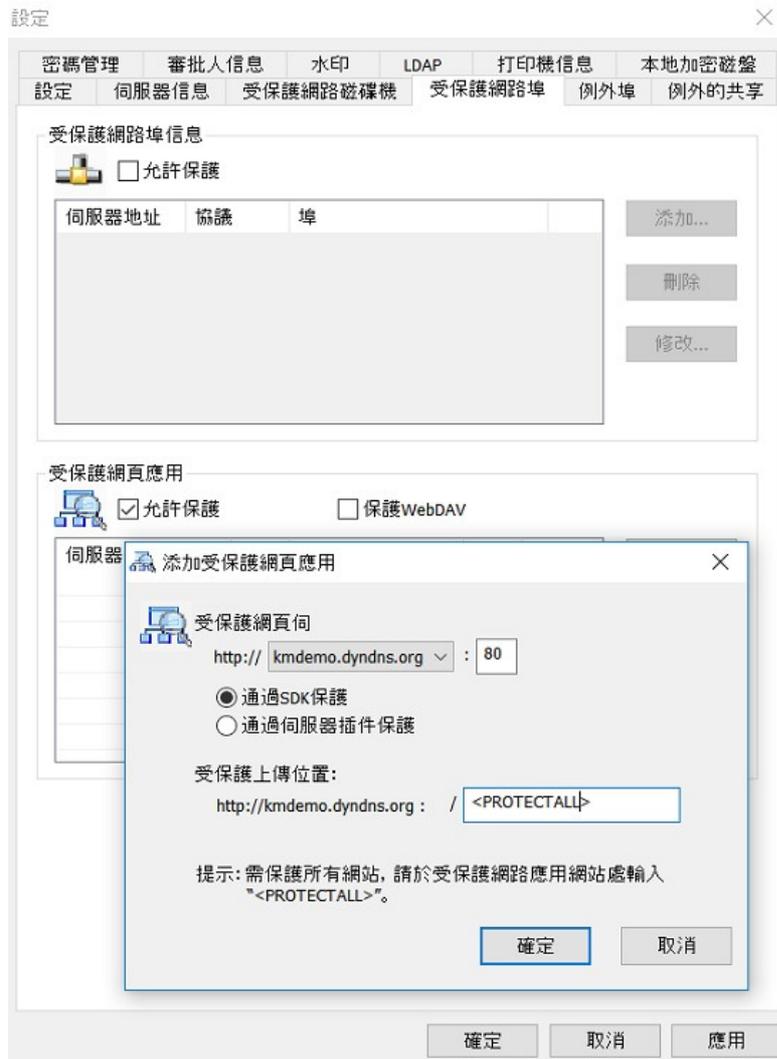
通過客戶端保護: 此選項只適用於你需要保護沒有安裝Curtain服務器插件的共享文件夾(如: NAS - Network Attached Storage)。

DFS路徑: 如果在上述的共享文件夾是由DFS(Distributed File System)來管理的, 請點選此選項。

- 服務器 - 輸入服務器名稱(用戶應該在我的網絡上看到該服務器名稱)
- 路徑 - 輸入路徑(用戶應該在我的網絡上看到該路徑)

情況2 - 保護應用網站

- 於"受保護網頁應用", 點選"允許保護"。
- 按"添加"按鈕, 系統會彈出對話框。



受保護網頁服務器: http://服務器:埠

- 服務器 - 選擇服務器(電腦名稱或IP地址)
- 埠 - 輸入埠(大部份的應用網站都是用80的)

通過SDK保護: 如果應用網站使用我們的SDK(software development kit)來跟Curtain e-locker作出整合, 請選擇此選項。

通過服務器插件保護: 如果應用網站並沒有專門跟Curtain e-locker作出整合, 請選擇此選項。

受保護上傳位置: http://服務器/路徑

- 路徑 - 輸入你想保護的路徑

例子1 - Microsoft SharePoint (如:http://SharePoint服務器/Site)

- 管理員可以於SharePoint上建立很多Site。如果管理員只想用Curtain e-locker來保護其中一些Site, 管理員可以於路徑上輸入Site名稱。設置後, 用戶需要使用受保護的Internet Explorer瀏覽器來訪問受保護的Site, 所有在這個Site內的資料都被Curtain e-locker保護起來。

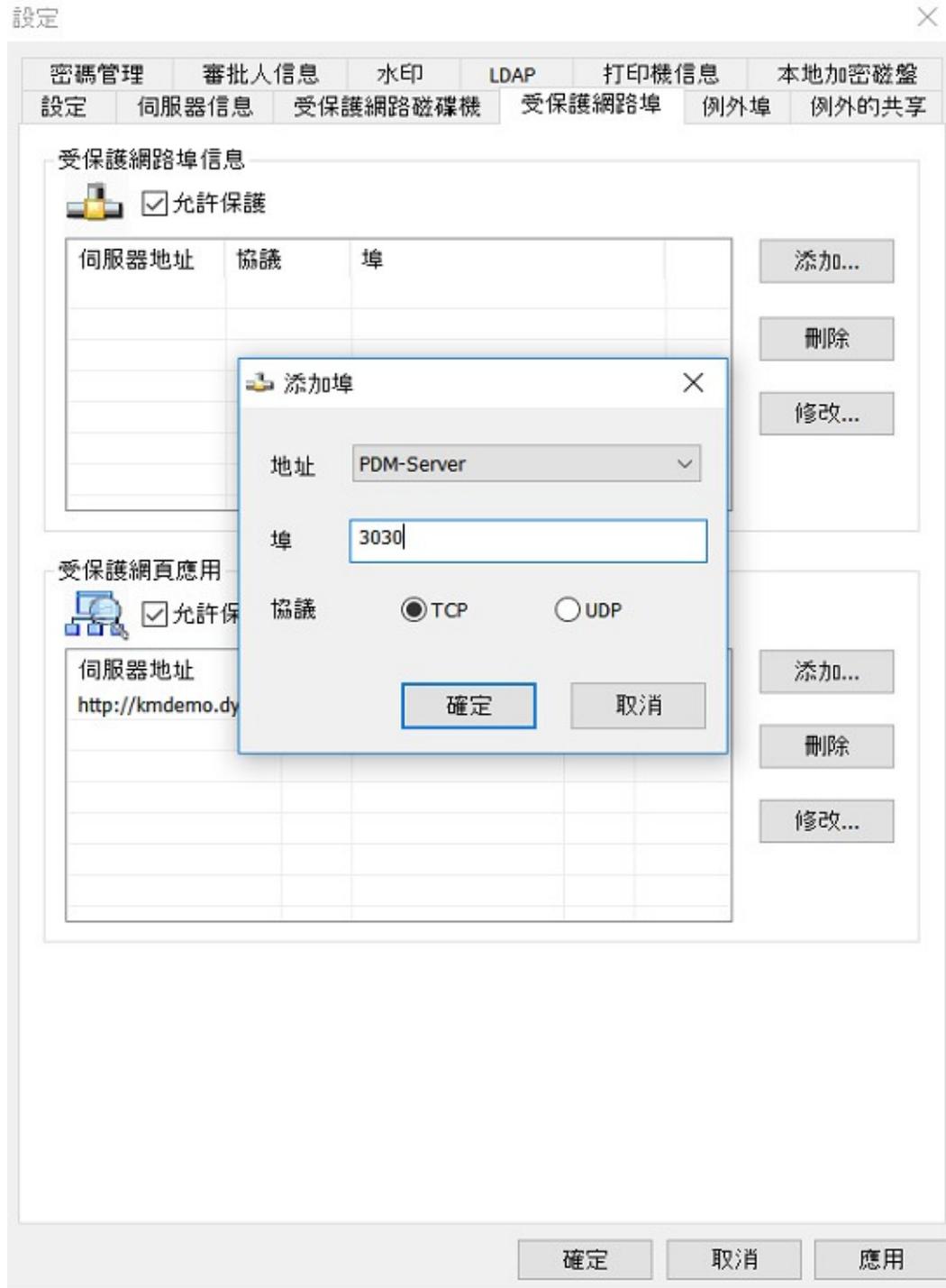
例子2 - IBM Lotus Quickr (如:http://Lotus Quickr服務器/Place)

- 管理員可以於Lotus Quickr上建立很多Place。如果管理員只想用Curtain e-locker來保護其中一些Place, 管理員可以於路徑上輸入完整Place的路徑(如:quickr/place1.nsf)。設置後, 用戶需要使用受保護的Internet Explorer瀏覽器來訪問受保護的Place, 所有在這個Place內的資料都被Curtain e-locker保護起來。

如果管理員想保護整個應用網站, 請輸入 "<PROTECTALL>"。

情況3 - 保護網路埠(用於SolidWorks PDMWorks)

- 於"受保護網路埠信息"，點選"允許保護"。
- 按"添加"按鈕，系統會彈出對話框。



- 地址 - 選擇服務器(電腦名稱或IP地址)
- 埠 - 輸入埠(PDMWorks的默認值是3030)
- 協議 - 選擇協議(PDMWorks的默認協議是TCP)

4. 按確定鍵確認

5.7 - 保護共享文件夾下的子文件夾

舉例：文件伺服器上有一個共用文件夾pro（根目錄），下面分別有pro1, pro2, pro3 ... pro9共9個子文件夾（子目錄）。假如目前僅需要保護3個子文件夾即pro1, pro2, pro3，其他的子文件夾不用受Curtain e-locker保護，那麼如何來實現這一需求？

方法一：

在文件伺服器上，把那些需要保護的子文件夾設定為共享文件夾（即是pro1, pro2, pro3），並且於Curtain管理端"受保護網路磁碟機"內設定為受保護的共享文件夾。

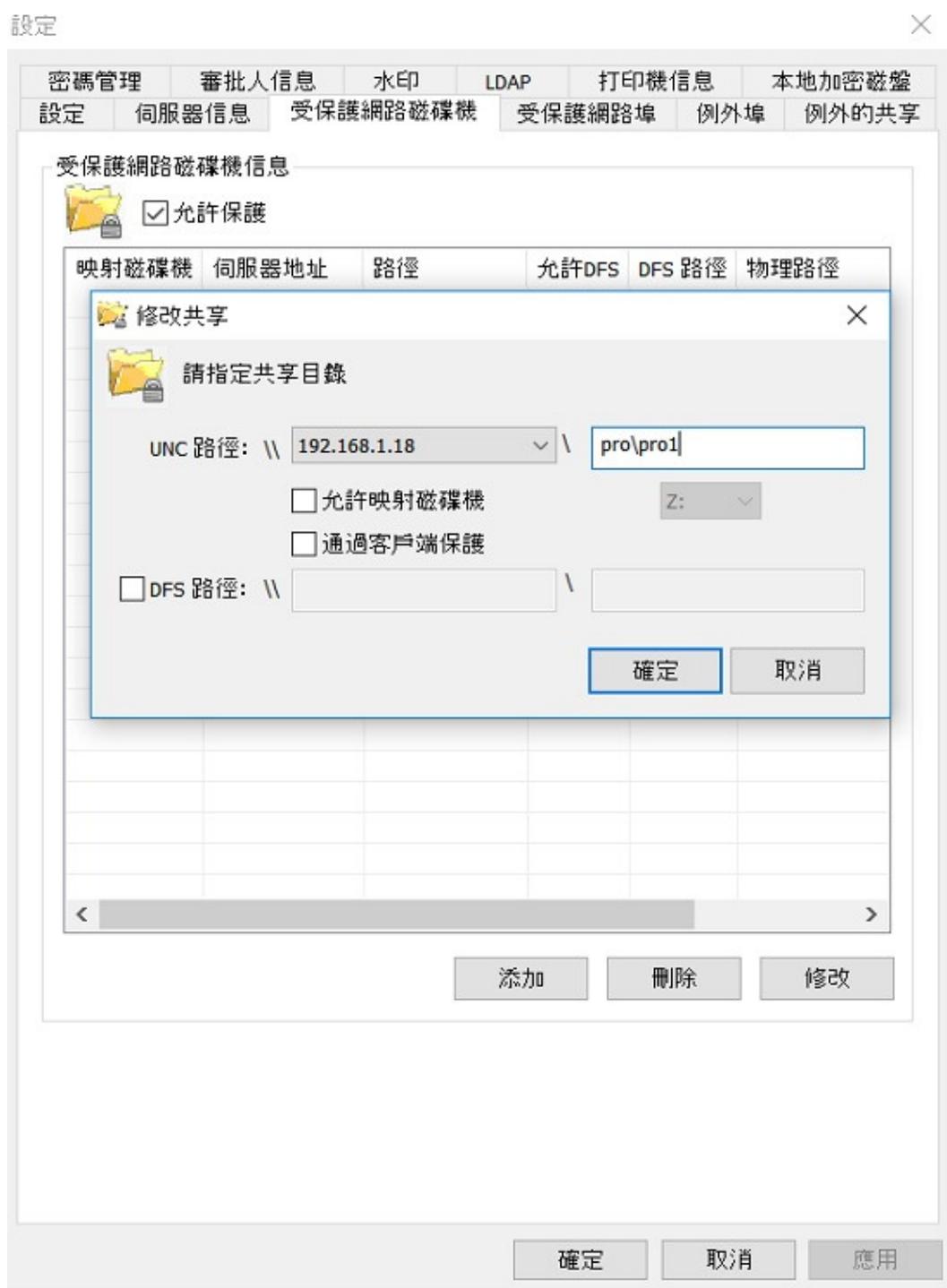
方法二：

不用於文件伺服器上把那些需要保護的子文件夾設定為共享（即是pro1, pro2, pro3），只需要於Curtain管理端"受保護網路磁碟機"內直接將子文件夾設定為受保護即可，請參考以下步驟。

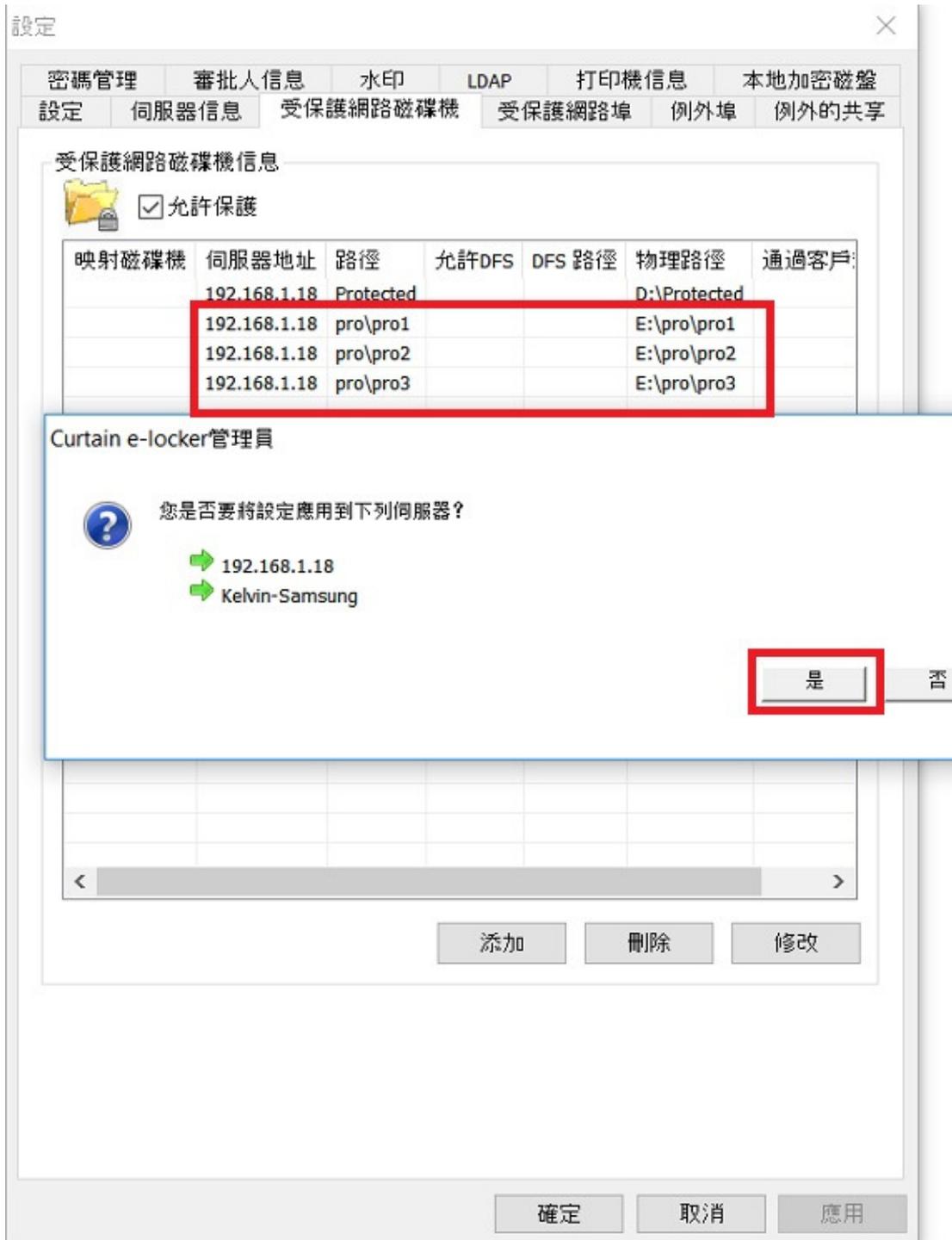
[直接將子文件夾設定為受保護的步驟:](#)

1. 在Curtain管理端，於菜單上選擇"文件>設定"。

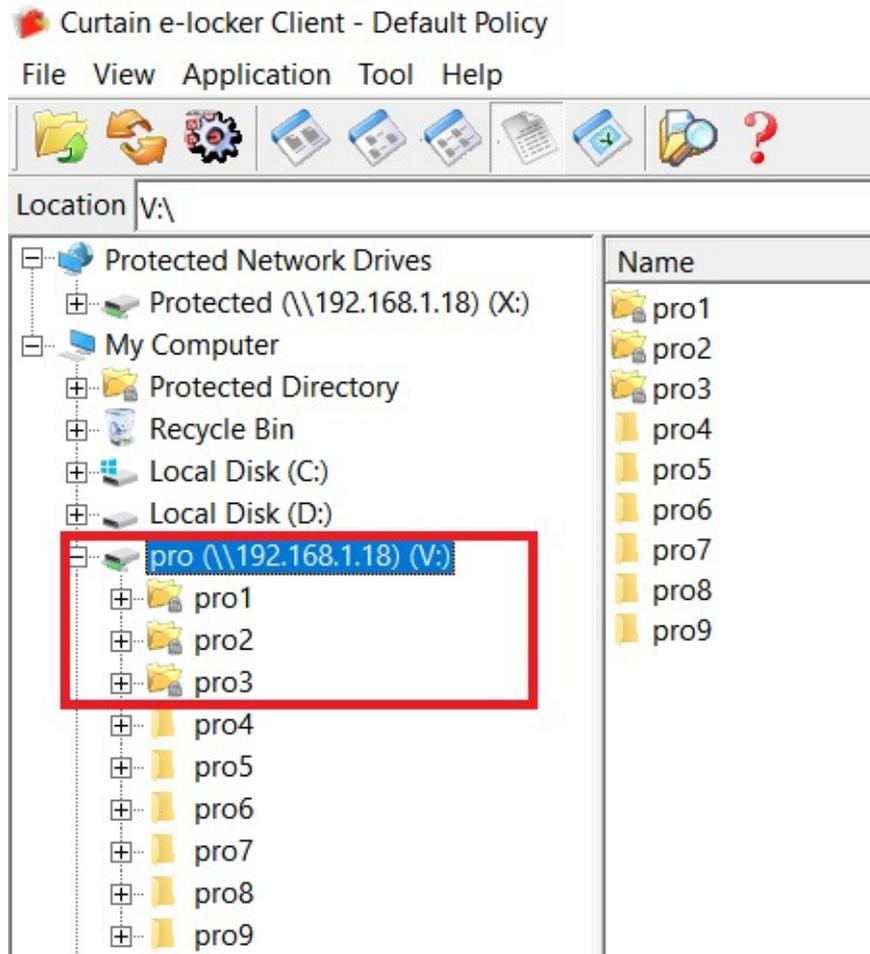
3. 然後依次序添加受保護的子文件夾路徑：（下圖為添加pro1示圖）。



4. 接著依次序添加完成pro2, pro3的保護路徑後，點擊“確定”，推送並完成該設置。



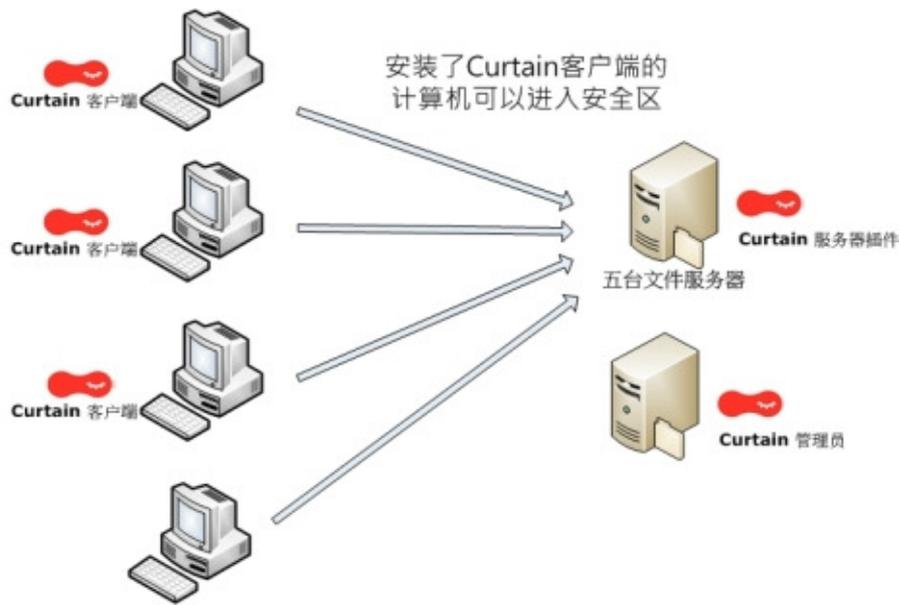
5. 於Curtain用戶端，共用文件夾pro在我的電腦下方顯示，其中帶鎖的3個子文件夾pro1, pro2, pro3為受保護的，而剩下的沒有帶鎖的pro4至pro10這幾個文件夾不受Curtain e-locker保護。



5.8 - 例外規則

5.8.1 - 例外規則

例外規則的功能一方面是為了方便用戶使用保護環境的同時，又不會影響特定條件下沒有安裝Curtain客戶端的電腦訪問安全區。如下圖所示架構，安裝了Curtain客戶端的電腦可以訪問安全區（即文件伺服器上的保護共享文件夾），而沒有安裝Curtain客戶端的電腦只能夠訪問非受控區（即文件伺服器上的普通共享文件夾）。有時候為了滿足用戶沒有安裝Curtain客戶端的電腦（如經理，老板，管理層的電腦不需要管控）同樣可以訪問安全區，那麼可以設置“例外規則”來實現這一需求。



沒有安裝Curtain客戶端的計算機只可以使用非機密資料

例外規則的功能另一方面是方便了用戶在現實環境中能夠兼顧測試環境一起使用而不受影響，從而達到預期測試的效果。舉例：公司研發部門正在使用EPDM系統，希望在現有工作環境中測試受e-locker保護的EPDM，其中抽出工程師A和B的電腦作為測試對象，那么在實施過程中A和B的電腦首先需要安裝Curtain客戶端，並且設置了“例外規則”保護，從而可以只針對這兩臺電腦測試受e-locker保護EPDM環境，那些沒有安裝e-locker客戶端的用戶電腦仍然可以正常使用EPDM系統工作。

保護規則類型共分為4種：全部保護，全部不保護，只對列表中的保護，除列表之外全部保護

- 全部保護：安裝環境中該規則類型為默認設置，即安裝了Curtain客戶端的電腦將會被保護並且可以自由使用受保護區內的文件而不會外泄，而沒有安裝Curtain客戶端的電腦訪問受保護的共享文件夾或者保護端口等行為時將會被禁止。
- 全部不保護：相當於停止e-locker的保護功能，即安裝了Curtain客戶端的電腦和沒有安裝Curtain客戶端的電腦都能夠訪問受保護的共享文件夾或者訪問受保護端口等，保護區內的文件和控制等行為都可以通過非受控區途徑來獲取或操作。
- 只對列表中的保護：顧名思義加入該列表裡面的電腦(以IP地址來設定)將會被保護起來，在列表外不管是安裝了或者沒有安裝Curtain客戶端的電腦都將被視為不保護。
- 除列表之外全部保護：加入到該列表裡面的電腦(以IP地址來設定)將不會被保護，而在列表外安裝了Curtain客戶端的電腦仍然受到保護和沒有安裝Curtain客戶端的電腦無法訪問保護區內的文件或者保護端口等行為。



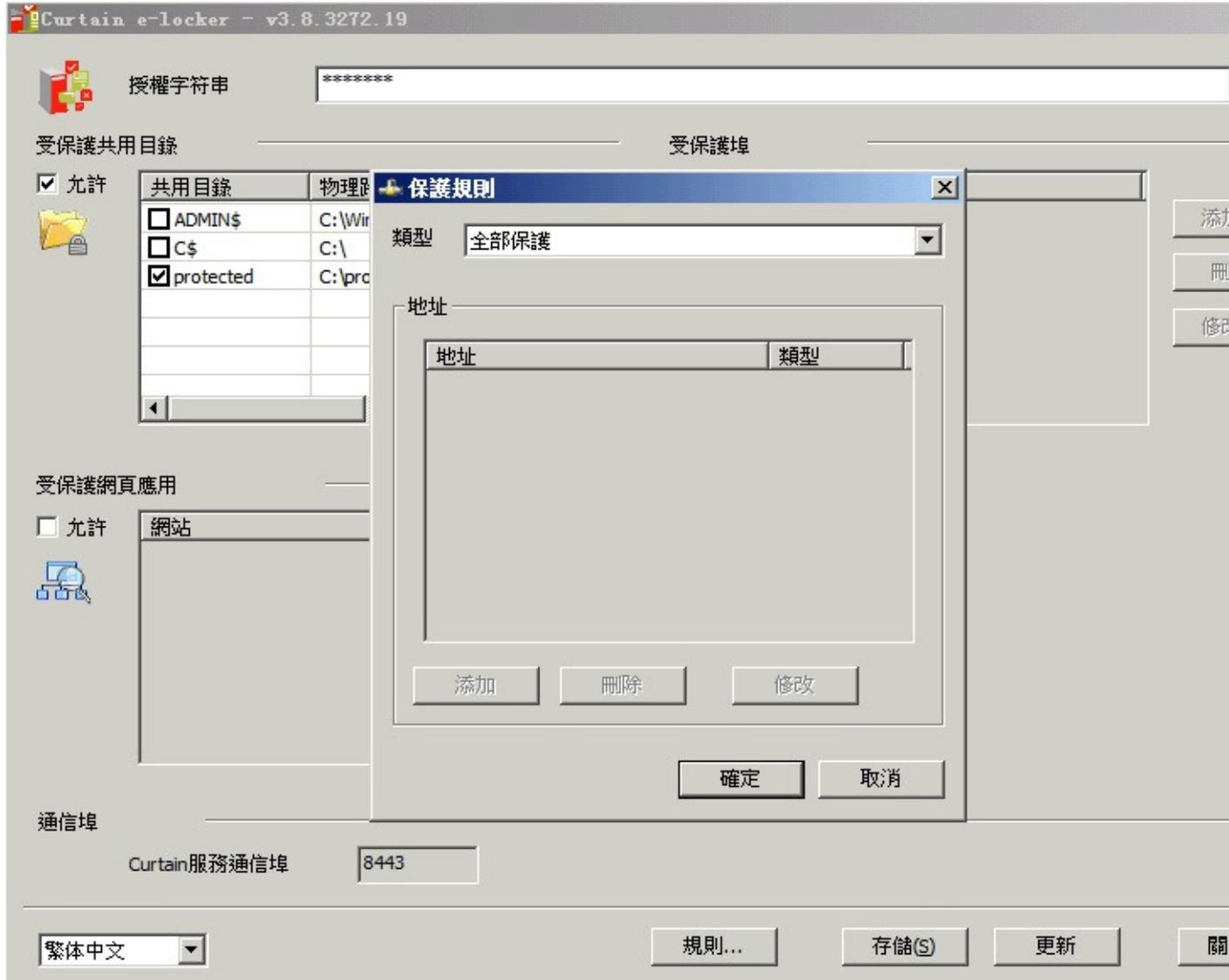
5.8.2 - 設置例外規則

例外規則的功能一方面是為了方便用戶使用保護環境的同時，又不會影響特定條件下沒有安裝Curtain客戶端的電腦訪問服務器上的安全區。因此，這功能是在Curtain服務器插件上設置的。

[設置例外規則的步驟:](#)

1. 在開始菜單欄里找到Coworkshop Curtain e-locker文件夾，并打開“安全網絡管理界面”。

2. 點擊“規則”選項，彈出保護規則一欄，選擇需要保護的規則類型。



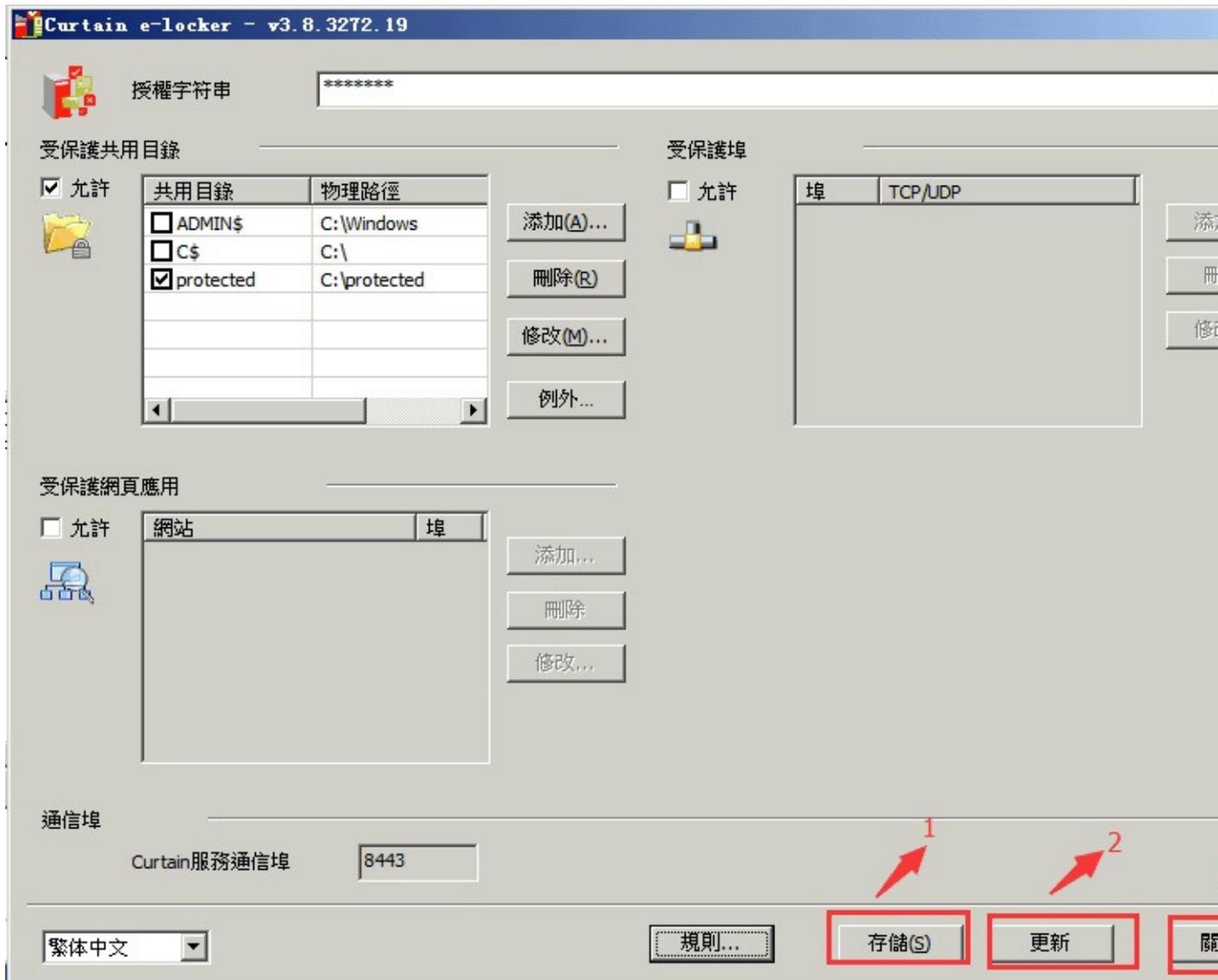
3. 如選擇“只對列表中的保護”或“除列表之外全部保護”，按“添加”輸入電腦的IP地址到列表中。

4. 選擇類型並輸入電腦的IP地址，可以選擇IP地址段添加或者指定一個IP地址，如192.168.0.1。



5. 然后點擊確定。

6. 然后在主界面依照順序保存，刷新，最后關閉三個步驟：



注意：當第三步“關閉”時會提示“是否需要重啟插件服務器”，在這裡可以點擊“NO”選擇不重啟。



7. 設置完成

5.9 - 暫時停止受保護區的保護

"停止受保護區的保護" 為管理員提供彈性，管理員可以暫時停止對某安全策略群組下的電腦/用戶的保護。因為使用此功能時客戶端將不受保護，有機會導致敏感文檔的外泄，因此一般情況不推薦使用。但是在某些情況下管理員需要暫時停止e-locker的保護，管理員可以預先創建一個安全策略群組並啟動此功能(停止保護)，在有需要時就可以將電腦/用戶指派到此安全策略群組中。

啟動"停止受保護區的保護"的步驟：

1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵，並選擇"內容"。



2. 選擇 "停止對受保護區的保護" 。



3. 然後單擊 "確定" 。

當電腦/用戶被暫時停止保護時，於Curtain客戶端的標題會顯示FULL ACCESS，如下圖。



4. 完成。

6 - 其他功能

6.1 - 保護文件初稿

保護文件初稿這個功能，是用作保護新建立的文檔。當此功能啟動後，用戶必需要將新建立的文檔保存在受保護區之內，Curtain e-locker確保機密文檔從一開始便受到嚴密的保護。

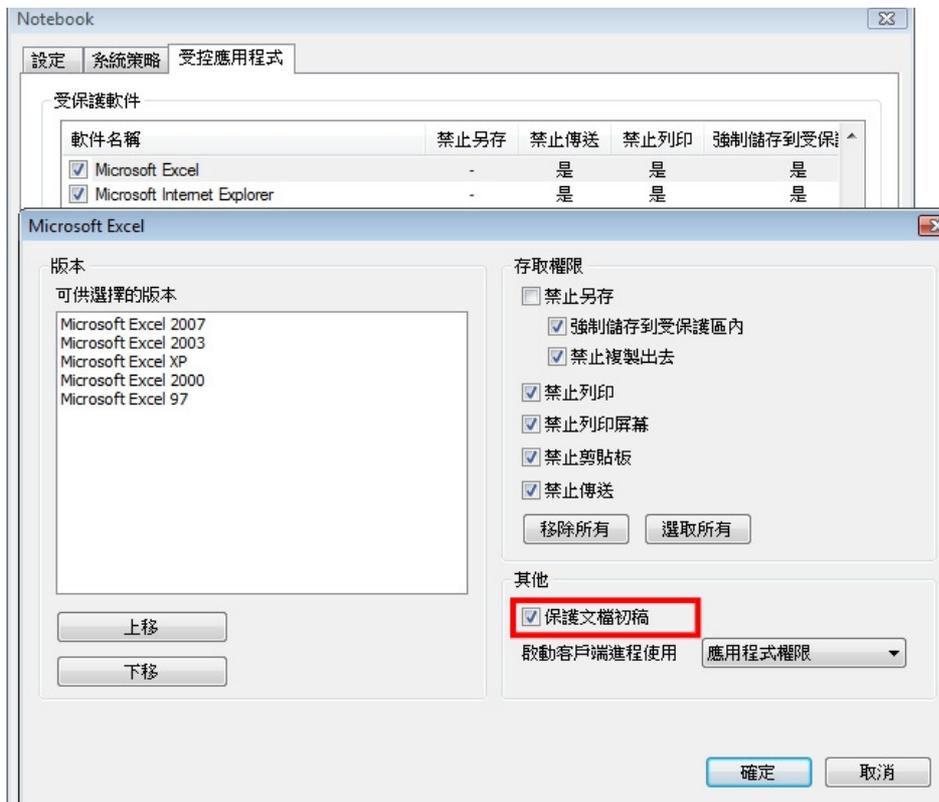
這功能可以針對個別安全策略群組和應用軟件來啟動的。以下是使用此功能的例子。
- 限制工程師只可以將所有新建立的AutoCAD和Photoshop文檔保存在受保護區之內。

為個別應用軟件啟動"保護文件初稿"的步驟:

1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵，並選擇"內容"。
2. 於"受控應用程式"頁，雙擊你想啟動"保護文件初稿"的應用軟件。
3. 選擇"保護文件初稿"，並按確定鍵確認。

"啟動客戶端進程使用> 應用程式權限" - 此選項被選取時，代表保護文件初稿只針對此應用程式。

"啟動客戶端進程使用> 父進程權限" - 此選項被選取時，代表保護文件初稿會保護此應用程式及其所有子進程(如: 從AutoCAD下開啟的Excel程式)。



備註: 當個別應用軟件的"保護文件初稿"已被啟動(如:MS Excel)，代表該應用軟件只容許在Curtain控制下使用。在這個例子，用戶不能開啟非受控的Excel，如果他們嘗試開啟非受控的Excel，Curtain e-locker會自動將該應用軟件關閉。用戶只可以開啟受控的Excel來建立新的文檔，所有新的Excel文檔只可以保存到Curtain保護區之內(故此這功能稱之為"保護文件初稿")。對於在非受保護區下的文檔，用戶必需要先將文檔複製到保護區之內才能打開，可以用複製粘貼或拖拉的方法將文檔移到保護區之內。

6.2 - 在線/離線保護

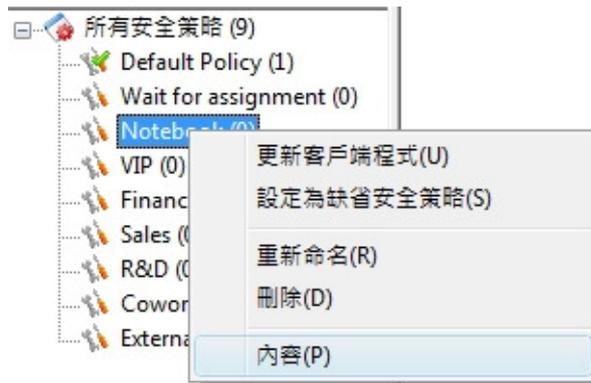
在線/離線保護是一個控制用戶使用已下載文檔的功能。

此功能的主要目的:

- 當電腦離開公司後(意思是指當電腦不能連接Curtain管理員), 公司不想用戶繼續使用已被下載到本地受保護區內的機密文檔。

啟動"在線/離線保護"功能的步驟:

1. 在Curtain管理員, 點選一個安全策略, 按滑鼠右鍵, 並選擇"內容"。

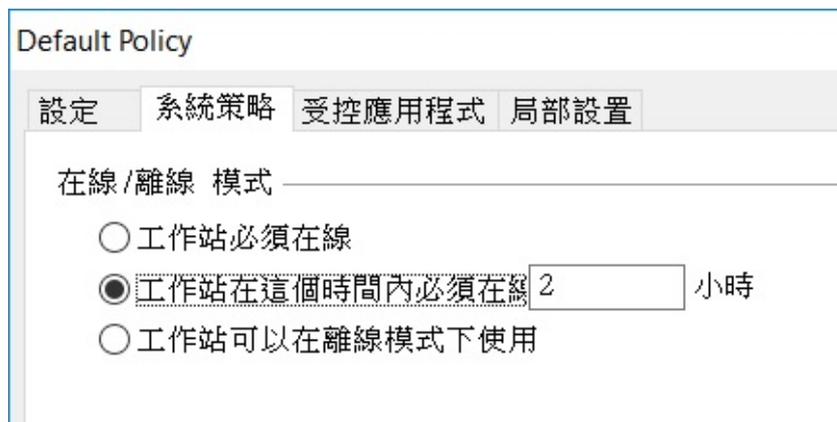


2. 於"系統策略"頁的"在線/離線模式"下, 有3個選項。

"工作站必需在線" - 此選項被選取時, 如果用戶電腦不能連接Curtain管理員, 用戶是不能開啟Curtain客戶端的。

"工作站在這個時間內必需在線[]小時" - 此選項被選取時, 如果用戶電腦超過指定的時間內依然不能連接Curtain管理員, 用戶是不能開啟Curtain客戶端的。

"工作站可以在離線模式下使用" - 此選項被選取時, 無論用戶電腦能不能連接Curtain管理員, 用戶依然可以開啟Curtain客戶端的。



6.3 - 自動清理

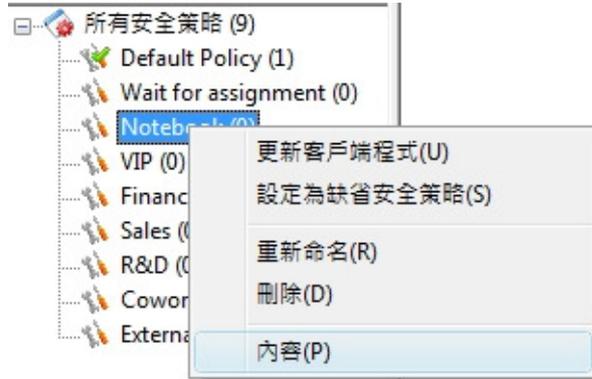
“自動清理”是一個自動清除用戶電腦上本地受保護區內文檔的功能。

此功能有兩個主要用途：

- 不希望用戶永久保存文檔在本地受保護區中。
- 清理本地受保護區中的緩存、臨時文檔和回收站，以釋放磁盤空間。

啟動“自動清理”功能的步驟：

1. 在Curtain管理員中，選擇一個安全策略，然後右鍵單擊並選擇“內容”。



2. 選擇清理本地受保護區的方式，然後單擊“確定”按鈕進行確認。

自動清理

<input type="checkbox"/> 清理本地受保護區 <input checked="" type="radio"/> 啟動 <input type="radio"/> 每週 日 一 二 三 四 五 六 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> 清理本地受保護區暫存目錄 <input checked="" type="radio"/> 啟動 <input type="radio"/> 每週 日 一 二 三 四 五 六 <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
<input type="checkbox"/> 清理本地受保護區內文檔 <input type="checkbox"/> 下載后刪除文檔 0 天 <input type="checkbox"/> 修改后刪除文檔 0 天 刪除文檔如 所有 符合	<input type="checkbox"/> 清理本地受保護區內回收站文件 <input type="checkbox"/> 刪除后永久刪除 10 天

“清理本地受保護區” - 如果選擇此選項，本地受保護區內的所有文檔將被刪除。

啟動 - 如果選擇此選項，系統會於用戶電腦每次啟動時，自動進行清理工作。

每週 - 如果選擇此選項，系統會於用戶電腦在選定的日子啟動時，自動進行清理工作。

“清理本地受保護區暫存目錄” - 如果選擇此選項，本地受保護區內的所有臨時文檔將被刪除。

啟動 - 如果選擇此選項，系統會於用戶電腦每次啟動時，自動進行清理工作。

每週 - 如果選擇此選項，系統會於用戶電腦在選定的日子啟動時，自動進行清理工作。

“清理本地受保護區內文檔” 基於下載日期和/或修改日期 - 如果選擇此選項，本地受保護區內符合準則（即下載日期和/或修改日期）的所有文檔將被刪除。

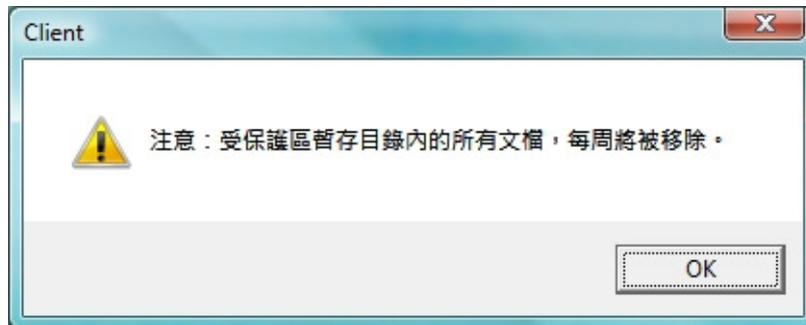
下載[]天後刪除文件 - 如果選擇此選項，下載日期超過指定天數的本地受保護區文檔將被刪除。

修改[]天後刪除文件 - 如果選擇此選項，最後修改日期超過指定天數的本地受保護區文檔將被刪除。

“清理本地受保護區內回收站文件”基於刪除日期 - 如果選擇此選項，回收站內符合準則（即刪除日期）的所有文檔將被刪除。

刪除[]天後刪除文件 - 如果選擇此選項，刪除日期超過指定天數的回收站文檔將被刪除。

如果啟動了自動清除功能，則每次啟動Curtain客戶端時系統都會提示用戶。



6.4 - 截屏控制

Curtain e-locker很聰明地處理截屏這個功能:

- 使用截屏時，系統會聰明地將顯示敏感資料的窗口變成灰色;
- 對於普通的資料，用戶依然可以利用截屏功能帶來的方便;
- 截屏軟件同樣被系統堵住。



6.5 - 智能複製粘貼控制

Curtain e-locker很聰明地處理複製粘貼上這個功能:

- 在受保護區的文檔之間複製粘貼上是容許的;
- 從受保護區以外複製資料並粘到受控文檔內也是容許的;
- 但是，從受控文檔內複製資料並粘到受保護區以外是受Curtain e-locker控制的，如果沒有授權是絕對不容許的。

這方法既不影響正常操作，亦可以確保資料的安全，Curtain e-locker在方便性和資料保安之間取得很好的平衡。

6.6 - 安全生成PDF文檔

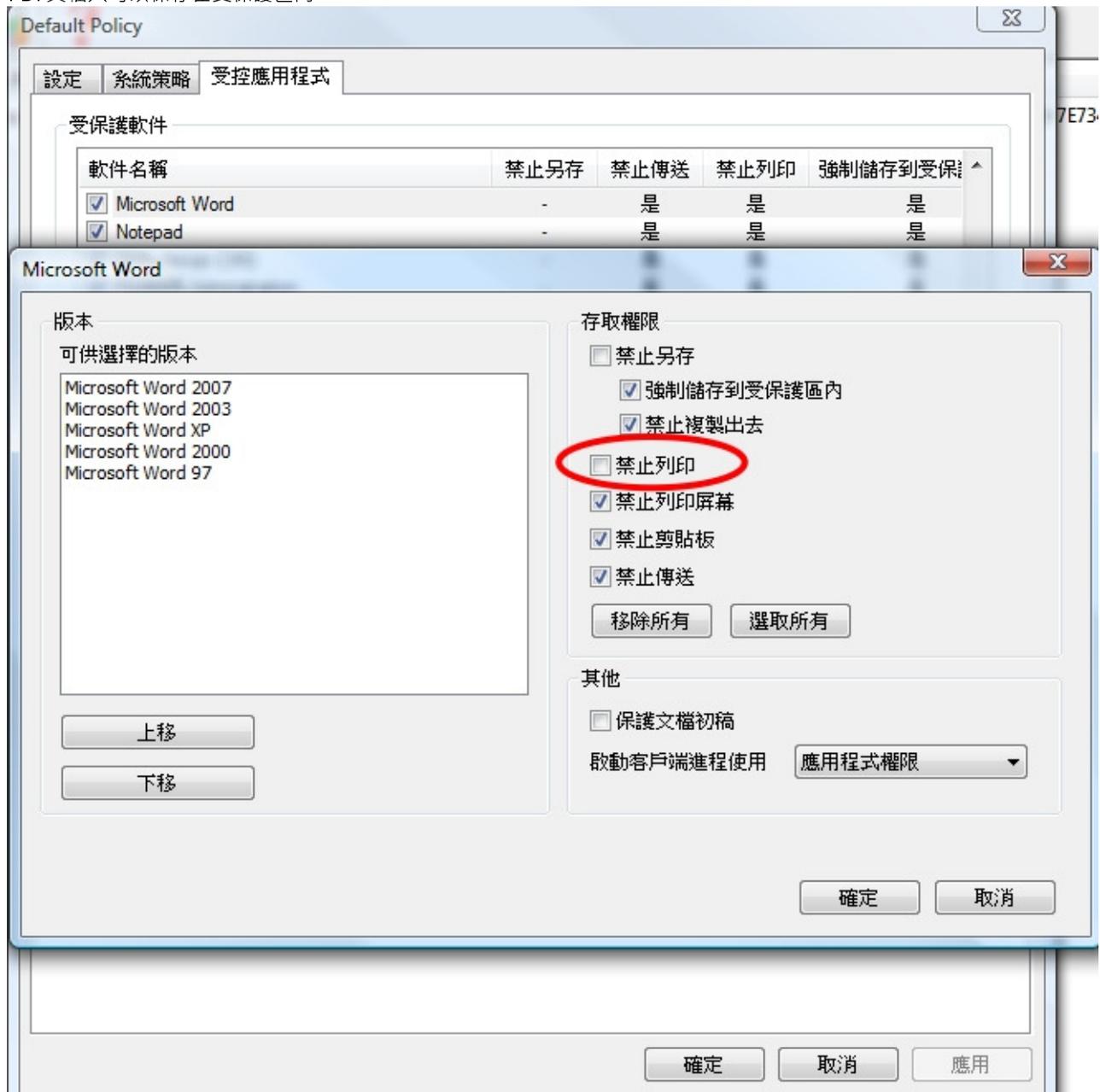
"安全列印成PDF文檔"這個功能容許用戶將敏感資料以"列印成PDF"的方法，將文檔轉成PDF格式，而又不構成資料外洩的問題。

此功能的主要目的:

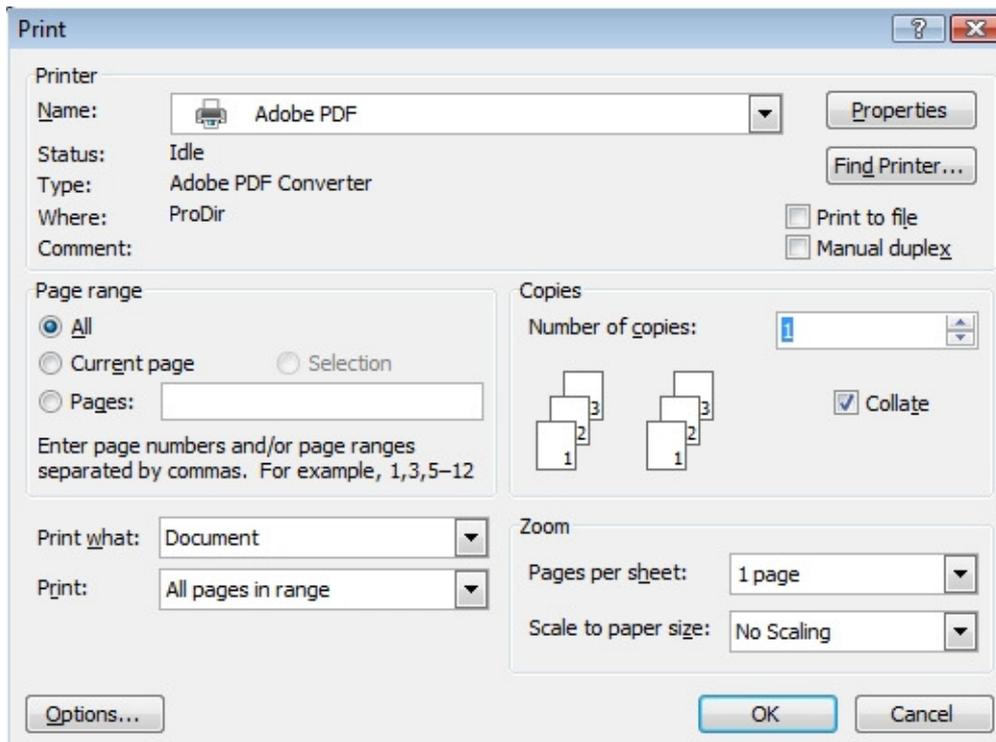
- 用戶可以將敏感資料以"列印成PDF"的方法，將文檔轉成PDF格式。但生成的PDF文檔只可以保存在受保護區內。此功能在方便性和保護機密資料中間取得很好的平衡。用戶可以將文檔轉換成PDF格式的時，機密資料又不能被帶走。

例子: 容許用戶將受保護的Word文檔轉成PDF格式

如果管理員容許用戶將受保護的Word文檔(即是在受保護內的Word文檔)轉成PDF格式，管理員應該先在Word的安全策略上容許"打印"。設定後，用戶便可以打印受保護的Word文檔，並將它們轉成PDF格式。所有生成的PDF文檔只可以保存在受保護區內。



先容許用戶打印Word文檔



以"列印成PDF"的方法，將文檔轉成PDF格式

6.7 - 與其他人分享受保護文件

一般來說，有三種不同的權限級別：

- (情況1) 用戶被授權可以加密並將加密文檔保存到保護區之外。這些文檔只能在受保護區域中被解密。
- (情況2) 用戶被授權可以加密並將加密文檔保存到保護區之外。只需輸入正確密碼就可以在任何地方解密文檔。
- (情況3) 用戶有權儲存/發送/複製文檔到保護區之外（沒有加密文檔）。但這些文檔不再受Curtain e-locker保護。

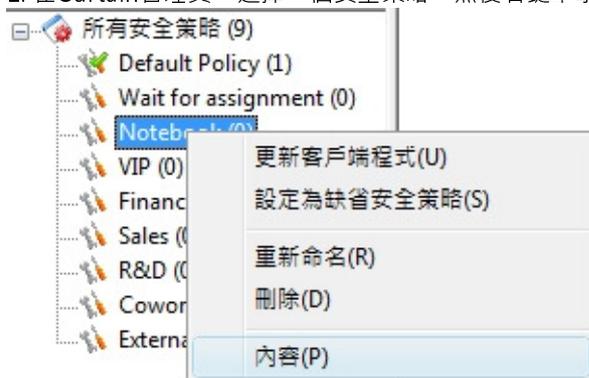
情況 1 - 加密（僅由客戶端解密）：

此功能對於用戶在公司內共享受保護的文檔是非常有用的。因此，你可以將此功能授予大多數用戶。

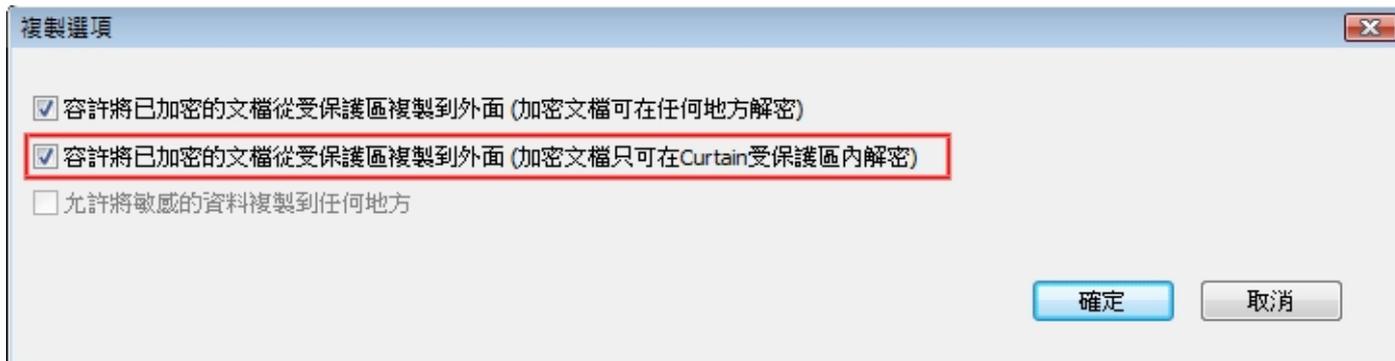
如果用戶被允許加密（僅由客戶端解密），用戶可以加密受保護的文檔，並與其他人分享加密的文檔。當其他用戶收到文檔時，他們的電腦必須安裝Curtain 客戶端（並屬於同一台Curtain管理員）。用戶可以雙擊文檔進行解密。文件將自動解密到本地保護區內。

授予“加密（僅由客戶端解密）”權限的步驟：

1. 在Curtain管理員，選擇一個安全策略，然後右鍵單擊以選擇“內容”。

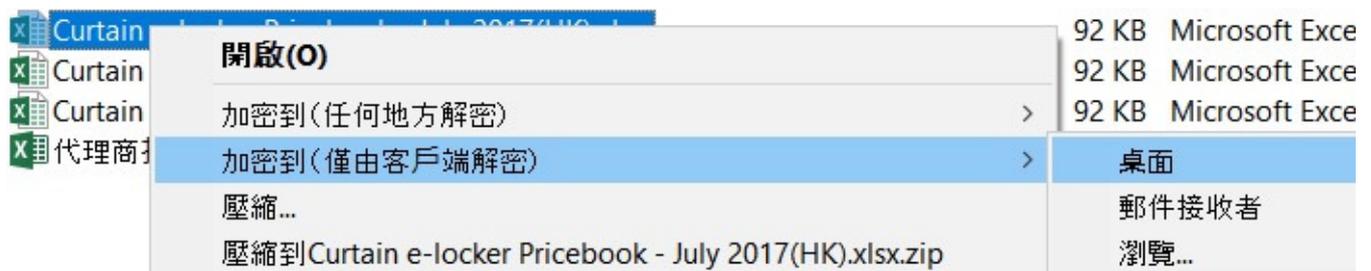


2. 點擊“複製選項”按鈕，選擇如下圖所示的第二個選項，單擊“確定”。

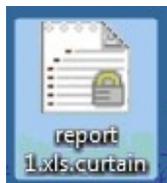


與其他人士分享加密文檔的步驟：

1. 在Curtain客戶端，選擇受保護的文檔，然後右鍵單擊選擇“加密到（僅由客戶端解密）”。然後加密的文檔將被複製到選擇的位置。



2. 將加密文檔發送給其他人。由於文檔被加密，文檔在傳送過程中（例如：USB盤或電子郵件）是非常安全的。



3. 當用戶收到文檔時，用戶只需雙擊該文檔即可。它將被解密到本地受保護區內。

情況 2 - 加密（任何地方解密）：

實際上用戶只需輸入正確密碼後就可以獲取文檔。因此，此功能只能授予授權用戶。

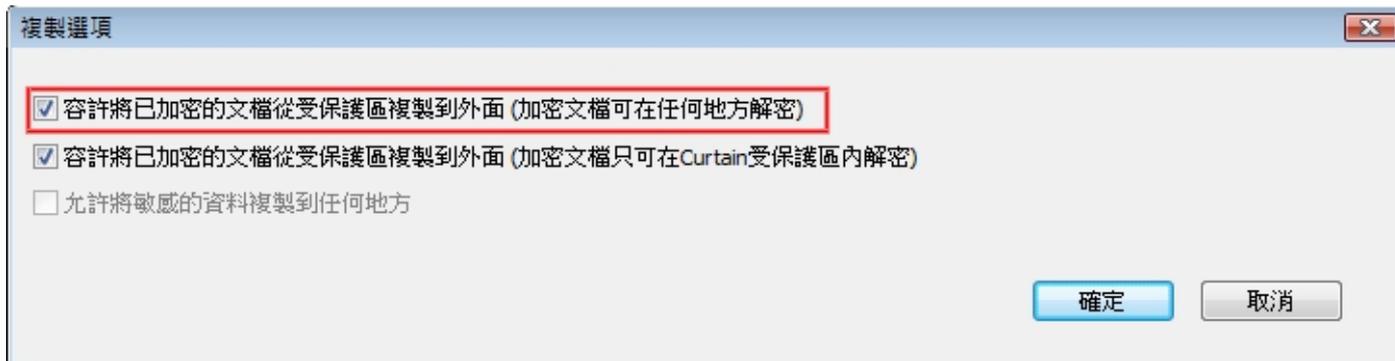
如果用戶被允許加密（任何地方解密），用戶可以使用密碼加密受保護的文檔，並與其他人士分享加密的文檔。當其他用戶收到文檔時，他們可以輸入正確的密碼對文檔進行解密。

備註：解密不需要Curtain客戶端的。文檔成功解密後，Curtain將不再保護文檔。

授予“加密（任何地方解密）”權限的步驟：

1. 在Curtain客戶端，選擇一個安全策略，然後右鍵單擊以選擇“內容”。

2. 單擊“複製選項”按鈕，選擇如下圖所示的第一個選項，然後單擊“確定”。

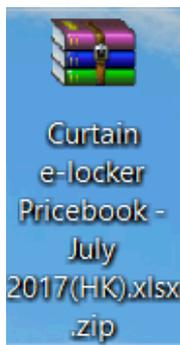


與其他人士分享密碼加密文檔的步驟：

1. 在Curtain客戶端，選擇受保護的文檔，然後右鍵單擊，並選擇“加密到（任何地方解密）”。
2. 設置密碼後單擊確定，加密文檔將被複製到選擇的位置。



3. 將密碼加密的文檔發送給他人。由於文檔被加密，文檔在傳送過程中（例如：USB盤或電子郵件）是非常安全的。



4. 當用戶收到文檔時，用戶只需雙擊該文檔即可。用戶輸入正確密碼後，文檔將被解密到選擇的位置。

情況 3 - 拷走原文檔 (沒有加密文檔) :

當某些用戶需要頻繁地與外面分享受保護文檔，又或者你不需要控制他們使用受保護文檔時，你可以允許他們將受保護的文檔儲存到受保護區之外，而無需加密文檔。此功能只能授予授權用戶。

有關設置方法，請參閱FAQ00084或“安裝指南”中的第5.2節。

如果允許用戶可以將文檔以“儲存到任何地方/發送/複製文檔到任何地方”拷走，用戶就可以與其他人分享未加密的文檔（原文檔）。由於文檔未加密，用戶可以不受Curtain保護下使用文檔。“儲存到任何地方/發送/複製文檔到任何地方”這三個控制的主要分別在於Curtain可以將“發送/複製文檔到任何地方”作日誌記錄。但是，“儲存到任何地方”是沒有日誌記錄的。

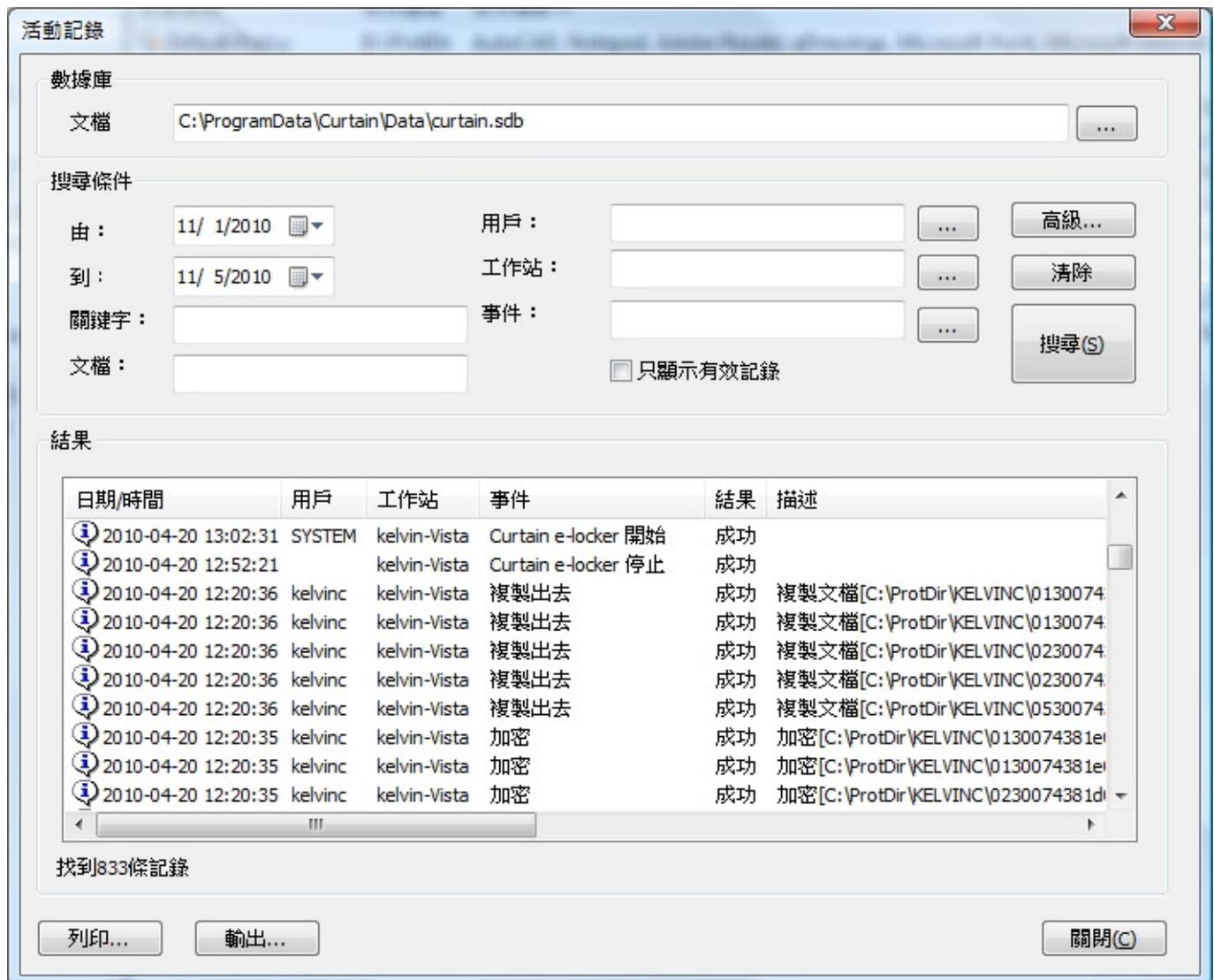


6.8 - 活動記錄

有的，Curtain e-locker是有活動記錄的。

[查看活動記錄的步驟:](#)

1. 開啟Curtain管理員。
2. 於工具列上按"活動記錄"按鈕，或於菜單上選擇"檔案>活動記錄"。接著，系統會顯示活動記錄。



3. 如果有記錄到打印內容，可以雙擊記錄查看打印內容(快照)。

活動記錄

數據庫
文檔: C:\ProgramData\Curtain\Data\curtain.sdb

搜尋條件

由: 19/ 1/2012 用戶:
到: 19/ 1/2012 工作站:
關鍵字: 事件:
文檔: 結果:

結果

日期/時間	用戶	工作站	事件
2012-01-19 14:25:13	kelvinc	kelvin-Vista	列印
2012-01-19 14:24:52	kelvinc	kelvin-Vista	啟動
2012-01-19 14:24:40	kelvinc	kelvin-Vista	啟動
2012-01-19 14:22:58	kelvinc	kelvin-Vista	列印
2012-01-19 14:22:25	kelvinc	kelvin-Vista	啟動
2012-01-19 14:22:06	kelvinc	kelvin-Vista	啟動
2012-01-19 13:10:10	kelvinc	kelvin-Vista	複製出去
2012-01-19 13:10:03	kelvinc	kelvin-Vista	複製出去
2012-01-19 13:09:56	kelvinc	kelvin-Vista	啟動
2012-01-19 13:09:49	kelvinc	kelvin-Vista	啟動

找到144條記錄

列印... 輸出...

列印

基本信息

日期: 2012-01-19
時間: 14:25:13
用戶: kelvinc
電腦名稱: kelvin-Vista
事件: 列印
結果: 允許

附加信息

應用程式: C:\Program Files\Microsoft Office\OFFIC
文件名: Microsoft PowerPoint - Curtain e-locker P
頁數: 3
打印機: Adobe PDF

打印內容

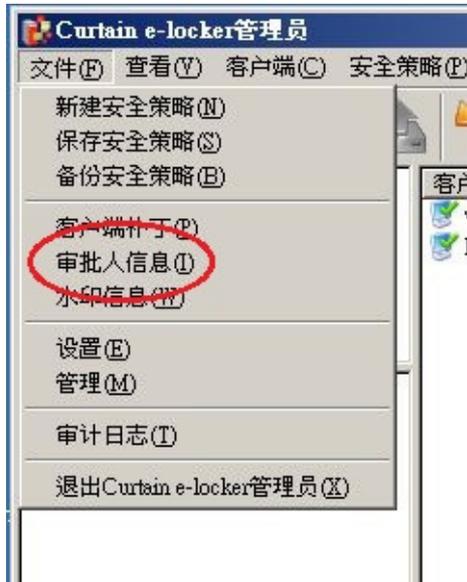
[第1頁](#)
[第2頁](#)
[第3頁](#)

6.9 - 外發申請

如果用戶需要將受控文件拿出受保護區給公司以外的人使用，而用戶又沒有此權限時，用戶可以使用 "外發申請"，如果審批人批准有關申請，該文件會以電郵形式發送給申請人，由於該文件已經離開了受保護區並且沒有加密，申請人可以轉發給公司以外的人使用而不受e-locker控制。整個審批過程都會記錄在活動記錄中。

設定審批人的步驟:

1. 在Curtain管理員，於菜單上選擇"檔案> 審批人信息"。



2. 按"添加"按鈕來新增審批人。
 - 輸入審批人姓名、電郵、職位
 - 在Windows用戶名，輸入"電腦名\用戶名" 或 "域名\用戶名" (如: M32w2k8-PC\Administrator 和 Curtain\Tester)



備註: 審批人和申請人的電腦必需安裝Curtain客戶端才可以提交或批准申請。

提交申請的步驟:

1. 在Curtain客戶端，點選一個或多個文件，按滑鼠右鍵，並選擇"外發申請"。



備註:

- 不支持文件夾操作
- 支持多個文件 (按Ctrl鍵選擇多個文件)

2. 填寫申請人，郵箱以及申請原因等信息，並選擇審批人。

The '外发申请' dialog box has the following fields and content:

- 申请文件:** C:\ProtDir\ADMINISTRATOR\testing.doc
- 申请人 *:** Lily
- 申请人邮箱 *:** lily@coworkshop.com
- 申请原因:** 外发
- 选择审批人 *:** A table with columns: 审批人姓名, 邮箱, Windows用..., 职位, 说明. The first row is selected: tester, tester@co..., M32XP\adm..., tester, 123.

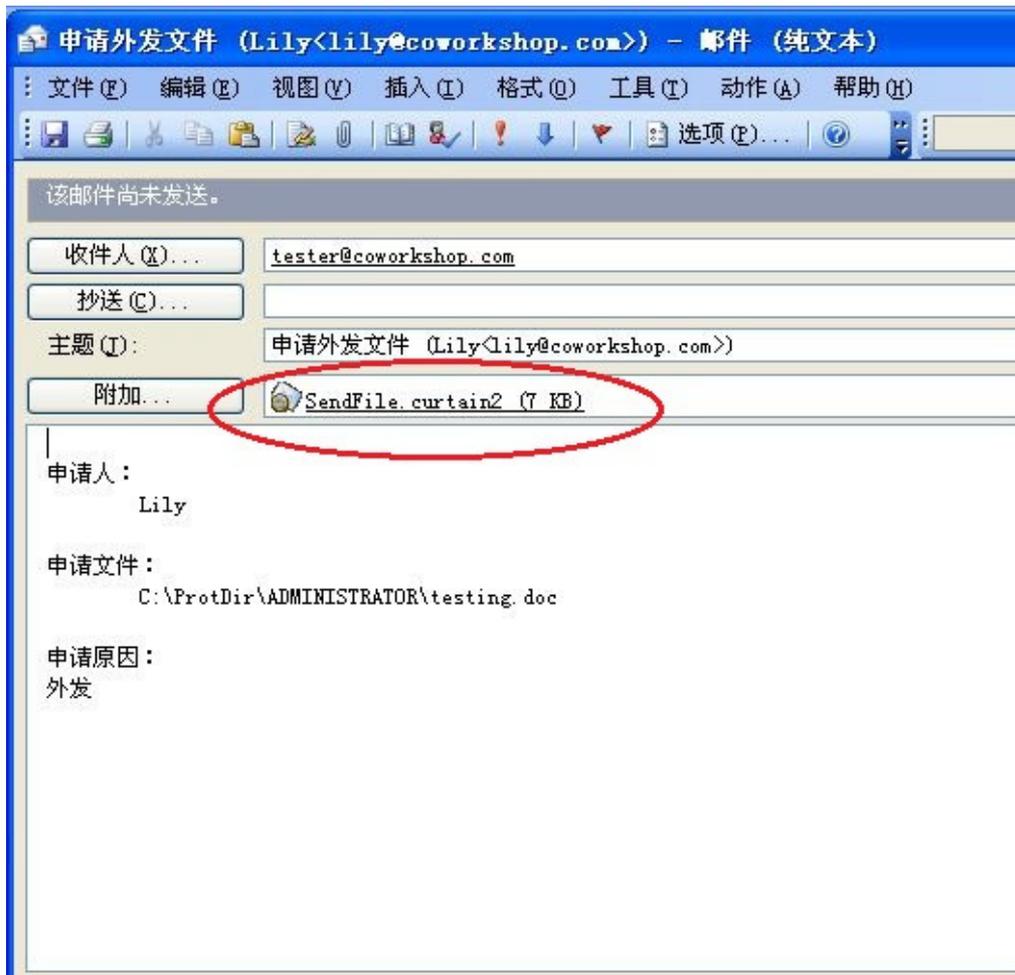
Buttons: OK, Cancel

3. 完成後按確定鍵確認。

系統會使用你預設的電郵客戶端新增一份草稿，並自動附加一個附件(文件名為SendFile.curtain2)，用戶可以簡單地按 "發送" 來將申請發送到審批人。現時Curtain支持Microsoft Office Outlook、Outlook Express和Windows Mail。

允許/拒絕申請的步驟:

1. 當審批人收到該電郵時，審批人可以雙擊附件(檔案名為"SendFile.curtain2")來審批有關申請。審批人可查看申請原因，申請人名，申請文件等，若要查看文件內容，單擊該文件名即可打開，此時的文件不受Curtain保護。



系統會對比當前Windows用戶以確認審批人身份，如當前用戶跟記錄不一樣，則不能打開"SendFile.curtain2"檔案。

2. 選擇允許或拒絕，並輸入意見(如適用)。

外发审批

申请信息

审批人: tester (tester@coworkshop.com)

申请人: Lily (lily@coworkshop.com)

申请时间: 2012/05/02 14:23:07

申请原因: 外发

文件列表

全部允许 全部拒绝

文件路径	允许	拒绝
testing.doc	<input checked="" type="radio"/>	<input type="radio"/>

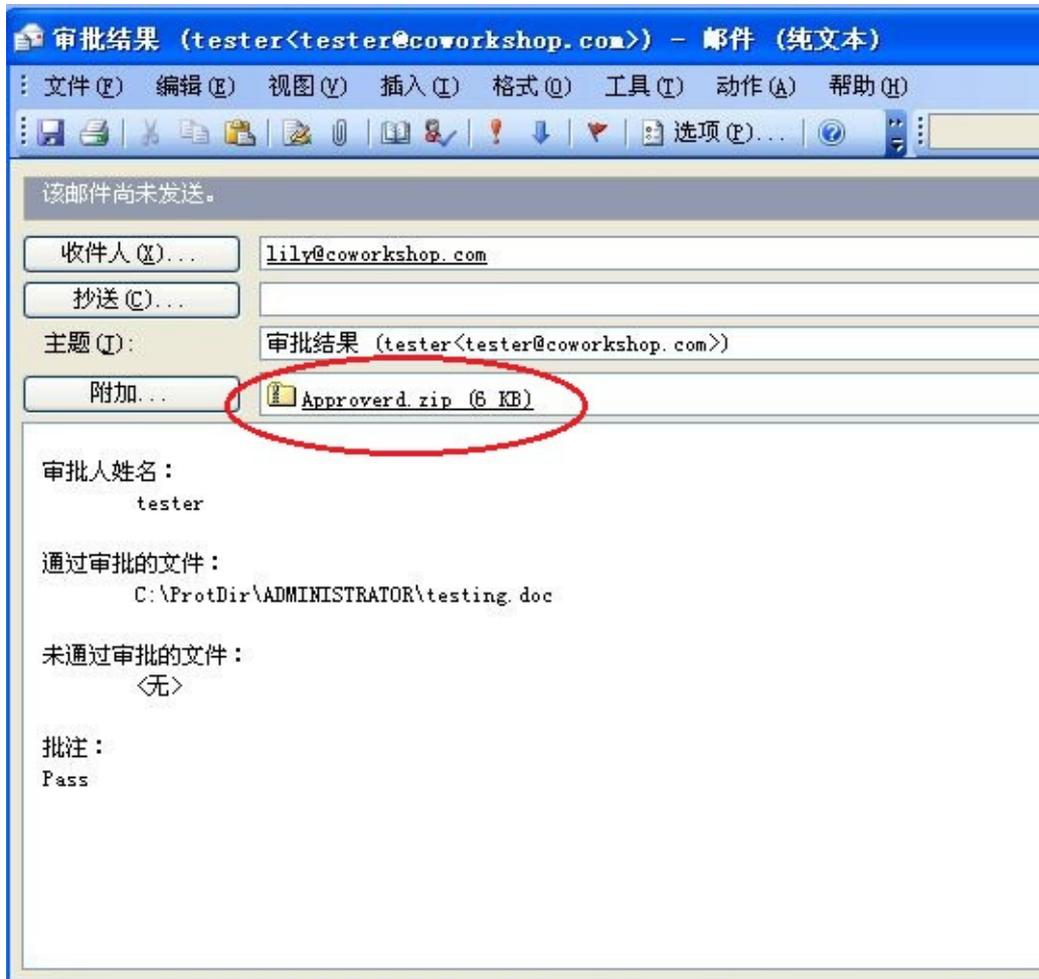
批注

Pass

确定 取消

3. 按確定鍵確認。

系統會使用預設的電郵客戶端新增一份草稿，如果審批人批准有關申請，系統會並自動附加一個附件(文件名為 Approved.zip)，審批人可以簡單地按 "發送" 來回覆申請人。由於該文件已經離開了受保護區並且沒有加密，申請人可以轉發給公司以外的人仕使用而不受e-locker控制。

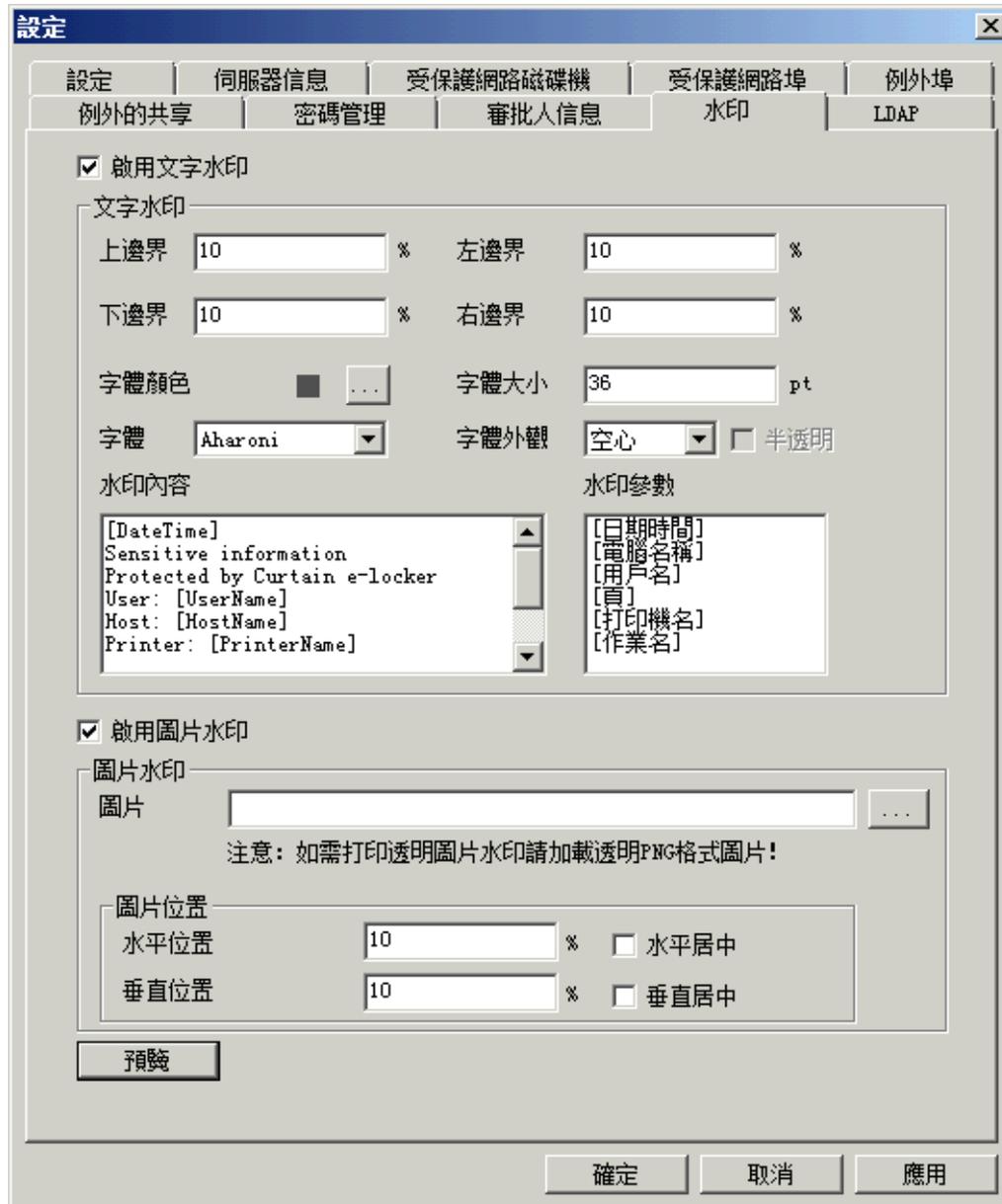


6.10 - 附加水印

如果你在打印文件時加上水印，你可使用此功能，水印分別有文字水印和圖片水印。

設定"水印"的步驟:

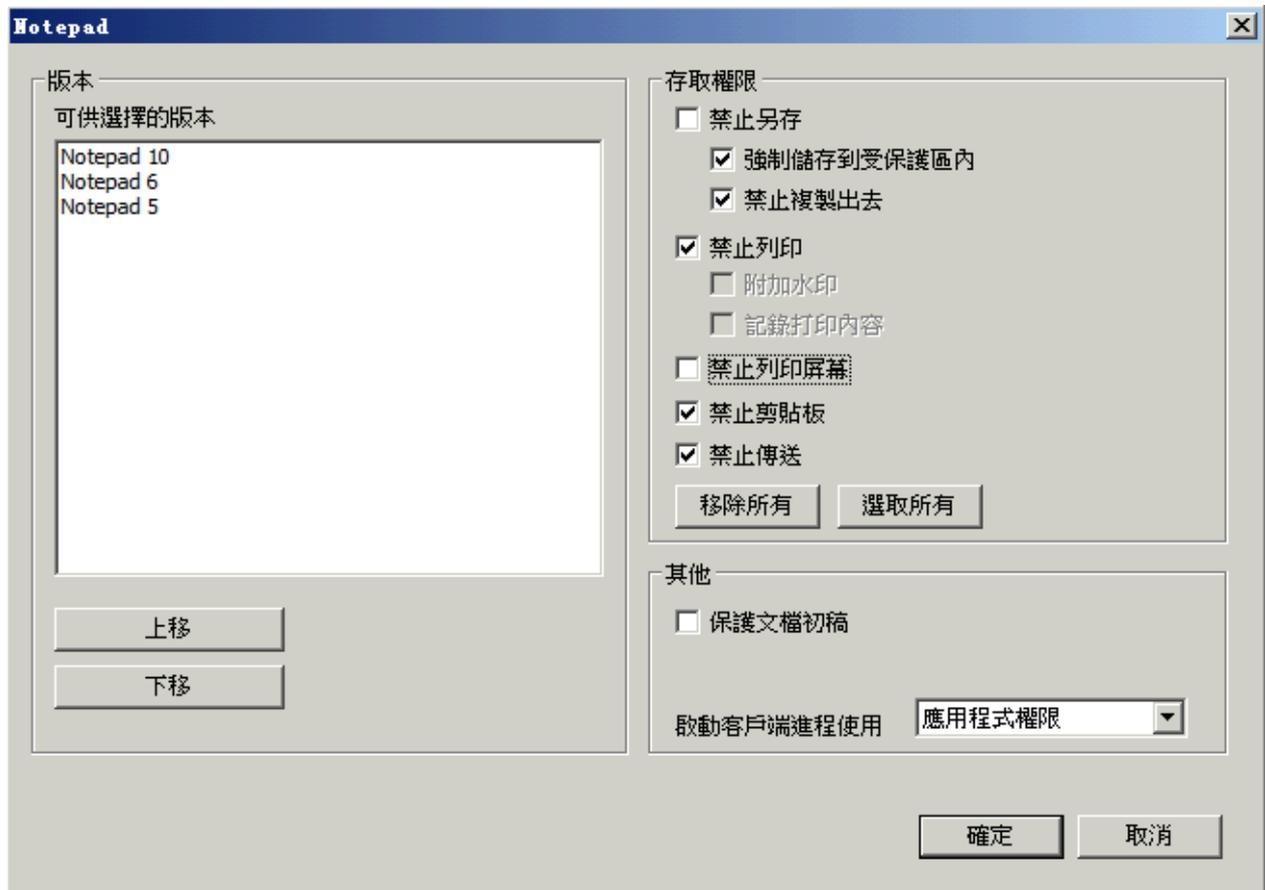
1. 在Curtain管理員菜單：選擇“文件->設置->水印”。



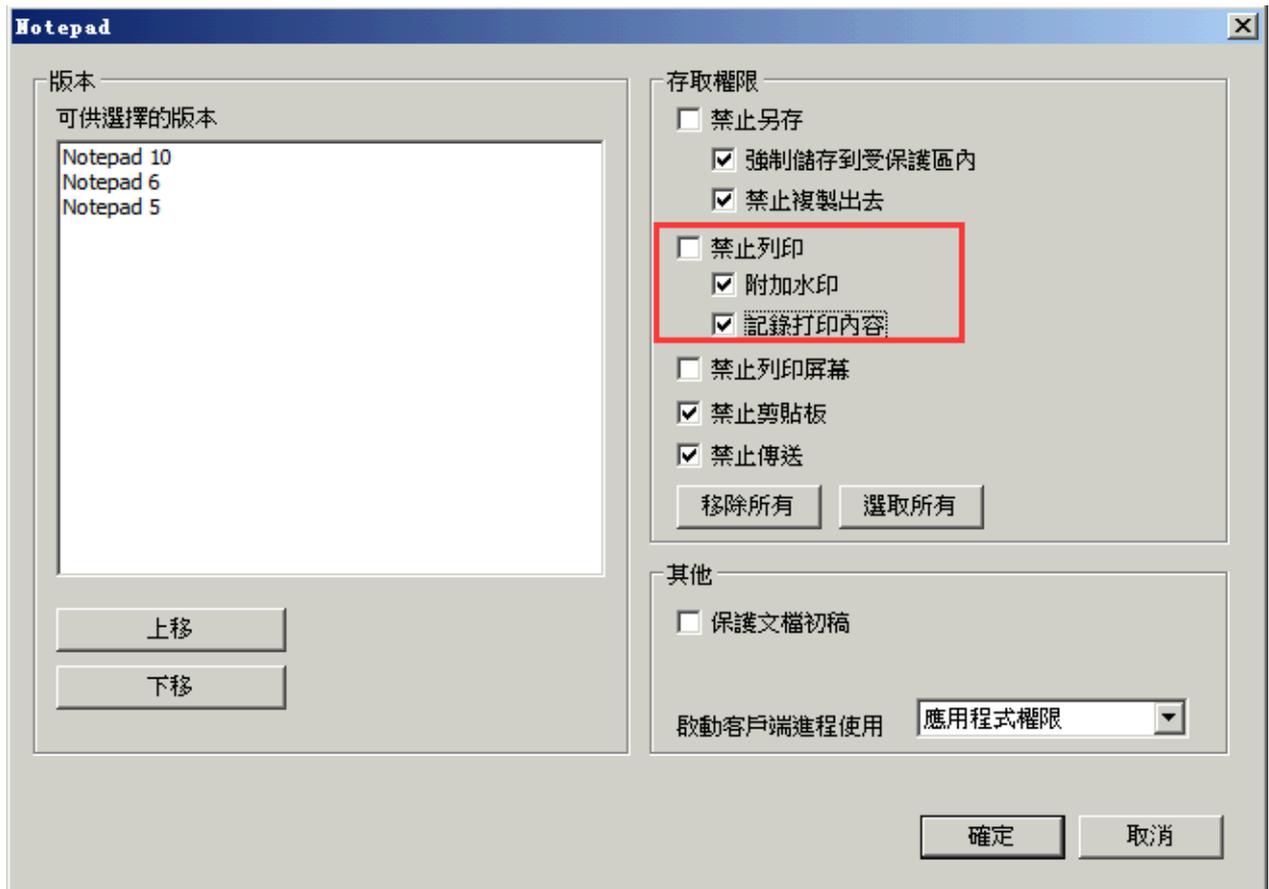
2. 完成後按"確定"。

為個別應用軟件啟動"水印"的步驟:

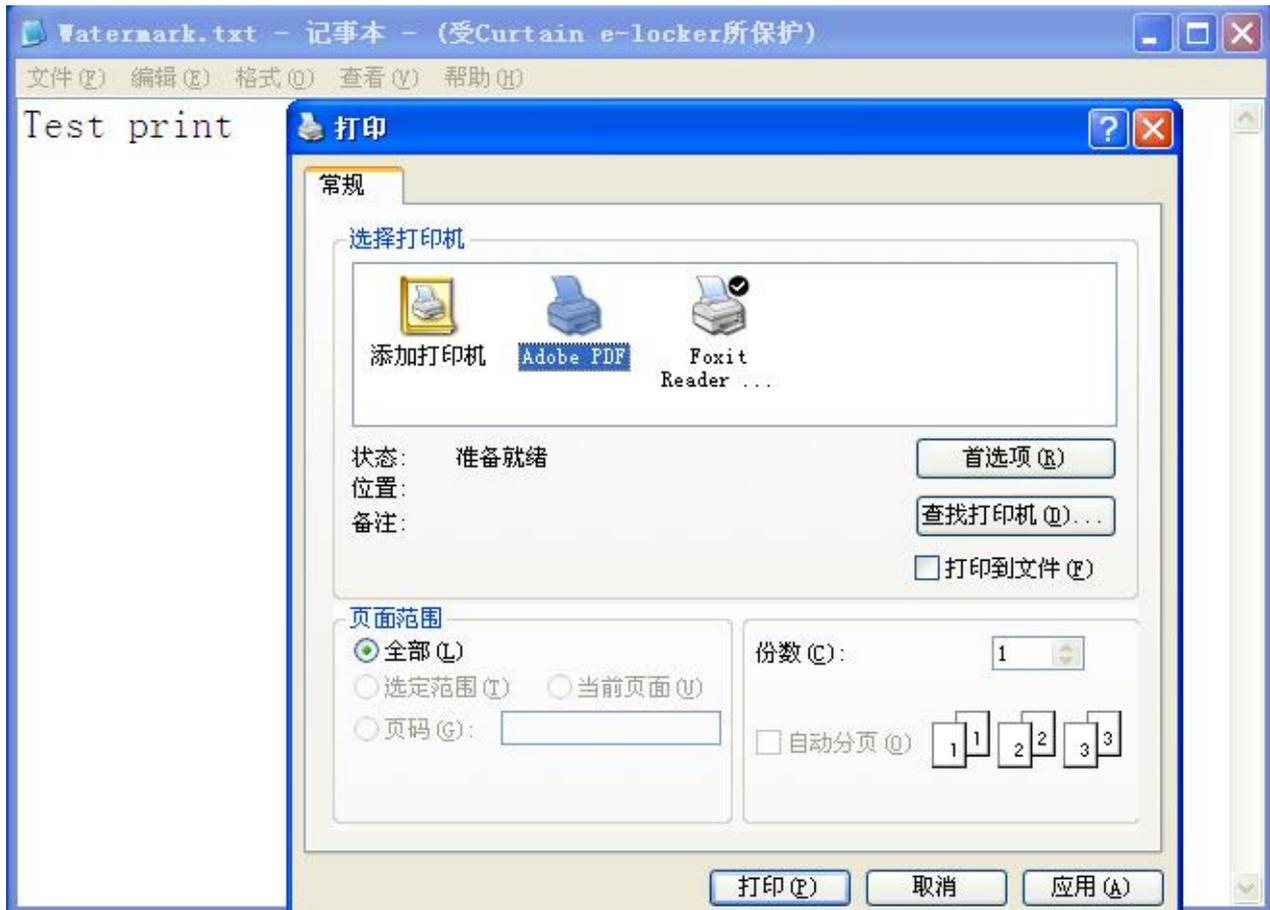
1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵，並選擇"內容"。
2. 於"受控應用程式"頁，雙擊你想啟動"水印"的應用軟件。



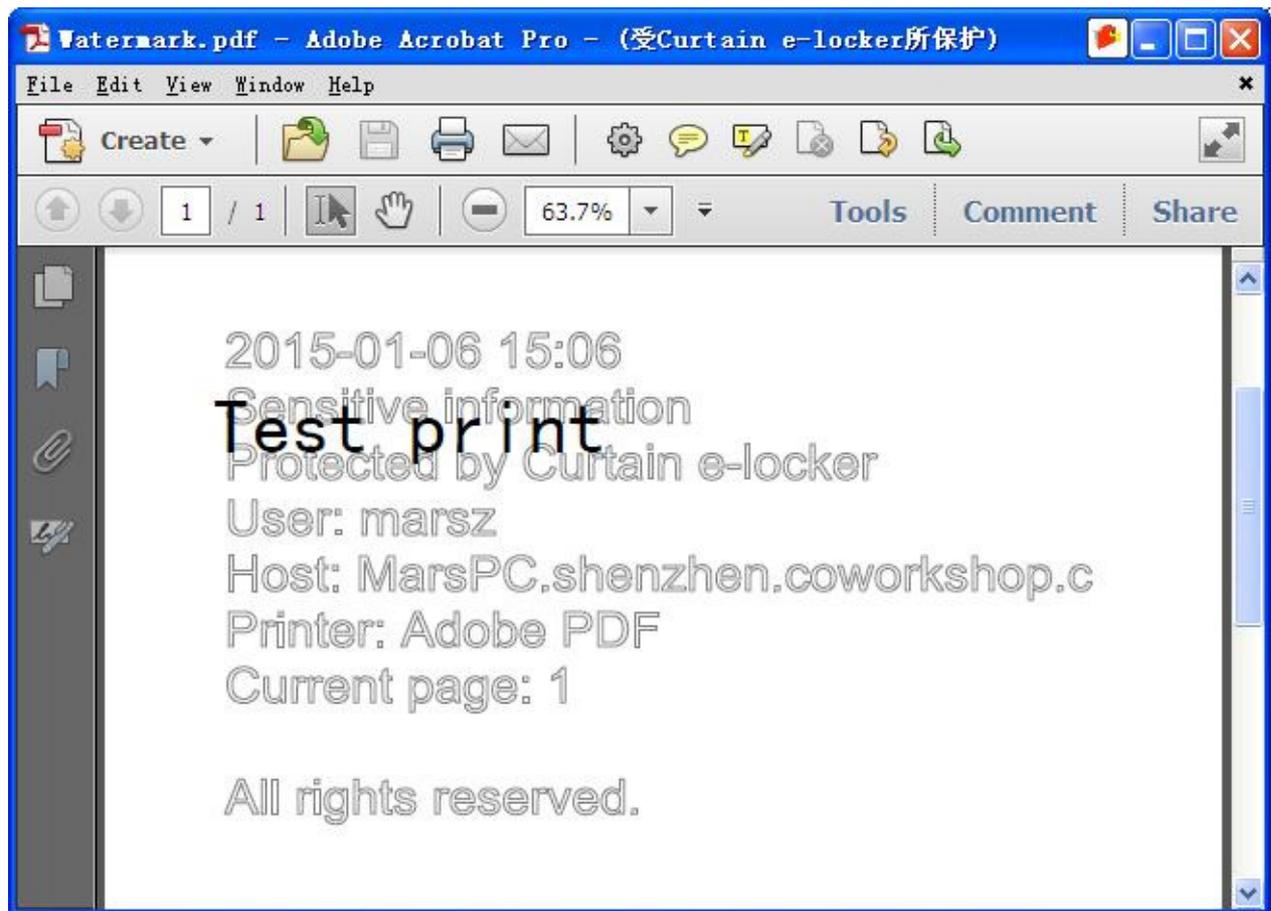
3.將“禁止打印”權限的勾去掉，再選擇“附加水印”，完成後按“確定”。



水印例子:
完成後，當使用此應用軟件打印時，系統會自動加上水印。



如果使用"打印成PDF"功能，水印會加到生成出來的PDF上。



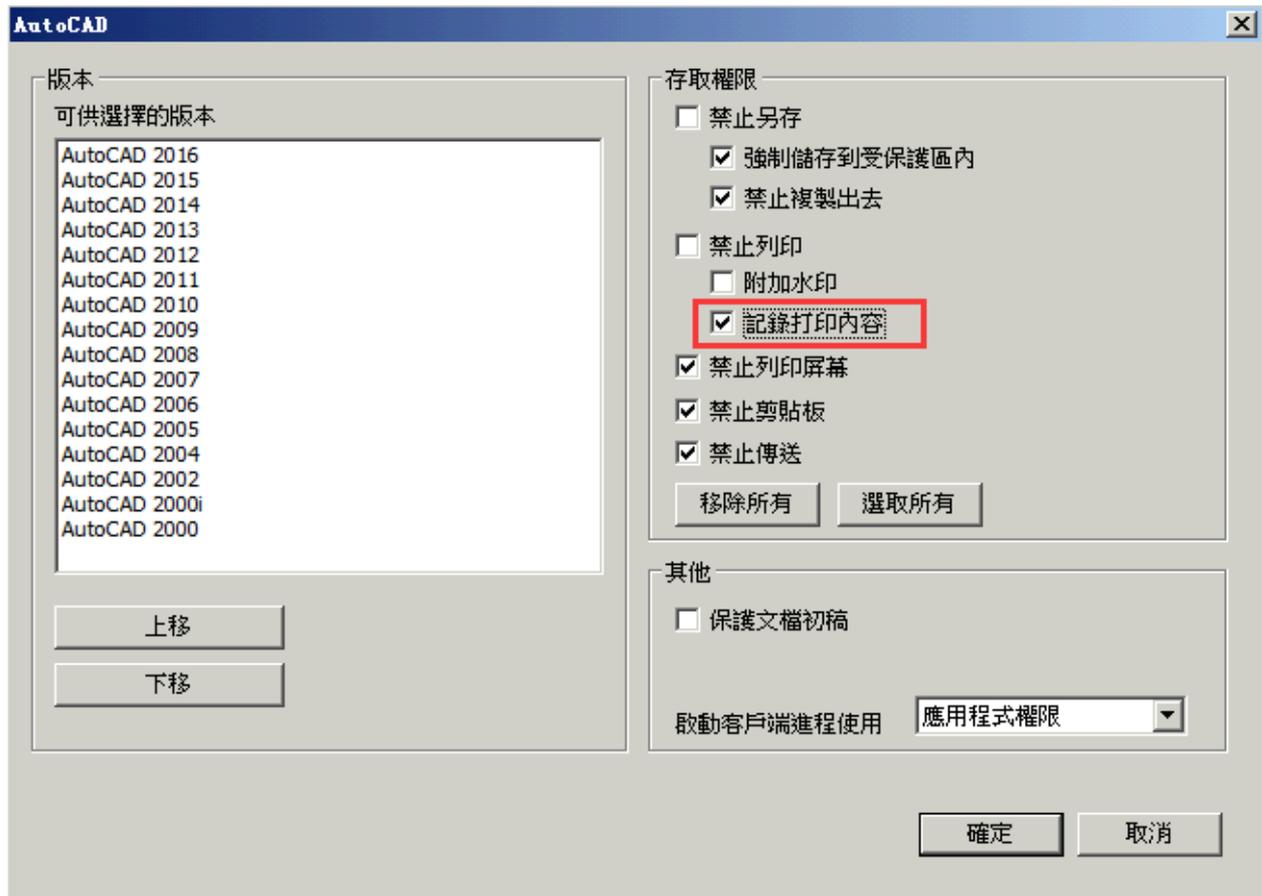
6.11 - 記錄打印內容

在預設情況下，Curtain e-locker管理員通過列印日誌來跟蹤使用者的文檔列印情況。然而，管理員只能猜測這個文件名到底列印了什麼資訊。管理員如果想要知道列印的內容，他們需要使用到“記錄列印內容”這個功能。開啟這個功能後，系統將記錄所有列印的文檔內容並將其儲存為JPG文件。管理員可以查看審計跟蹤裡的列印記錄。

開啟“記錄列印內容”應用的步驟:

1. 在Curtain管理端，選擇策略組並右鍵查看“屬性”。

2. 在應用中，按兩下你需要開啟“記錄列印內容”的應用。



3. 選擇“記錄列印內容”並確定。

備註：如果開啟這個功能，請注意系統日誌文件的大小。

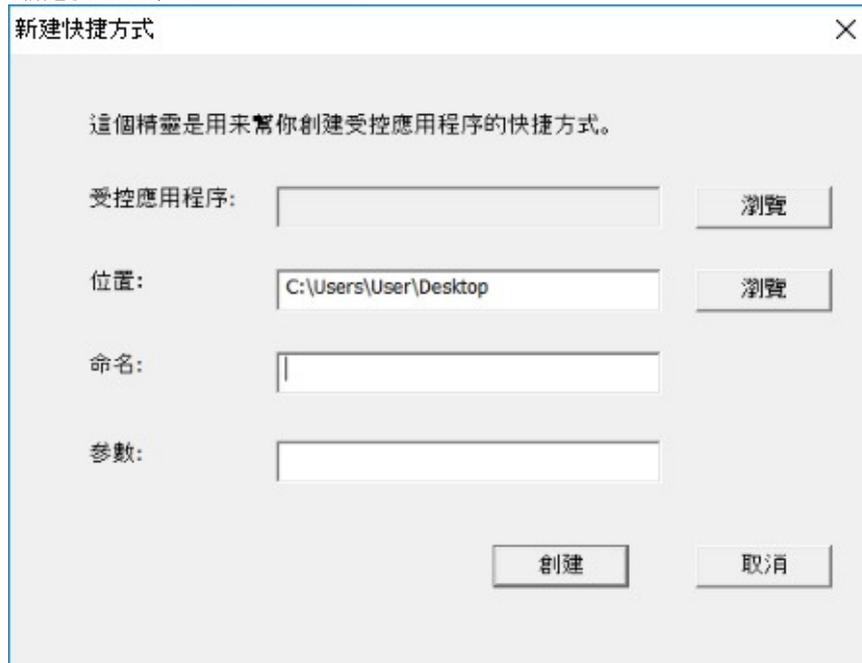
6.12 - 為受控應用程序創建快捷方式

用戶可以使用Curtain客戶端的菜單，來開啟受Curtain e-locker控制的應用程序，用戶亦可以為受控應用程序創建快捷方式，以下是創建快捷方式的步驟。

[為受控應用程序創建快捷方式的步驟：](#)

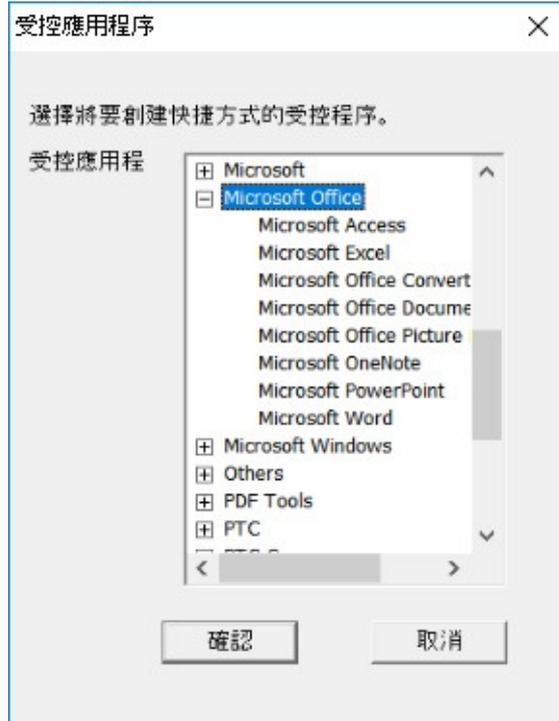
1. 在Curtain客戶端，於菜單上選擇“工具 > 新建快捷方式”。

"新建快捷方式" 窗框會如下圖顯示。



備註：選擇的應用程序必須已安裝在電腦上。

2. 使用 "瀏覽" 按鈕，來選擇你想創建快捷方式的應用程序。完成後按確認鍵確定。



3. 使用 "瀏覽" 按鈕，來選擇創建快捷方式的位置。完成後按確認鍵確定。

4. 按 "創建" 鍵。

5. 完成。

6.13 - 本地加密磁盤

預設情況下，剛剛安裝Curtain客戶端後本地受保護目錄是並沒有加密的，管理員可以啟動本地加密磁盤來將本地受保護目錄加密來提升保安性，電腦啟用了本地加密磁盤後是不能退回使用原先沒有加密的本地受保護目錄。

本地加密磁盤其實是一個虛擬磁盤，當電腦關機時此虛擬磁盤是一個加密文件，當電腦啟動時，此加密文件會以虛擬磁盤形式掛載，由於當電腦關機時，虛擬磁盤上的資料以加密文件形式保存，故此就算電腦丟失或被盜，資料依然受到很好的保護。本地加密磁盤的空間等同於該加密文件的大小，因此必須要確保儲存該加密文件的位置有足夠空間，這就是本地加密磁盤的設計。

於管理端啟動本地加密磁盤的步驟：

1. 在Curtain管理端，於菜單上選擇"文件> 設定"。

2. 於"本地加密磁盤"頁，如圖下勾選"啟動本地加密磁盤"。

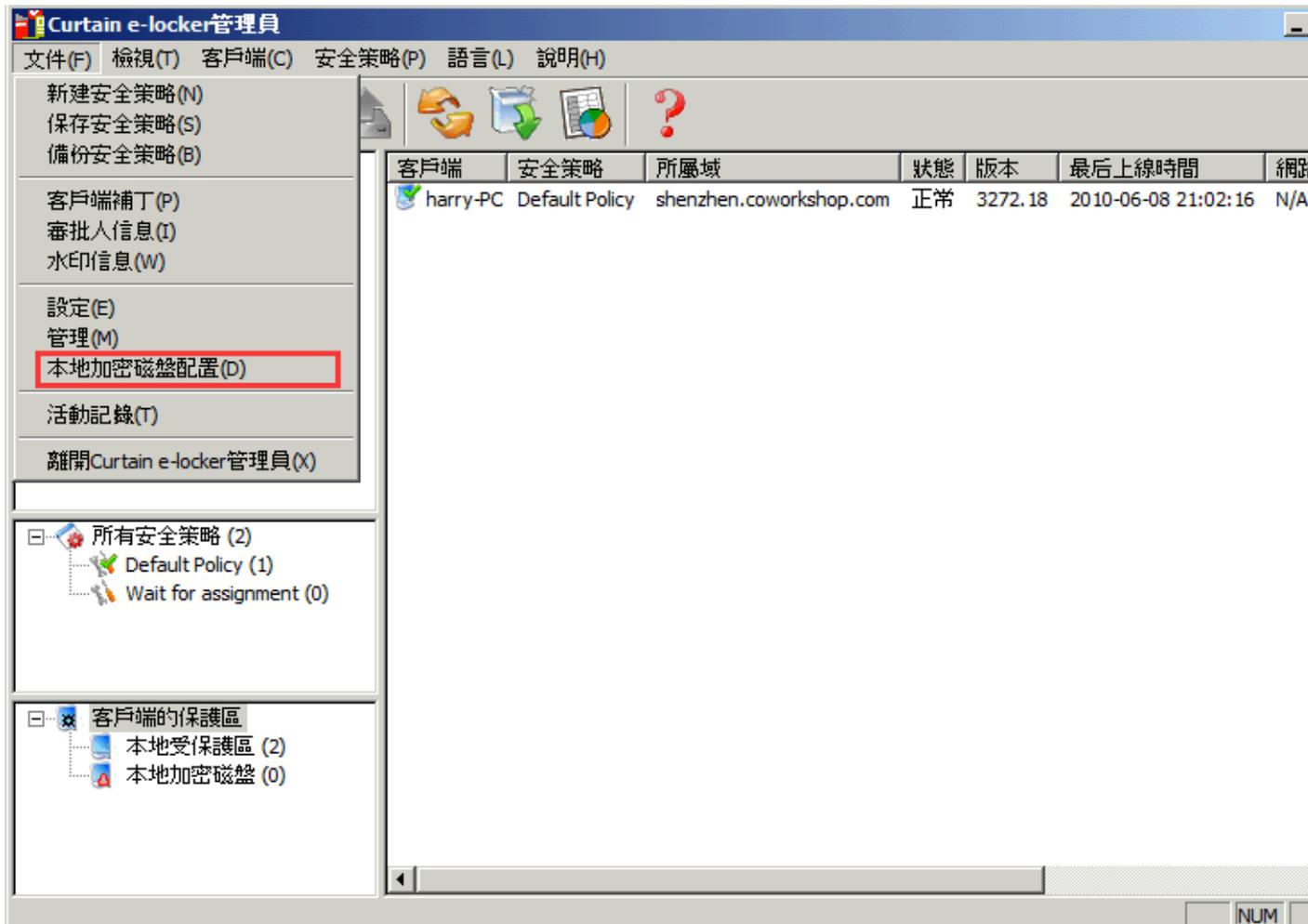
現時Curtain e-locker支持三個廣為人知的加密工具來加密本地保護目錄，分別是VeraCrypt、BitLocker和TrueCrypt，你可以選擇其中一個加密工具。



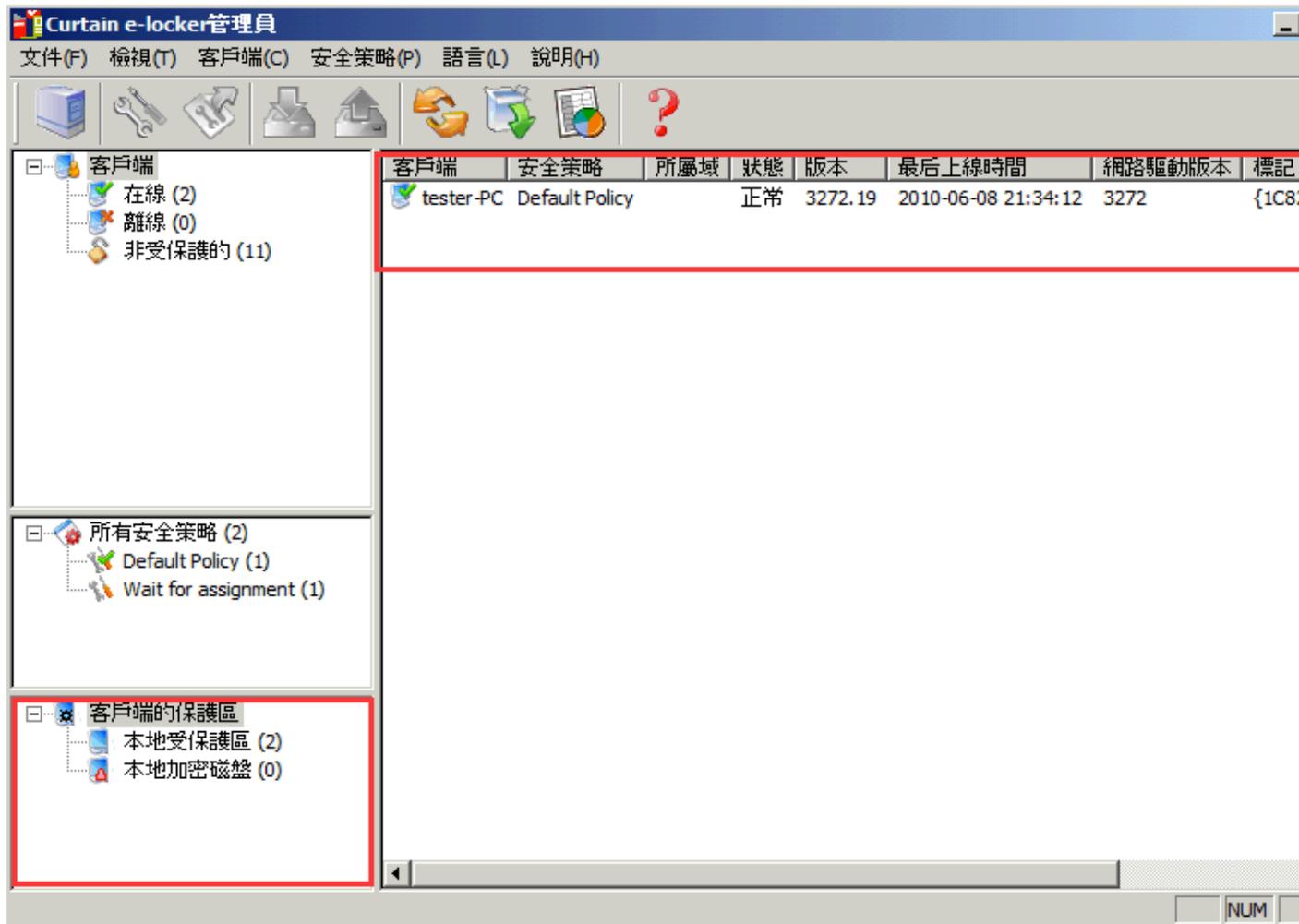
3. 按確定鍵確認 (確認後不能關閉本地加密磁盤)。

4. 啟動本地加密磁盤後，於菜單上會多了一個"本地加密磁盤配置"選項，並且在左手邊新增了"客戶端的保護區"視窗。

菜單上多了一個"本地加密磁盤配置"選項



左手邊新增客戶端的保護區"視窗



在"客戶端的保護區"視窗內，會顯示兩種不同的客戶端：

本地受保護區 - 會列出所有正在使用預設的本地受保護目錄的客戶端，代表在本地受保護目錄內的資料並沒有加密。

本地加密磁盤 - 會列出所有正在使用本地加密磁盤的客戶端，代表所有本地受保護資料會儲存在加密磁盤內。

啟動本地加密磁盤後，管理員可以搜尋合適的客戶端並為它們創建本地加密磁盤，請參考以下步驟。

於管理端搜尋合適的客戶端並為它們創建本地加密磁盤的步驟：

1. 在Curtain管理端，於菜單上選擇"文件>本地加密磁盤配置"。

本地加密磁盤配置窗框會如下圖顯示出來，管理員可以輸入不同的搜尋條件，找出合適的電腦並進行設置。舉例：你可以搜尋最少有10GB剩餘空間的電腦，並為它們建立1GB空間的本地加密磁盤。

本地加密磁盤配置

搜索條件

保護類型: 本地受保護區 本地加密磁盤

客戶端名稱: 操作系統:

本地磁盤: ... 本地加密磁盤狀態:

本地磁盤總空間: MB~ MB 本地磁盤剩餘空間:

本地加密磁盤總空間: MB~ MB 本地加密磁盤剩餘空間:

全部
全部
未獲取設置
已獲取設置
創建失敗
創建成功
掛載失敗
掛載成功
待刪除
刪除失敗
刪除成功

搜尋 清除

客戶端列表

客戶端名稱	本地磁盤	本地磁盤空間	本地加密磁盤空間	本地加密磁盤狀態	操作系統	版本	失敗原因

提示: 雙擊相應的客戶端條目可以查看更多的詳細內容, 包括更多的本地磁盤和更多的加密磁盤信息。

創建默認加密磁盤... 創建擴展加密磁盤... 刪除擴展加密磁盤... 加密密碼... 關閉

以下是每個搜尋條件的詳細介紹:

- 保護類型: 本地受保護區或本地加密磁盤。
- 客戶端名稱: 客戶端的電腦名稱 (支援模糊查詢)。
- 操作系統: 輸入作業系統關鍵字, 如Vista。
- 本地磁盤: 搜索有指定本地磁盤盤符的電腦。
- 本地磁盤總空間: 指定一個搜索本地磁盤總空間的區間值, 只要有一個本地磁盤滿足條件都當成查詢找到。
- 本地磁盤剩餘空間: 指定一個搜索本地磁盤剩餘空間的區間值, 只要有一個本地磁盤滿足條件都當成查詢找到。
- 本地加密磁盤總空間: 指定一個搜索本地加密磁盤總空間的區間值, 只要有一個本地加密磁盤滿足條件都當成查詢找到。
- 本地加密磁盤剩餘空間: 指定一個搜索本地加密磁盤剩餘空間的區間值, 只要有一個本地加密磁盤滿足條件都當成查詢找到。

- 本地加密磁盤狀態：指定欲搜索本地加密磁盤目前的狀態，包括以下狀態。
 - 全部：所有狀態。
 - 未獲取配置：客戶端未獲取到管理端的本地加密磁盤設置。
 - 已經獲取配置：客戶端已接收到管理端的本地加密磁盤設置。
 - 創建失敗：客戶端本地加密磁盤創建失敗。
 - 創建成功：客戶端本地加密磁盤已創建成功。
 - 掛載失敗：客戶端本地加密磁盤掛載失敗。
 - 掛載成功：客戶端本地加密磁盤已掛載成功（已映射為某個設置的盤符）。
 - 待刪除：管理端已配置刪除本地加密磁盤（只用於擴展本地加密磁盤）。
 - 刪除失敗：客戶端刪除本地加密磁盤失敗（只用於擴展本地加密磁盤）。
 - 刪除成功：客戶端刪除本地加密磁盤成功（只用於擴展本地加密磁盤）。

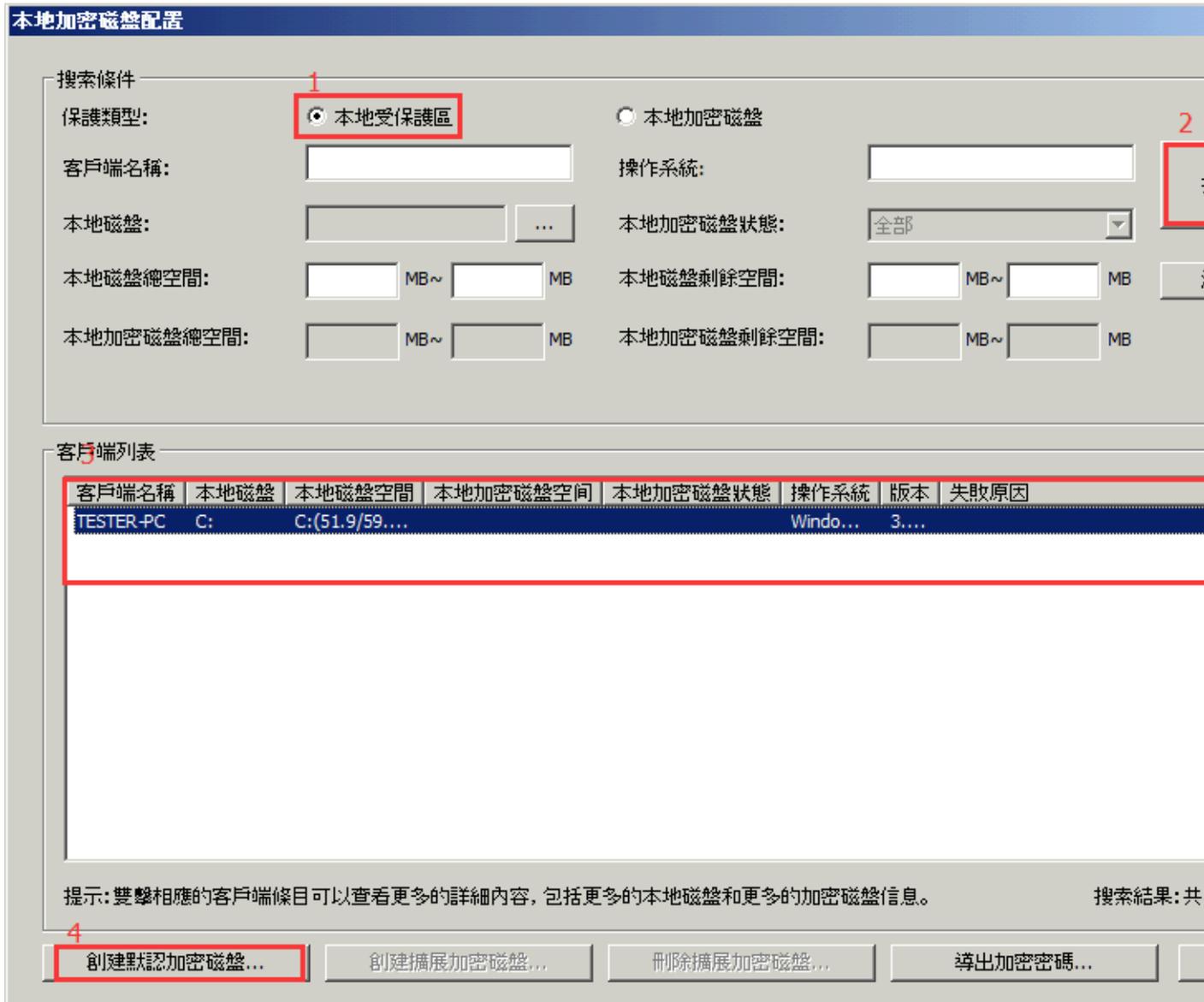
2. 點擊“加密密碼...”按鈕，設定用於加密的密碼。
在對客戶端配置本地加密磁盤之前，必須先設定加密密碼。



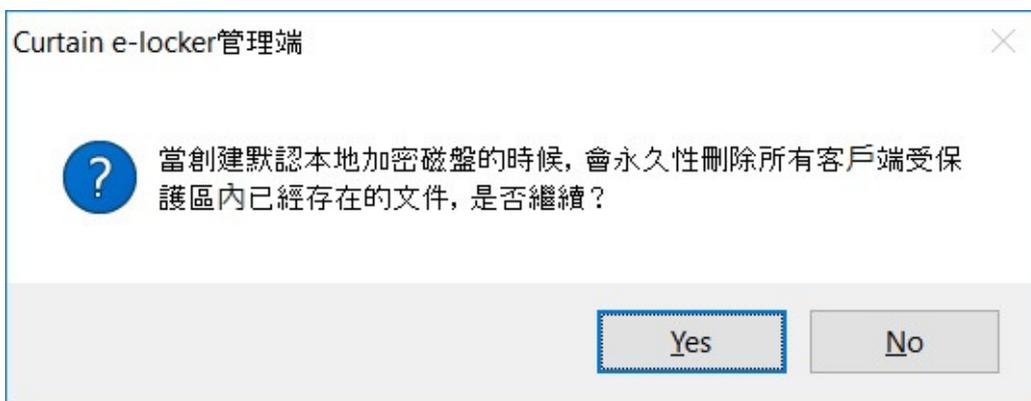
3. 輸入密碼，並按確認鍵確定。
按確認鍵後，系統會要求你把密碼文件保存起來，請小心保存此文件。

現在，你可以搜尋合適的客戶端並為它們創建本地加密磁盤(有需要可以參考上方的介紹)。舉例：你可以選擇保護類型為“本地受保護區”來找出所有還未使用本地加密磁盤的客戶端。又或是選擇保護類型為“本地加密磁盤”來找出所有已經使用本地加密磁盤的客戶端。

4. 選擇保護類型為“本地受保護區”，並按搜尋鍵。
系統會列出所有還未使用本地加密磁盤的客戶端(亦即是還在使用預設的本地受保護區)。



5. 選擇客戶端，並按"創建默認加密磁盤..." (按Ctrl鍵可選擇多個客戶端)。系統會提醒你在將本地受保護區升級到本地加密磁盤前，要先將本地受保護區內的資料備份。



6. 當已經將本地受保護區內的資料備份好，可以按 "Yes" 繼續。
然後，"創建默認加密磁盤"窗框會如下圖顯示，你可以為選擇了的客戶端設定如何創建本地加密磁盤。

"創建默認加密磁盤"窗框的選項：

- 默認加密磁盤大小（單位：GB）：要創建的本地加密磁盤的大小。
- 默認映射磁盤名稱（A-Z）：用作映射本地加密磁盤的盤符。
- 映射文件默認保存磁盤符：用作儲存本地加密磁盤的加密文件的默認盤符。
- 映射磁盤符被佔用時的處理：如果用作映射本地加密磁盤的盤符被佔用時的處理。
 - 自動選擇一個空閒的盤符: 系統會自動將本地加密磁盤映射到一個空閒的盤符
 - 停止處理並報告錯誤: 系統會停止處理並報告錯誤
- 磁碟空間不足時的處理：如果要創建的本地加密磁盤的大小超出實際磁碟空間時的處理。
 - 自動匹配一個不小於1GB的加密磁盤: 系統會自動創建1GB的本地加密磁盤 (不理管理員原先設定的大小)
 - 停止處理並報告錯誤: 系統會停止處理並報告錯誤

7. 配置好相應的參數後，點擊“確定”。

當下一次用戶打開Curtain客戶端時，系統會提示用戶創建本地加密磁盤。

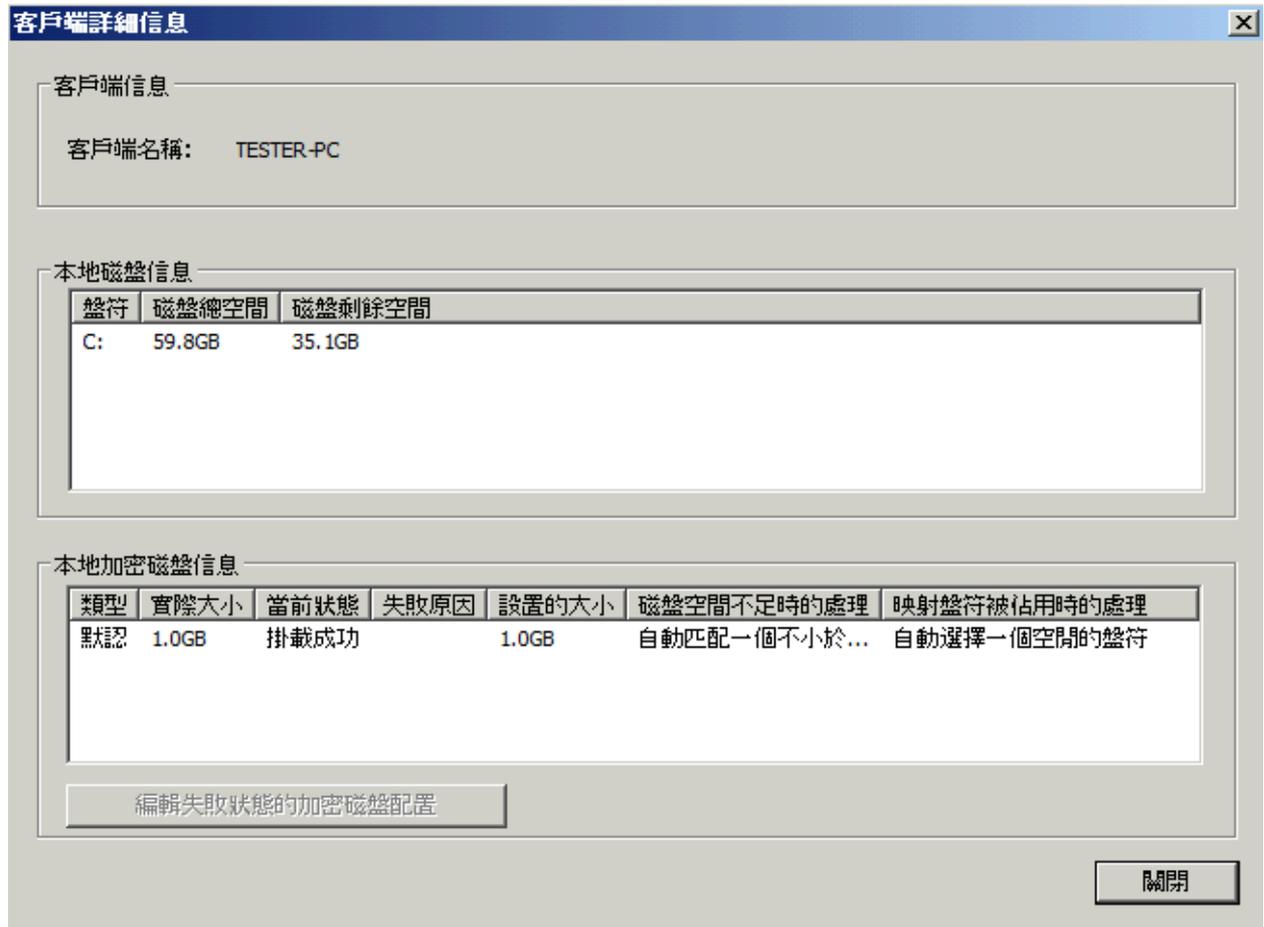
下面是一個例子，可以作為參考：

- 默認加密磁盤大小（單位：GB）：10
- 默認映射磁盤名稱（A-Z）：F:
- 映射文件默認保存磁盤符：C:
- 映射磁盤符被佔用時的處理：自動選擇一個空閒的盤符
- 磁碟空間不足時的處理：自動匹配一個不小於1GB的加密磁盤

這個例子代表會創建一個10GB大的本地加密磁盤，並將本地加密磁盤映射為F: 盤。當電腦關機時，本地加密磁盤的加密文件會儲存在C: 盤。如果C: 盤沒有10GB空間，系統會自動創建1GB的本地加密磁盤。如果F: 盤符被佔用時，系統會自動將本地加密磁盤映射到一個空閒的盤符。

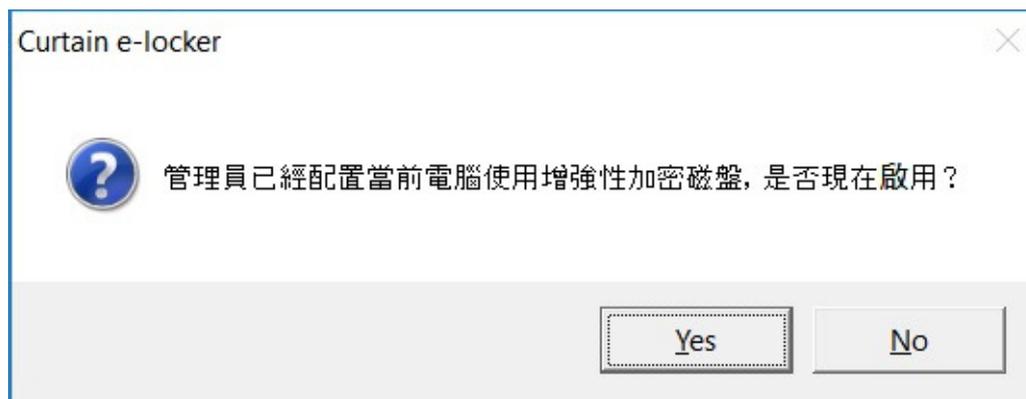
8. 於"本地加密磁盤配置"窗框，雙擊一個客戶端，可以查看客戶端詳細資訊。

下圖表示該客戶端已經成功創建了本地加密磁盤。



回到Curtain客戶端上，完成創建本地加密磁盤的步驟：

1. 當下一次用戶打開Curtain客戶端時，系統會提示用戶創建本地加密磁盤。



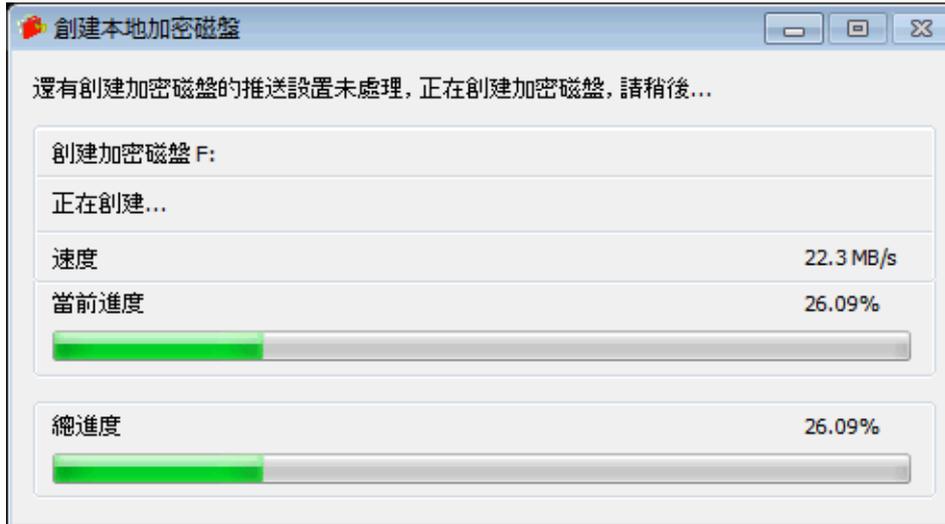
2. 按 "Yes" 繼續，或按 "No" 推遲創建本地加密磁盤。

按 "Yes" 後，當用戶重啟電腦後，系統會創建本地加密磁盤，請記得要先將本地受保護區內的資料備份。

3. 重啟電腦並打開Curtain客戶端後，系統會如下圖彈出提示。



4. 按 "OK" 繼續，系統會立即創建本地加密磁盤。



5. 完成後，Curtain客戶端的介面會顯示本地加密磁盤。

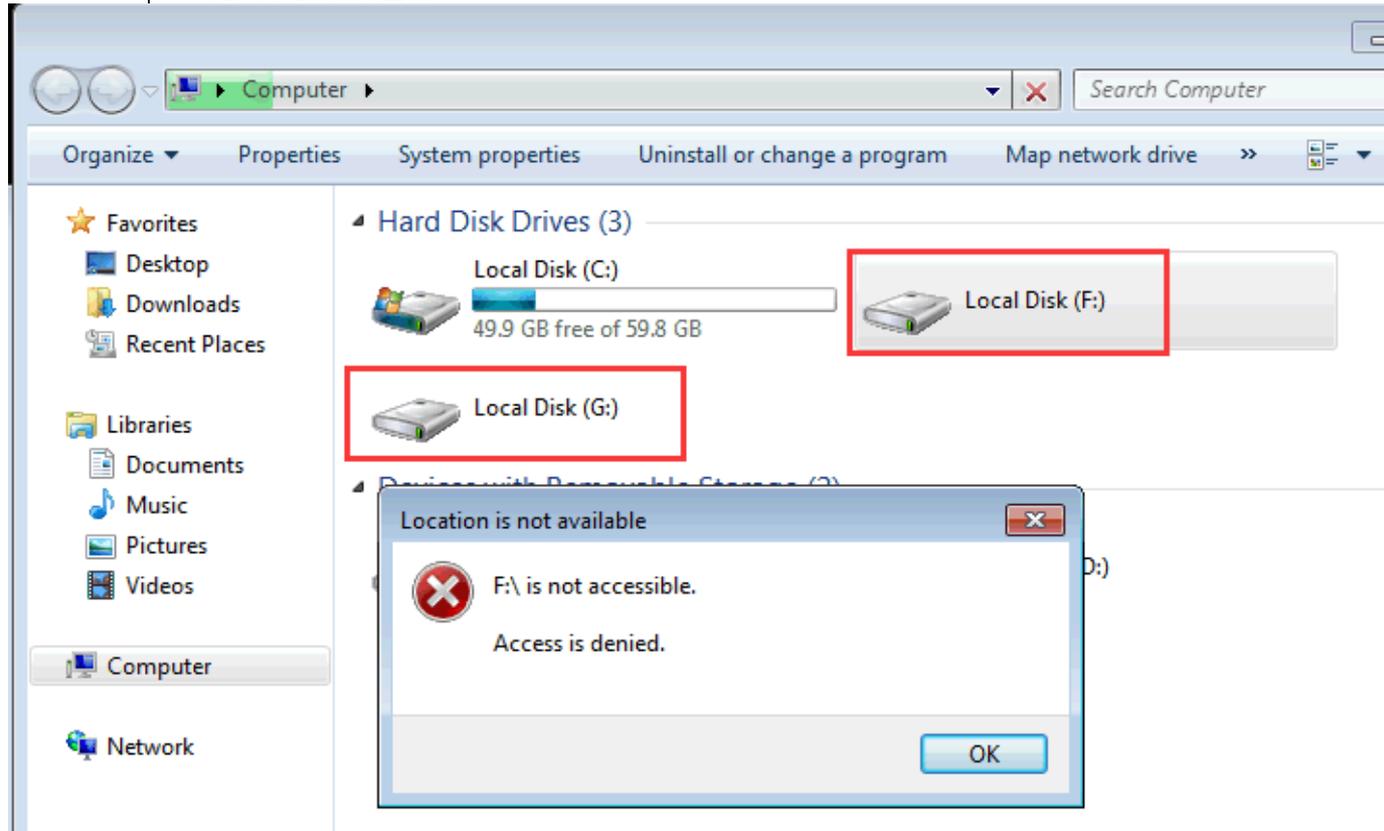


於Curtain客戶端，本地加密磁盤會顯示在我的電腦下面。

第一次創建的本地加密磁盤必定為默認的本地加密磁盤，如有需要，管理員可以創建擴展的本地加密磁盤。在加密磁盤下面，你可以看到有兩個文件夾，分別是個人及公共。個人的文件夾是只給當前登錄的用戶使用，所以個人文件夾可以用來存放個人敏感的文件，而公共的文件夾是給所有用戶使用的，所以公共文件夾可以用來作於客戶端上分享文件。

如果在升級本地加密磁盤前，在Curtain客戶端已有使用本地附加受保護區，則該本地附加受保護區會維持不變，本地加密磁盤不適用於本地附加受保護區的。

在上圖的例子中，F:盤是默認本地加密磁盤，而G:盤是擴展本地加密磁盤，用戶可以通過受Curtain e-locker保護的介面(如:Curtain客戶端或受保護的應用程式)來使用保護區內的資料(包括本地加密磁盤)，用戶是不能使用Windows Explorer進入本地加密磁盤的。



管理員處理那些創建/掛載失敗的客戶端的步驟：

有些客戶端會因為不同原因不能創建或掛載本地加密磁盤，例如：沒有足夠硬碟空間或映射盤符被佔用等，管理員可以找出那些創建/掛載失敗的客戶端，修改設定並再次為它們創建本地加密磁盤。

1. 在Curtain管理端，於菜單上選擇"文件>本地加密磁盤配置"。

本地加密磁盤配置

搜索條件

保護類型: 本地受保護區 本地加密磁盤

客戶端名稱: 操作系統:

本地磁盤: ... 本地加密磁盤狀態:

本地磁盤總空間: MB~ MB 本地磁盤剩餘空間:

本地加密磁盤總空間: MB~ MB 本地加密磁盤剩餘空間:

本地加密磁盤狀態:

- 全部
- 未獲取設置
- 已獲取設置
- 創建失敗
- 創建成功
- 掛載失敗
- 掛載成功
- 待刪除
- 刪除失敗
- 刪除成功

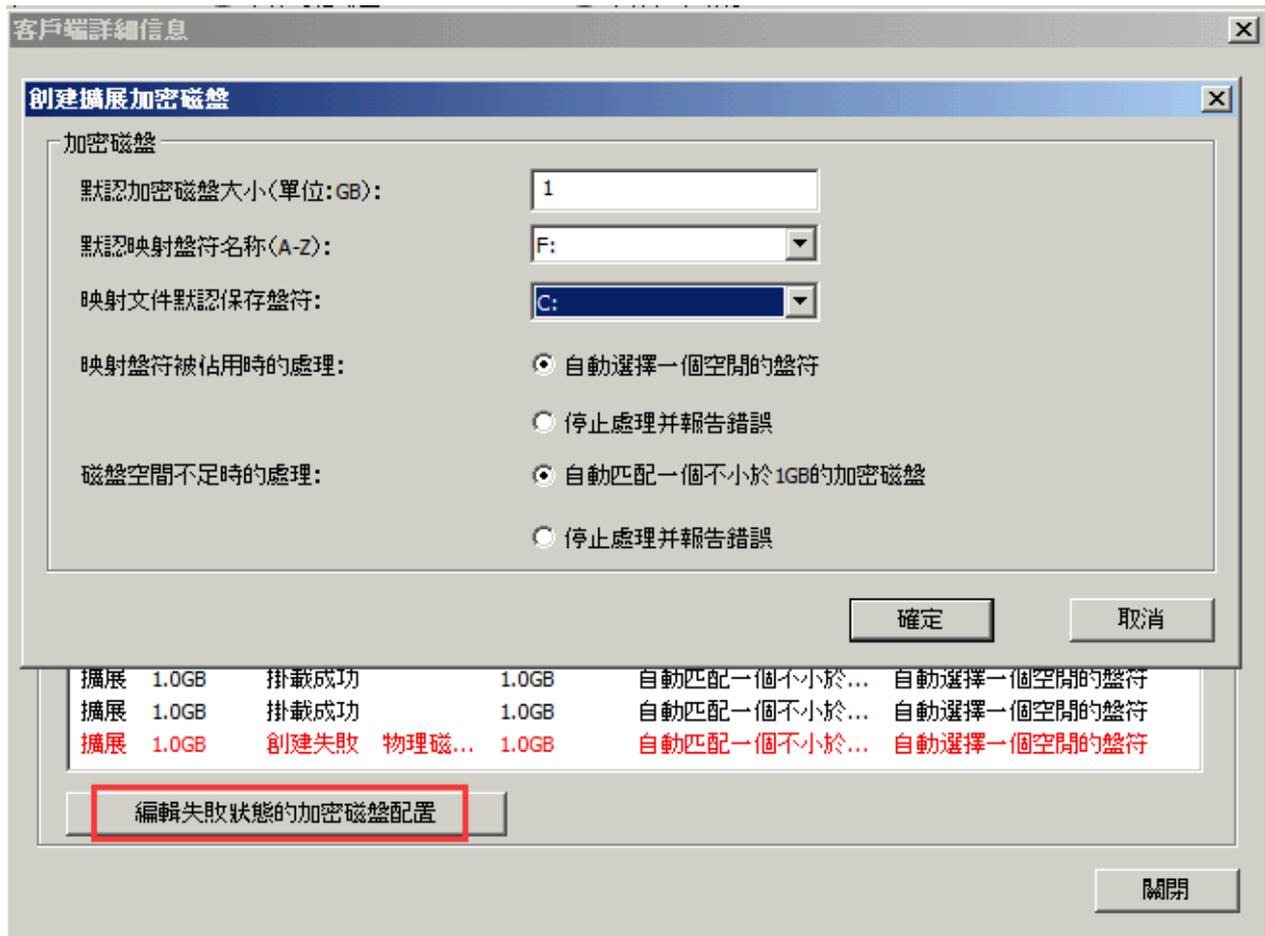
客戶端列表

客戶端名稱	本地磁盤	本地磁盤空間	本地加密磁盤空間	本地加密磁盤狀態	操作系統	版本	失敗原因

提示: 雙擊相應的客戶端條目可以查看更多的詳細內容, 包括更多的本地磁盤和更多的加密磁盤信息。

2. 於保護類型，選擇"本地加密磁盤"。
3. 於本地加密磁盤狀態，選擇"創建失敗"或"掛載失敗"。
4. 按搜尋鍵找出那些創建/掛載失敗的客戶端。
5. 雙擊一個客戶端，可以查看客戶端詳細資訊。

6. 按下圖的按鈕來修改本地加密磁盤的設定。



7. 配置好相應的參數後，點擊“確定”。

當下一次用戶打開Curtain客戶端時，系統會再次提示用戶創建本地加密磁盤。

於管理端搜尋合適的客戶端並為它們創建擴展本地加密磁盤的步驟：

有時管理員需要為客戶端創建擴展本地加密磁盤，例如：默認本地加密磁盤的空間已經不夠使用，這時管理員可以為這些客戶端創建擴展本地加密磁盤。

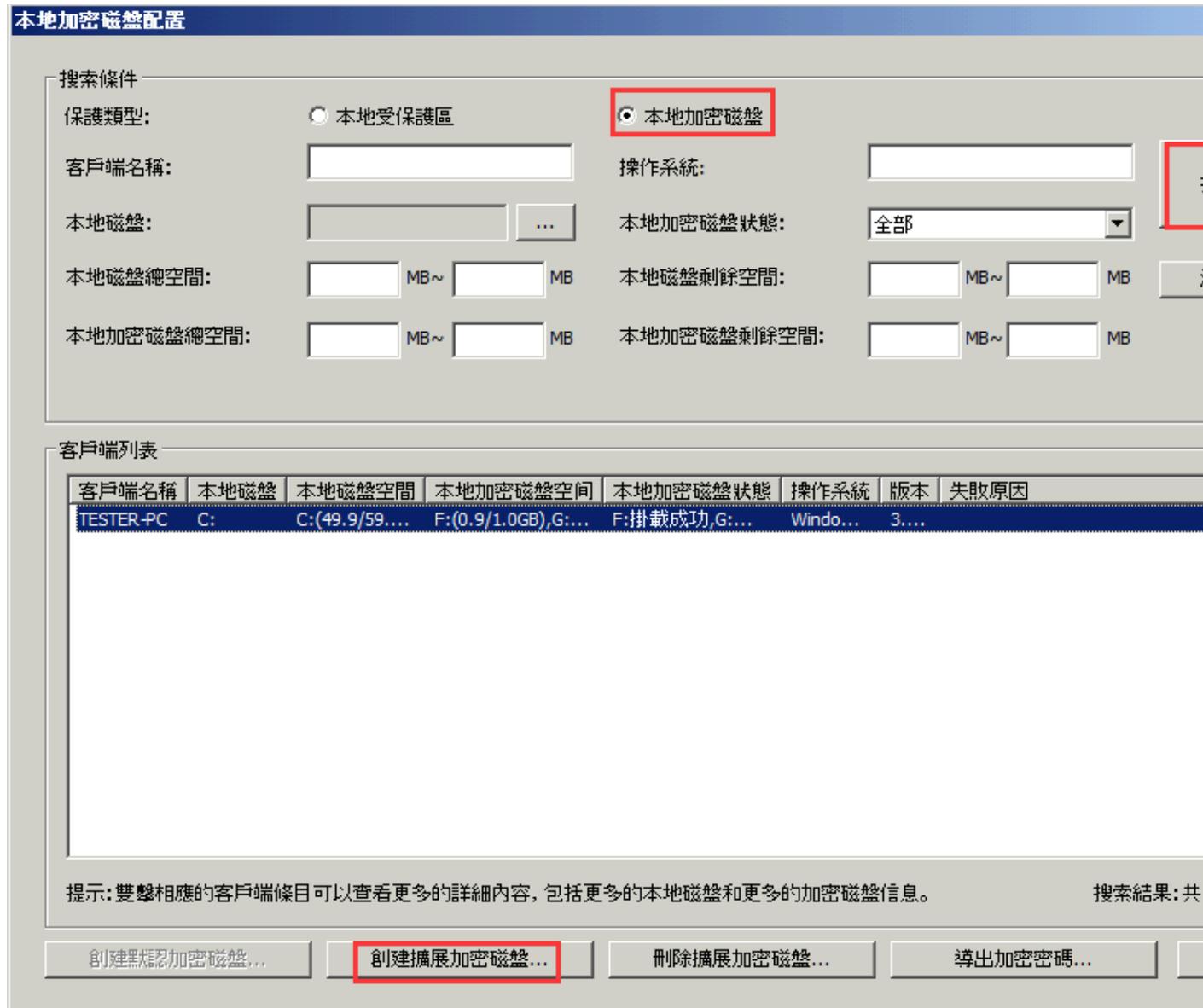
1. 在Curtain管理端，於菜單上選擇“文件>本地加密磁盤配置”。

本地加密磁盤配置窗框會如下圖顯示出來，管理員可以輸入不同的搜尋條件，找出合適的電腦並進行設置。舉例：你可以搜尋本地加密磁盤剩餘空間少於500MB的客戶端。

2. 輸入條件，並按搜尋。

3. 選擇客戶端，並按"擴展默認加密磁盤..." (按Ctrl鍵可選擇多個客戶端)。

創建擴展本地加密磁盤的步驟和創建默認本地加密磁盤是差不多的，你可以參考之前創建默認本地加密磁盤的步驟。



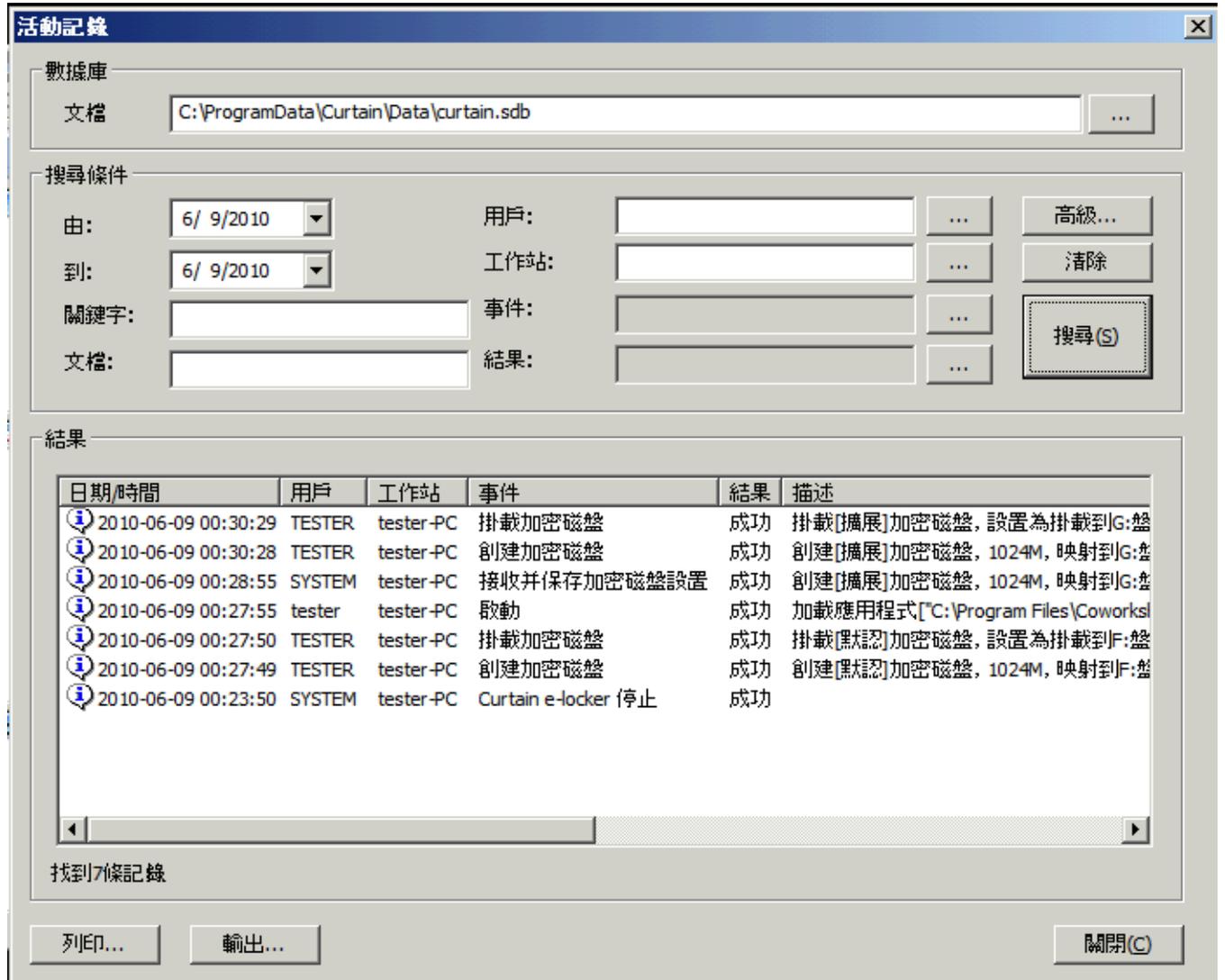
於管理端查看關於本地加密磁盤的審計日誌的步驟：

所有關於本地加密磁盤的操作(如:創建、掛載、刪除本地加密磁盤等)都會記錄到審計日誌中，以供查看。

1. 在Curtain管理端，於菜單上選擇"文件>活動記錄"。

2. 輸入條件，並按搜尋。

下圖是一個例子，以作參考。

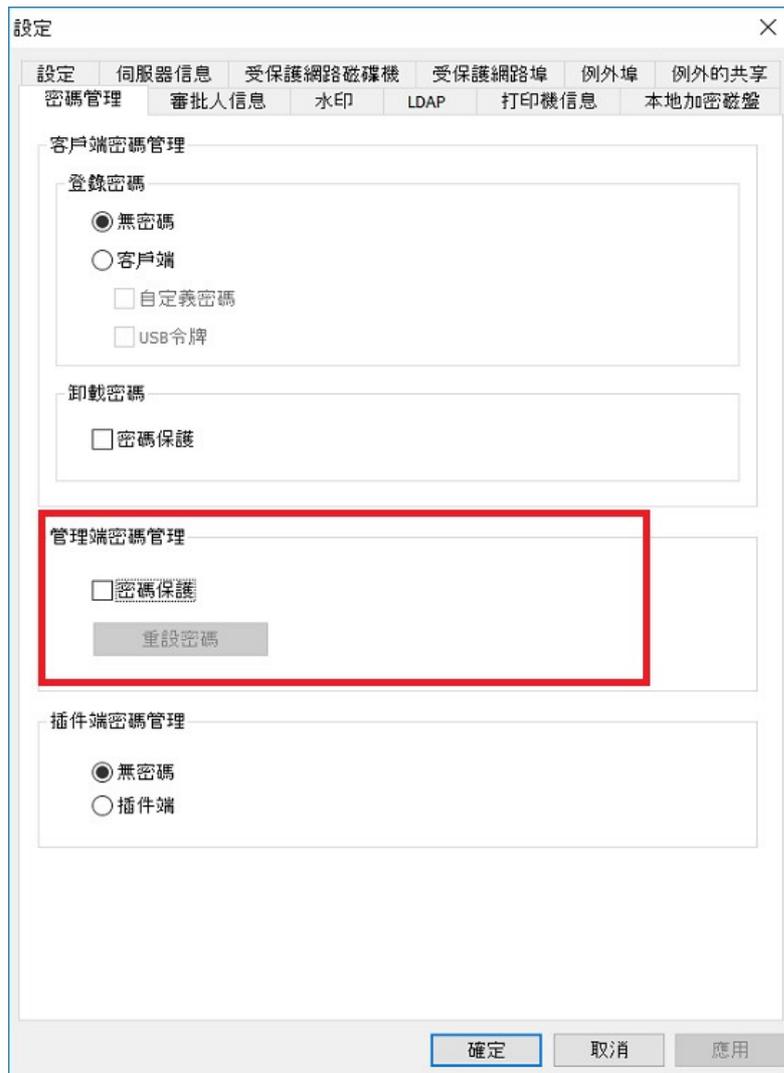


6.14 - 為Curtain管理端、服務器插件和客戶端設定登入密碼

在預設情況下，打開Curtain管理端、服務器插件或客戶端，是不用輸入密碼的，管理員可以啟動密碼保護來加強系統保安。

開啟Curtain管理端密碼保護的步驟:

1. 在Curtain管理端，於菜單上選擇"文件> 設定"。
2. 於"密碼管理"頁，啟動"管理端密碼管理"下的密碼保護。如果是第一次啟動管理端密碼保護，系統會彈出對話框要求設定密碼。如果之前啟動過此功能，則會使用原有完有密碼。



3. 輸入密碼後按確定鍵確認。

4. 完成，下一次管理員必需輸入正確密碼才能打開Curtain管理端。

開啟Curtain服務器插件密碼保護的步驟:

1. 在Curtain管理端，於菜單上選擇"文件> 設定"。

2. 於"密碼管理"頁，"插件端密碼管理"下選擇插件端。如果是第一次啟動插件端密碼保護，下一次打開Curtain服務器插件時，系統會彈出對話框要求設定密碼。如果之前啟動過此功能，則會使用原有完有密碼。

開啟Curtain客戶端密碼保護的步驟:

1. 在Curtain管理端，於菜單上選擇"文件> 設定"。

2. 於"密碼管理"頁，"客戶端密碼管理 > 客戶端"下有兩個選項:

自定義密碼 - 用戶下一次打開Curtain客戶端時，系統會彈出對話框要求設定密碼。如果之前啟動過此功能，則會使用原有完有密碼。

USB令牌 - 用戶下一次打開Curtain客戶端時，系統會彈出對話框要求插入載有個人電子證書的USB令牌作登入之用。

3. 按確定鍵確認。

4. 在管理員同時選擇了"自定義密碼"和"USB令牌"，代表用戶可以決定用其中一種方式登入。

6.15 - 為Curtain管理端、服務器插件和客戶端更改或重設登入密碼

如果管理員已為Curtain管理端、服務器插件或客戶端啟動了密碼保護，使用者必需輸入密碼才能打開相關程序，如果想更改或重設登入密碼，請參考以下步驟。

為Curtain管理端、服務器插件或客戶端更改或重設登入密碼的步驟:

1. 當登入Curtain管理端、服務器插件或客戶端時，選擇 "修改密碼"。



"密碼設置" 窗框會如下圖顯示。



2. 輸入舊密碼和新密碼。
3. 按確定鍵確認。
4. 如果你忘記了密碼，請聯絡管理員，管理員可以選擇 "忘記密碼"，並輸入授權字符串來重設你的登入密碼。



輸入授權字符串

請輸入授權字符串:

確定 取消

7 - 後續維護

7.1 - 補丁的管理

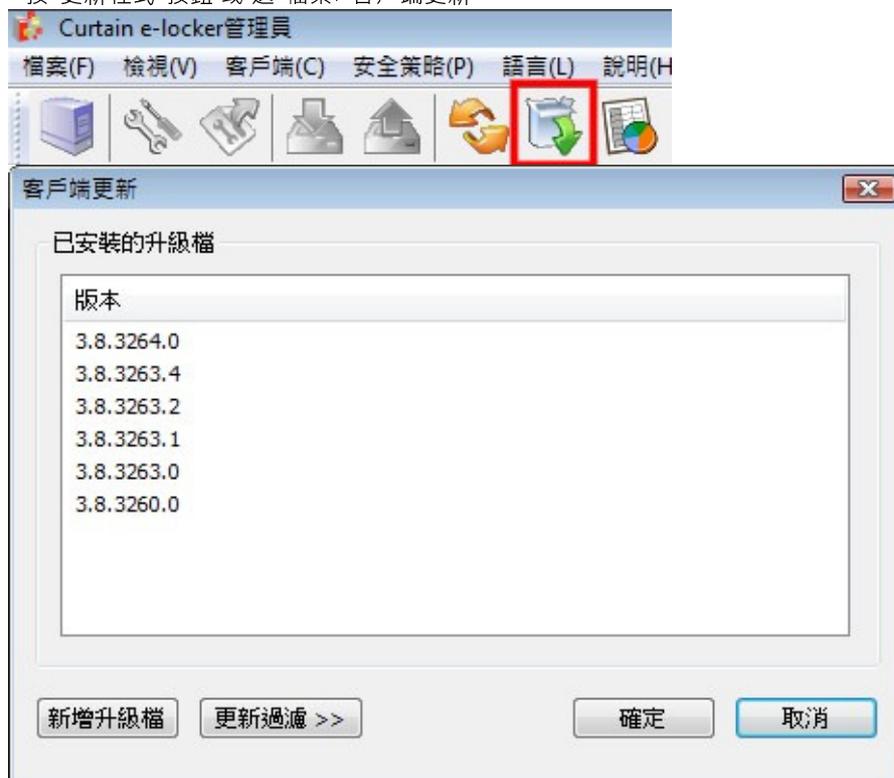
系統管理員可以從我們的網站下載最新補丁，然後將補丁安裝在Curtain管理員上，所有Curtain客戶端的程式便會自動被更新，系統管理員不需要在每一台用戶電腦上安裝最新補丁。

安裝補丁方法:

1. 從我們的網站下載適當的補丁。當發佈一個新的版本時，一般情況下會有五個補丁。舉例 (版本號是3273.04):
 - CurtainFullPatch_Win32(327304).zip - 給安裝在32位元操作系統上的Curtain管理員
 - CurtainFullPatch_X64(327304).zip - 給安裝在64位元操作系統上的Curtain管理員
 - CurtainAdminPatch_Win32(327304).zip - 如果你只想為Curtain管理員或Curtain服務器插件安裝新的版本，你可以運行此補丁，此補丁並不會更新客戶端的
 - CurtainAdminPatch_X64(327304).zip - 如果你只想為Curtain管理員或Curtain服務器插件安裝新的版本，你可以運行此補丁，此補丁並不會更新客戶端的
 - CurtainClientPatch(327304).zip - 如果你只想為個別的Curtain客戶端安裝新的版本，你可以直接在客戶端上運行此補丁
2. 解壓補丁。
3. 於安裝了Curtain管理員那台服務器上執行 CurtainFullPatch_Win32.exe 或 CurtainFullPatch_X64.exe 補丁，當下一次Curtain客戶端連接到Curtain管理員時，Curtain客戶端的程式便會自動被更新。
4. 如有其他Curtain服務器插件，需要執行 CurtainAdminPatch_Win32.exe 或 CurtainAdminPatch_X64.exe 補丁把服務器插件更新。

查看所有已安裝的補丁:

- 按"更新程式"按鈕 或 選"檔案> 客戶端更新"



7.2 - 管理員遷移到另一台電腦上

有以下兩種情況:

- (1) 新的Curtain管理員的電腦名稱與IP地址和現時的Curtain管理員的電腦名稱與IP地址是一樣的。
- (2) 新的Curtain管理員的電腦名稱與IP地址和現時的Curtain管理員的電腦名稱與IP地址是不一樣的。

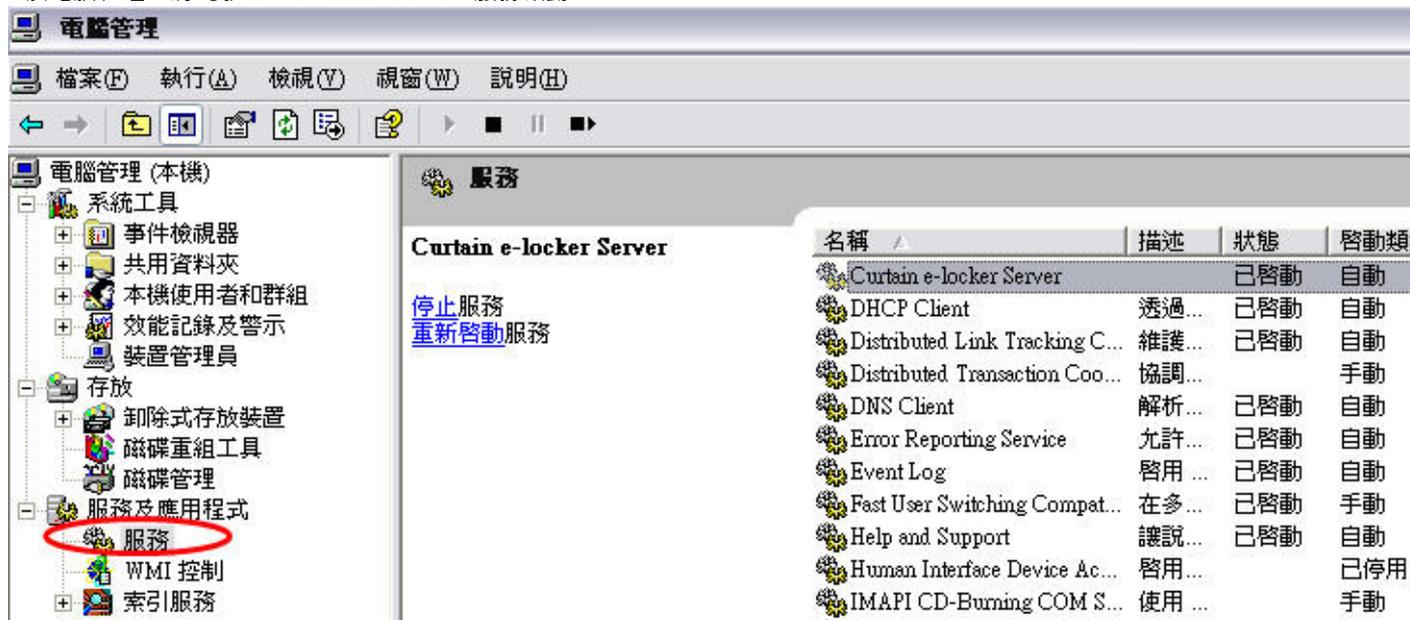
遷移前的準備事項:

1. 將現時Curtain管理員上的安全策略先作備份，請將以下文件夾和文檔複製一份。
 - 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. 將現時Curtain管理員上的活動記錄先作備份，請將以下文檔複製一份。
 - C:\Program Files\Coworkshop\Curtain 3\bin\Curtain.mdb (它存在於舊版本中)
 - 將整個 "Curtain" 文件夾備份
 - 於Windows 2000 / XP / 2003，此文件夾位於 C:\Documents and Settings\All Users\Application Data
 - 於Windows 2008 / 2010 / Vista / Win7 / Win8 / Win10，此文件夾位於 C:\ProgramData

情況1 - 新的Curtain管理員的電腦名稱與IP地址和現時的Curtain管理員的電腦名稱與IP地址是一樣的:

以下是遷移步驟:

1. 將現時Curtain管理員關機，或將它從網絡環境中斷開。
2. 安裝一台新電腦，並使用一樣的電腦名稱與IP地址。
3. 在該台新電腦上，安裝Curtain管理員(詳細步驟請參考相關資料)。
4. 激活剛安裝好的Curtain管理員(詳細步驟請參考相關資料)。
5. 將之前備份好的安全策略和活動記錄複製到新的Curtain管理員上。
 - 於電腦管理，將"Curtain e-locker Server"服務停止。
 - 將之前備份好的文件夾和文檔複製到相關位置。
 - 於電腦管理，將"Curtain e-locker Server"服務啟動。



- 由於新的Curtain管理員使用一樣的電腦名稱與IP地址，Curtain客戶端會自動連接到新的Curtain管理員。
- 完成遷移

情況2 - 新的Curtain管理員的電腦名稱與IP地址和現時的Curtain管理員的電腦名稱與IP地址是不一樣的:
 以下是遷移步驟:

- 安裝一台新電腦，並使用不一樣的電腦名稱與IP地址。
- 在該台新電腦上，安裝Curtain管理員(詳細步驟請參考相關資料)。
- 激活剛安裝好的Curtain管理員(詳細步驟請參考相關資料)。
- 將之前備份好的安全策略和活動記錄複製到新的Curtain管理員上。
 - 於電腦管理，將"Curtain e-locker Server"服務停止。
 - 將之前備份好的文件夾和文檔複製到相關位置。
 - 於電腦管理，將"Curtain e-locker Server"服務啟動。
- 在現時的Curtain管理員，於菜單上選擇"檔案>設定"。



- 於"指定新的管理員"上，輸入新的Curtain管理員的電腦名稱或IP地址，並按確定。

當Curtain客戶端連接到現時的Curtain管理員時，系統會通知客戶端有新的Curtain管理員。知悉後，Curtain客戶端的狀態會轉成"已轉移"。當所有的Curtain客戶端的狀態都會轉成"已轉移"後，管理員可以將舊的Curtain管理員關機，所有的Curtain客戶端正式被新的Curtain管理員管理。



- 完成遷移

備註: 新的Curtain管理員必須使用與舊的Curtain管理員使用的"授權字符串"一樣。

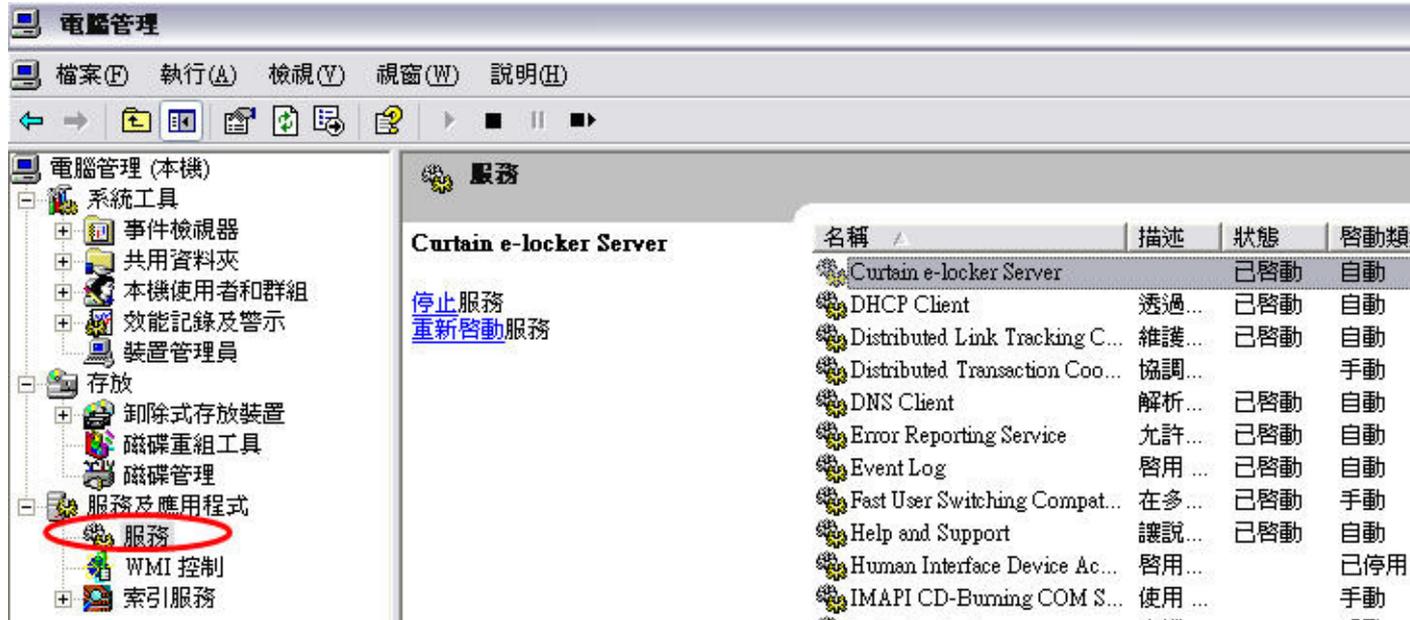
7.3 - 手動備份與恢復Curtain管理員的安全策略和活動記錄

備份安全策略和活動記錄:

- 將現時Curtain管理員上的安全策略先作備份，請將以下文件夾和文檔複製一份。
 - 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
- 將現時Curtain管理員上的活動記錄先作備份，請將以下文檔複製一份。
 - C:\Program Files\Coworkshop\Curtain 3\bin\Curtain.mdb (它存在於舊版本中)
 - 將整個 "Curtain" 文件夾備份
 - 於Windows 2000 / XP / 2003，此文件夾位於 C:\Documents and Settings\All Users\Application Data
 - 於Windows 2008 / 2010 / Vista / Win7 / Win8 / Win10，此文件夾位於 C:\ProgramData

恢復安全策略和活動記錄:

- 於電腦管理，將"Curtain e-locker Server"服務停止。
- 將之前備份好的文件夾和文檔複製到相關位置。
- 於電腦管理，將"Curtain e-locker Server"服務啟動。



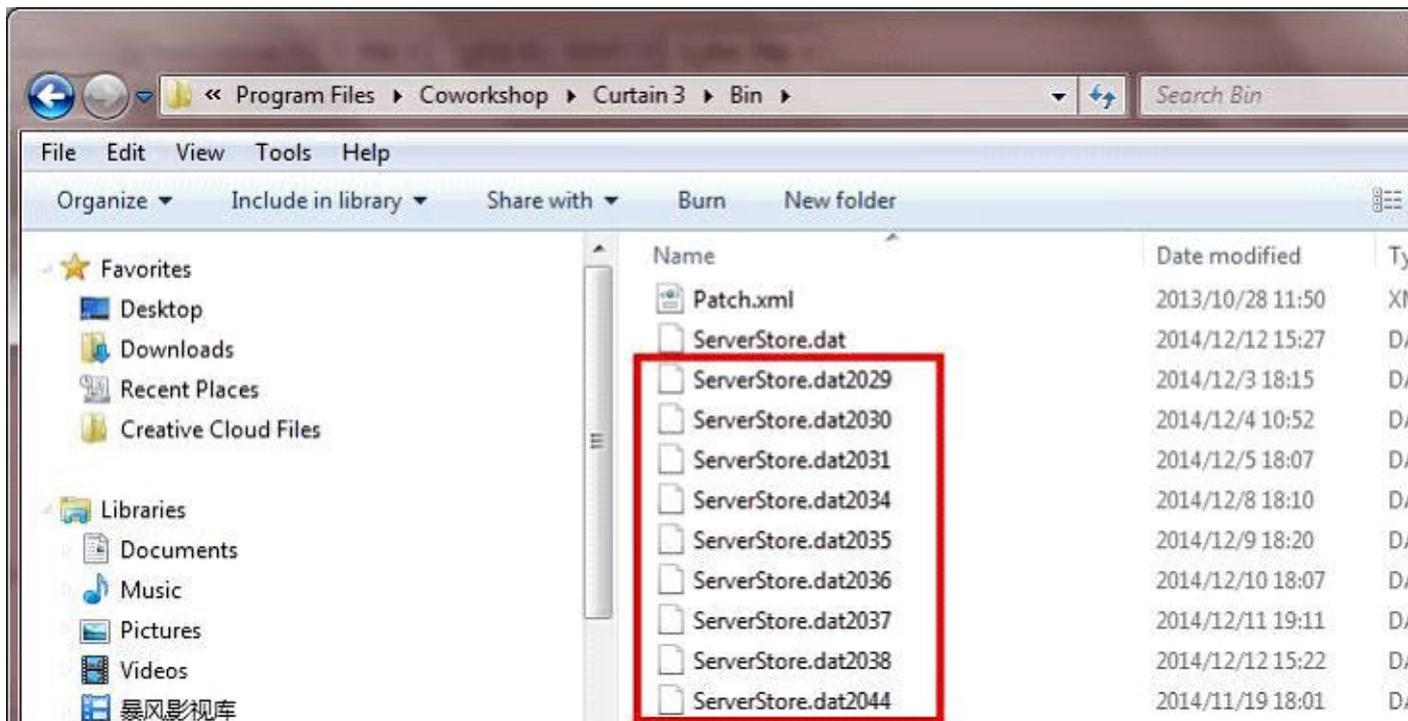
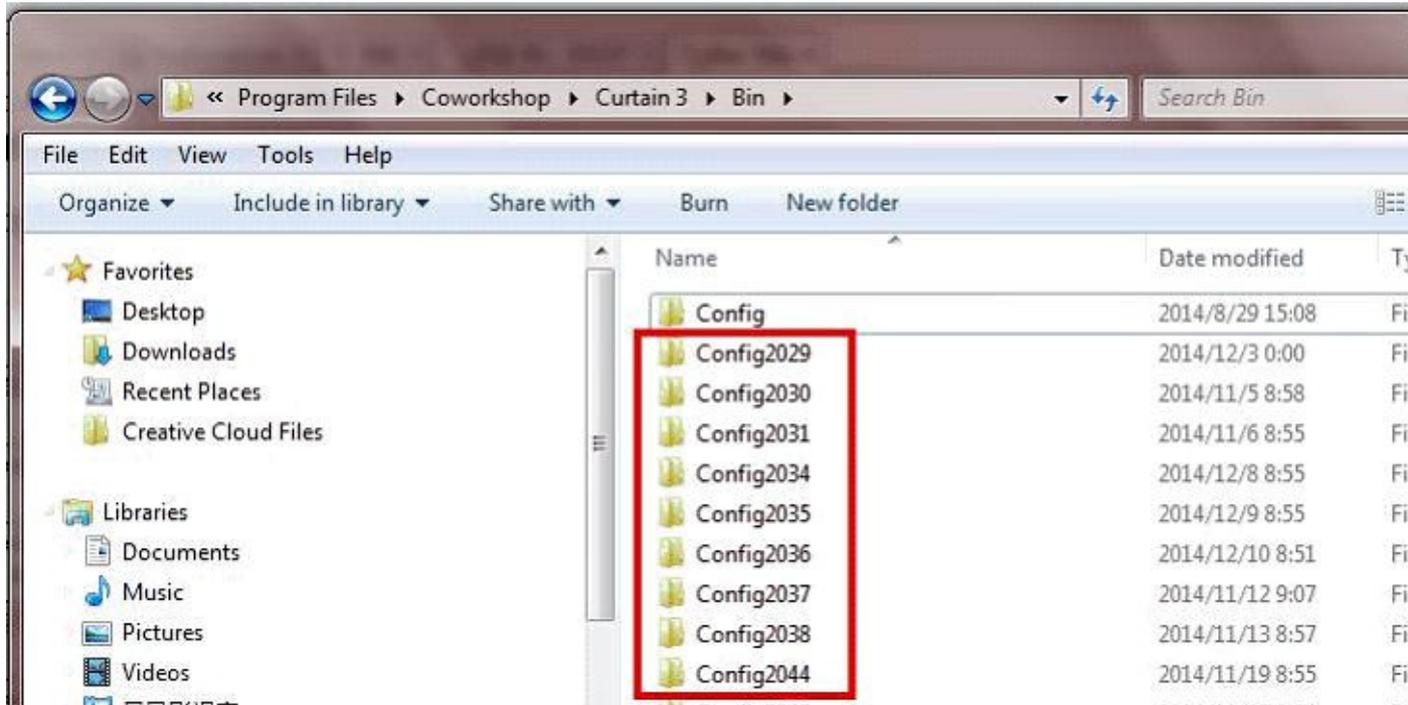
7.4 - 自動備份Curtain管理員的安全策略

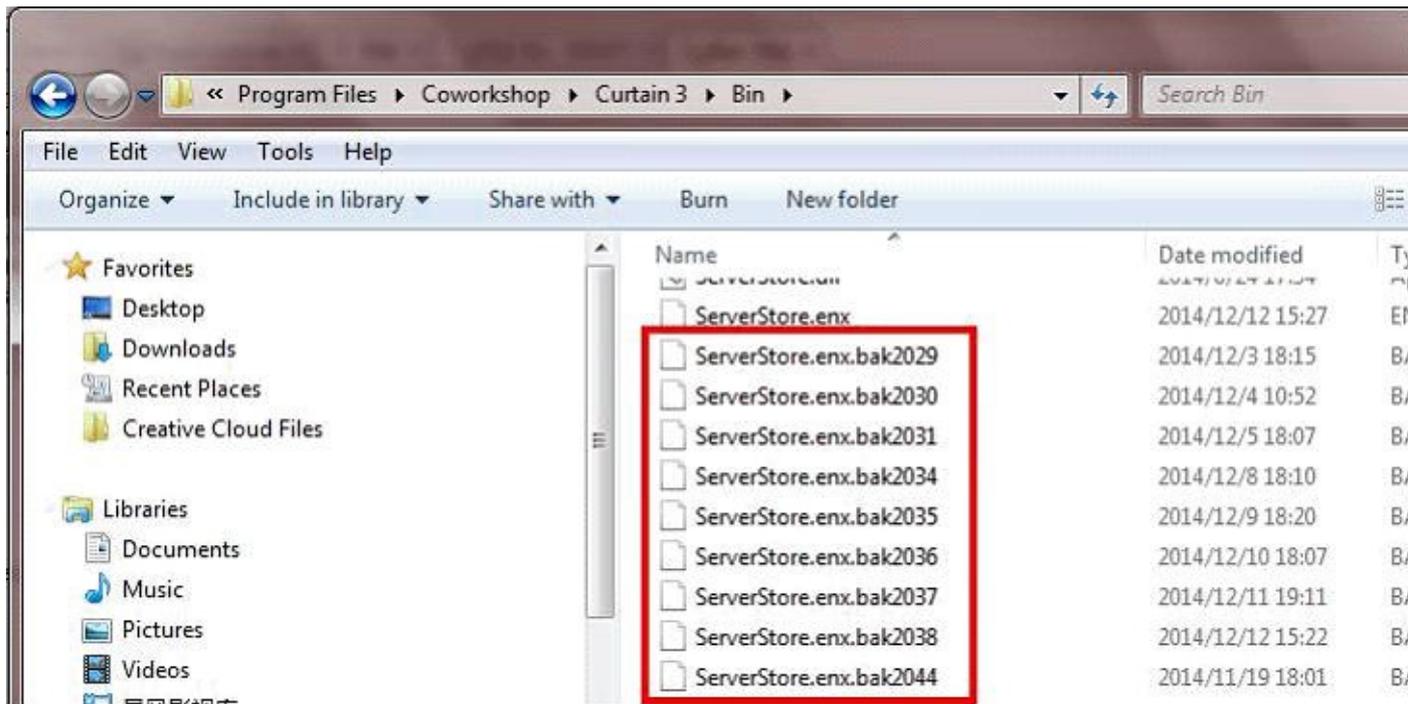
Curtain管理員有自動備份安全策略的功能，如果因為突發狀況而導致策略被損壞(如:異常關機)，管理員可以手動恢復安全策略。

安全策略是儲存在以下文件夾和文檔中：

- 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

在相關位置，你可以找到相同名稱的文件夾和文檔其後綴名會以數字編號標識(如下圖)，你可以按最後修改日期找出希望恢復的安全策略。





恢復安全策略:

- 於電腦管理，將"Curtain e-locker Server"服務停止。
- 將要恢復的安全策略的文件夾和文檔，重命名原名稱即可。
- 於電腦管理，將"Curtain e-locker Server"服務啟動。

重新開啟Curtain管理端，會發現之前的策略和設置已經全部還原。

8 - 常見問題

8.1 - 如何避免和殺軟沖突？

如今市場上流行的殺毒軟體有很多，例如趨勢(Trend Micro)·卡斯基(Kaspersky)·邁克菲(Mcafee)·360殺毒·愛維士(Avast)·AVG·金山毒霸等·有些殺毒軟體不需要更改任何設置即可和Curtain客戶端完美兼容·而有些殺毒軟體則需要設置Curtain客戶端相關文檔為“信任”或“例外”才能正常工作。以下是相關文檔清單和路徑：

Curtain 驅動路徑及文檔路徑：

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

如果殺毒軟體不允許添加路徑，那麼需要手動添加以下EXE執行檔：

- 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

備註: 包括C:\Program Files\Coworkshop\Curtain 3\CBin\和C:\Program Files (x86)\Coworkshop\Curtain 3\CBin\目錄下所有的EXE文件。

8.2 - 使用易鎖通過iSCSI來保護NAS

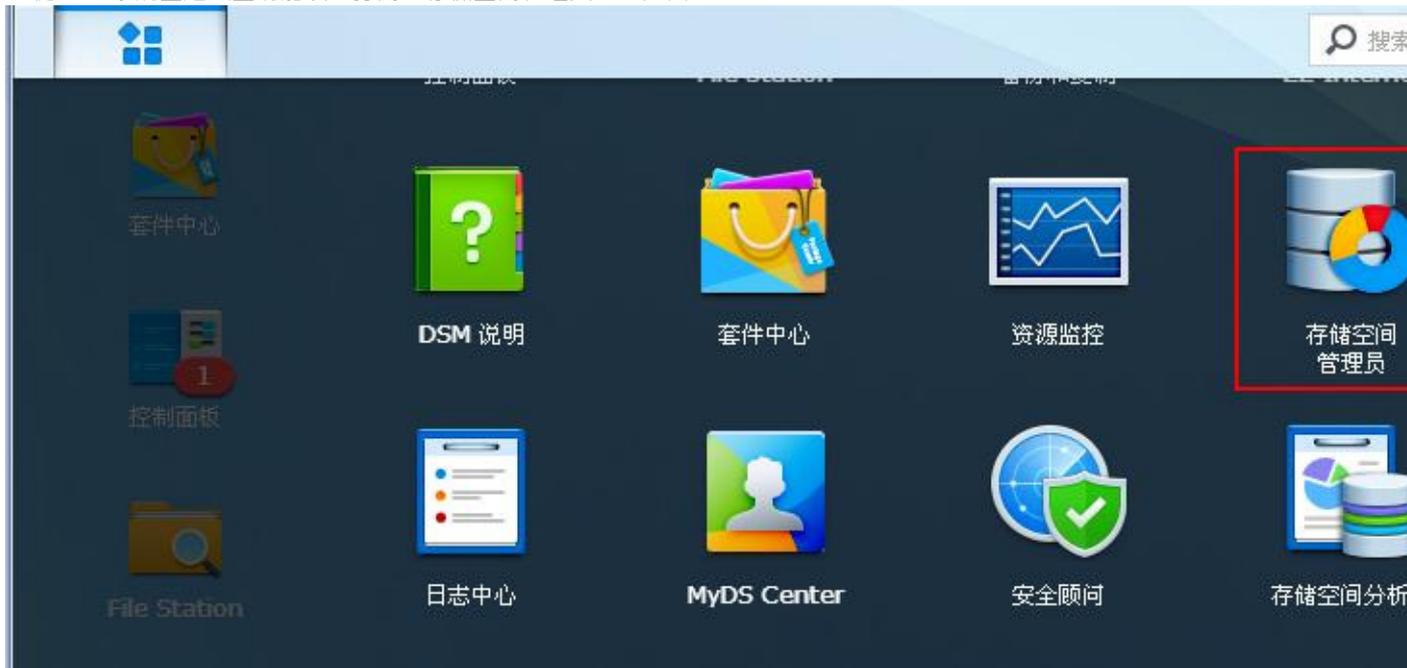
背景

目前大多數NAS存儲服務器都運行Linux，並不允許人們在NAS上安裝軟件，這意味著我們無法在NAS上安裝Curtain服務器插件來保護共享文件夾。故此，我們可以通過iSCSI將其作為本地虛擬磁盤掛載到Windows服務器上來保護NAS。首先，您需要在NAS上創建iSCSI LUN (邏輯單元)，然後使用Windows iSCSI Initiator在Windows服務器上創建虛擬磁盤。最後，您可以共享虛擬磁盤並通過Curtain e-locker進行保護。

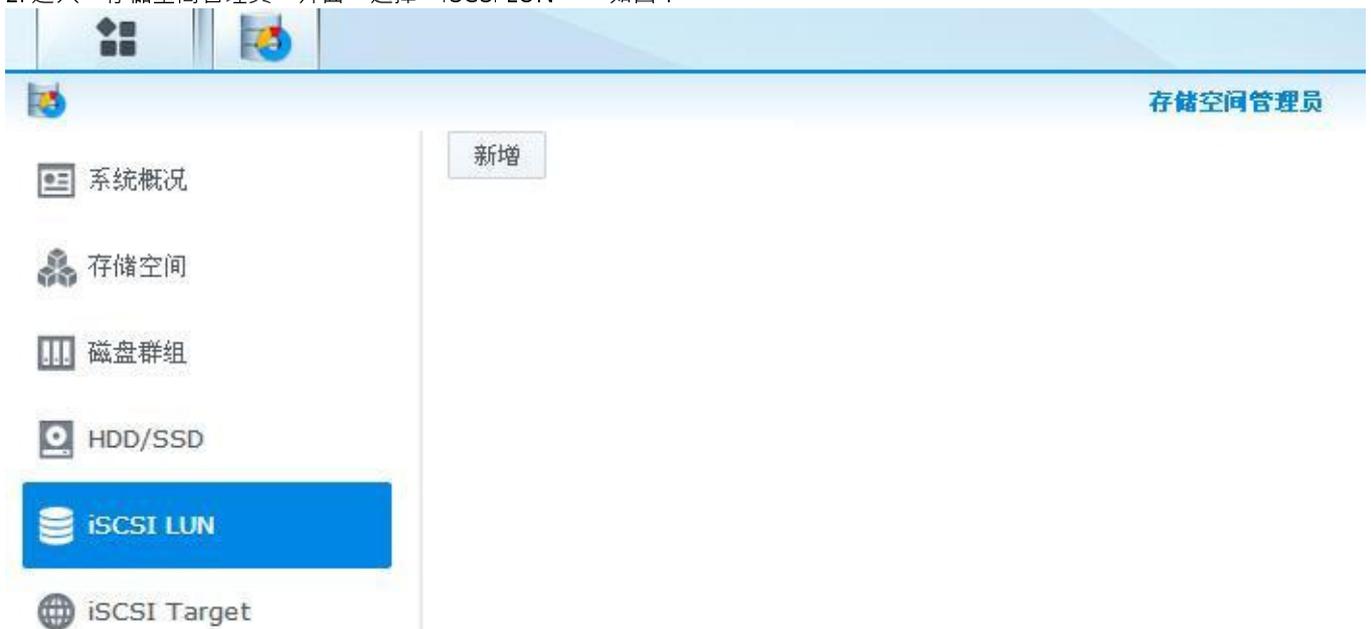
備註: 我們使用Synology DiskStation演示如何進行設定，如果使用其他NAS服務器，界面和命名將會不同。

創建iSCSI Target

1. 從DSM系統上進入主功能表，打開“存儲空間管理員”，如圖：



2. 進入“存儲空間管理員”介面，選擇“iSCSI LUN”。如圖：



3. 按一下“新增”按鈕，將會彈出設置窗口，引導創建“SCSI LUN”，選擇LUN類型為“iSCSI LUN(一般檔)”，按一下“下一步”。如圖：



iSCSI LUN 创建向导

选择 LUN 种类

iSCSI LUN (一般文件)
此形式的 iSCSI LUN 不仅提供弹性且动态的容量管理，且具备 Thin Provisioning 功能。

iSCSI LUN (段落分块) - 使用所有硬盘容量的 LUN
此形式的 iSCSI LUN 能提供最佳的访问性能。

名称:

iSCSI Target 链接:

iSCSI LUN (段落分块) - 可弹性使用部份磁盘群组容量的 LUN
此形式的 iSCSI LUN 创建在磁盘群组上，提供动态调整容量的弹性与优化的访问性能。

名称:

iSCSI Target 链接:

下一步 取消

4. 設置iSCSI LUN屬性，容量大小由管理員設定，以“G”為單位，其他設置保持不變，按一下“下一步”。如圖：



The screenshot shows a window titled "iSCSI LUN 创建向导" (iSCSI LUN Creation Wizard) with a sub-header "设置 iSCSI LUN 属性" (Set iSCSI LUN Properties). The form contains the following fields:

名称:	LUN-1
位置:	存储空间 1 (可用容量: 484 GB)
Thin Provisioning:	是
容量 (GB):	100
iSCSI Target 链接:	新增一个 iSCSI target

At the bottom of the window, there are three buttons: "上一步" (Previous Step), "下一步" (Next Step), and "取消" (Cancel). The "下一步" button is highlighted in blue.

5. 勾選“啟用CHAP”，並輸入名稱和密碼，按一下“下一步”。如圖：



The screenshot shows a window titled "iSCSI LUN 创建向导" (iSCSI LUN Creation Wizard) with a close button (X) in the top right corner. The main heading is "新增一个 iSCSI target" (Add a new iSCSI target). The form contains the following fields:

- 名称 (Name): Target-1
- IQN: iqn.2000-01.com.synology:NAS01.
- 启用 CHAP (Enable CHAP)
- 名称 (Name): Target1
- 密码 (Password): [Redacted]
- 确认密码 (Confirm Password): [Redacted]
- 启用相互 CHAP (Enable Mutual CHAP)
- 名称 (Name): [Empty]
- 密码 (Password): [Empty]
- 确认密码 (Confirm Password): [Empty]

At the bottom, there are three buttons: "上一步" (Previous Step), "下一步" (Next Step), and "取消" (Cancel).

6. 再次檢查設置，如果確認沒有問題，按一下“下一步”。如圖：



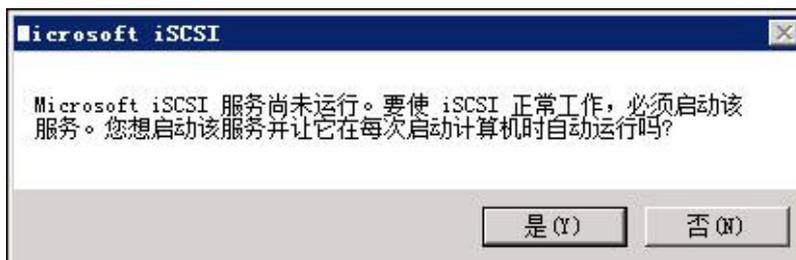
7. 在“存储空间管理员”介面上，你可以看到創建好的iSCSI LUN。如圖：



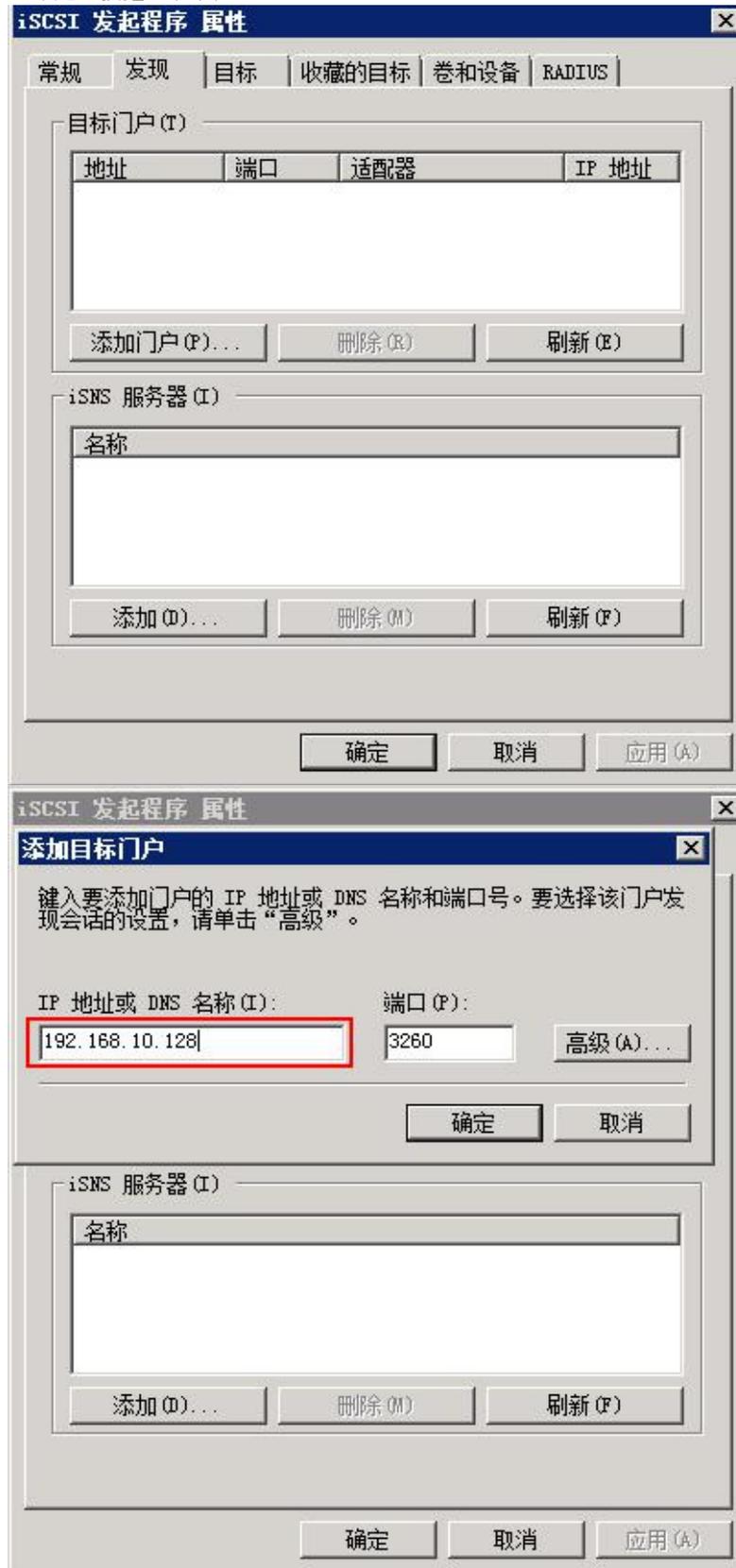


映射iSCSI Target到伺服器本地虛擬磁盤

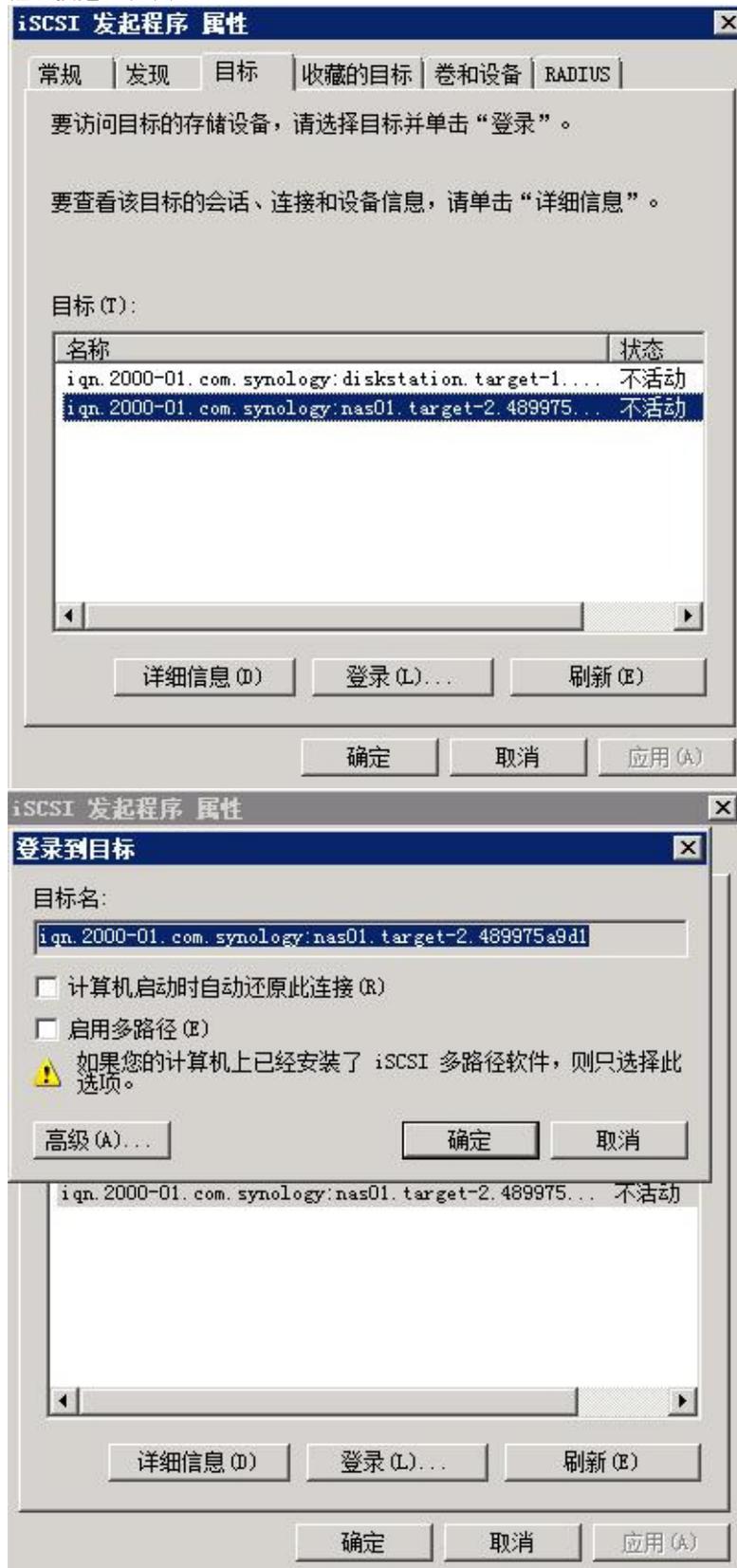
8. 在Windows伺服器中，依次打開“開始功能表> 管理工具> iSCSI發起程式”，如果是第一次啟用iSCSI服務，將會彈出對話方塊，按一下“是”即可。如圖：



9. 在“iSCSI發起程式”屬性介面，選擇“發現”，並按一下“添加門戶”，並輸入NAS的IP位址，然後按一下“確定”按鈕。如圖：

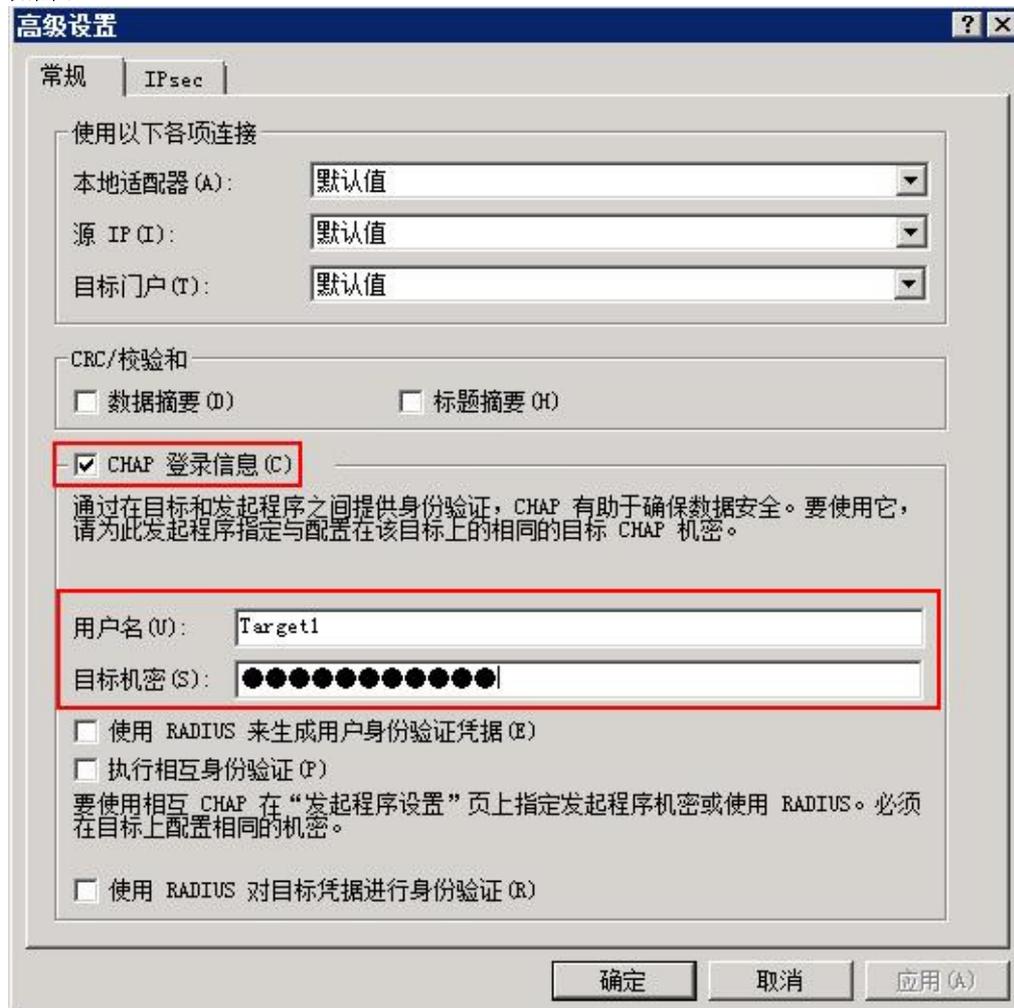


10. 在“iSCSI發起程式”屬性介面，選擇“目標”，將會發現目標已添加，但狀態顯示“不活動”，按一下“登陸”按鈕。如圖：

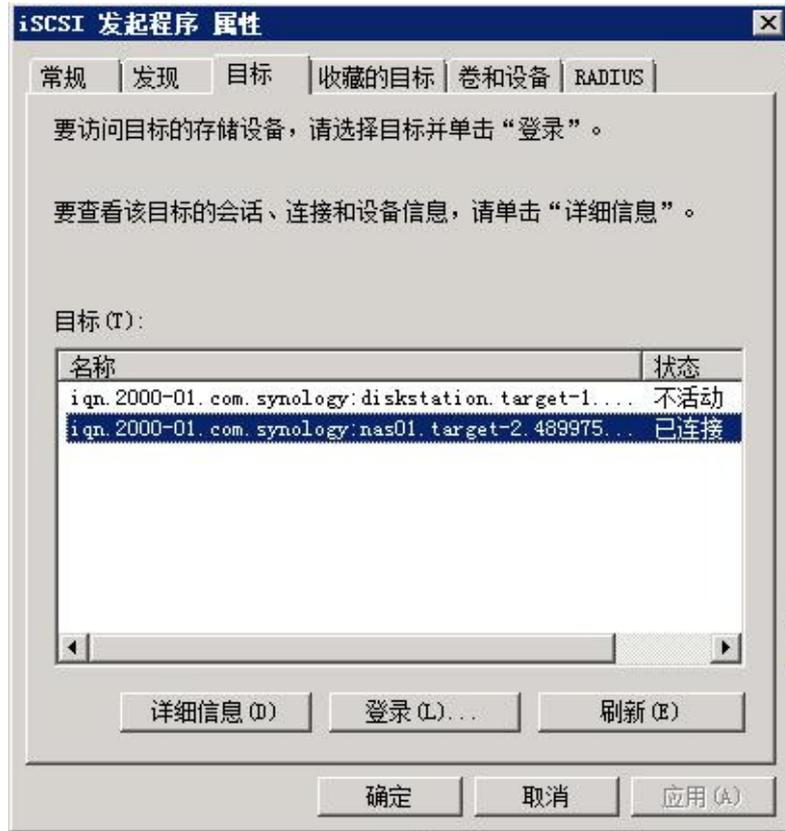


11. 繼續按一下“高級”按鈕，勾選“CHAP登錄資訊”，填入使用者名和密碼（見步驟5），然後按一下“確定”按鈕。

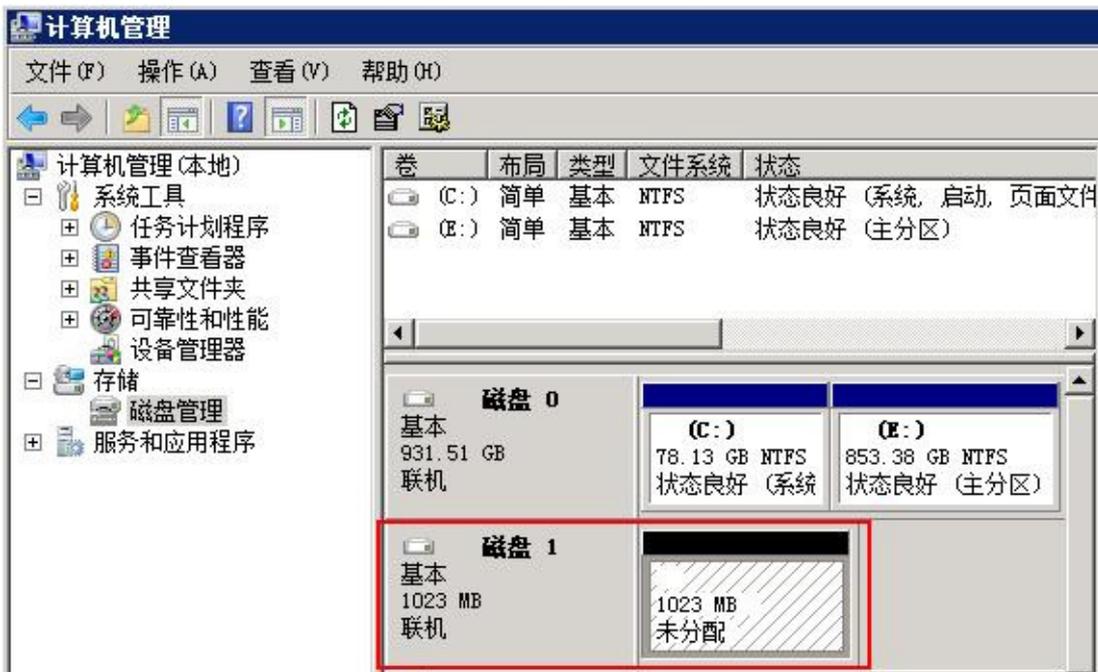
如圖：



12. 如果登錄驗證成功，目標狀態將更改為“已連接”，按一下“確定”推出。如圖：

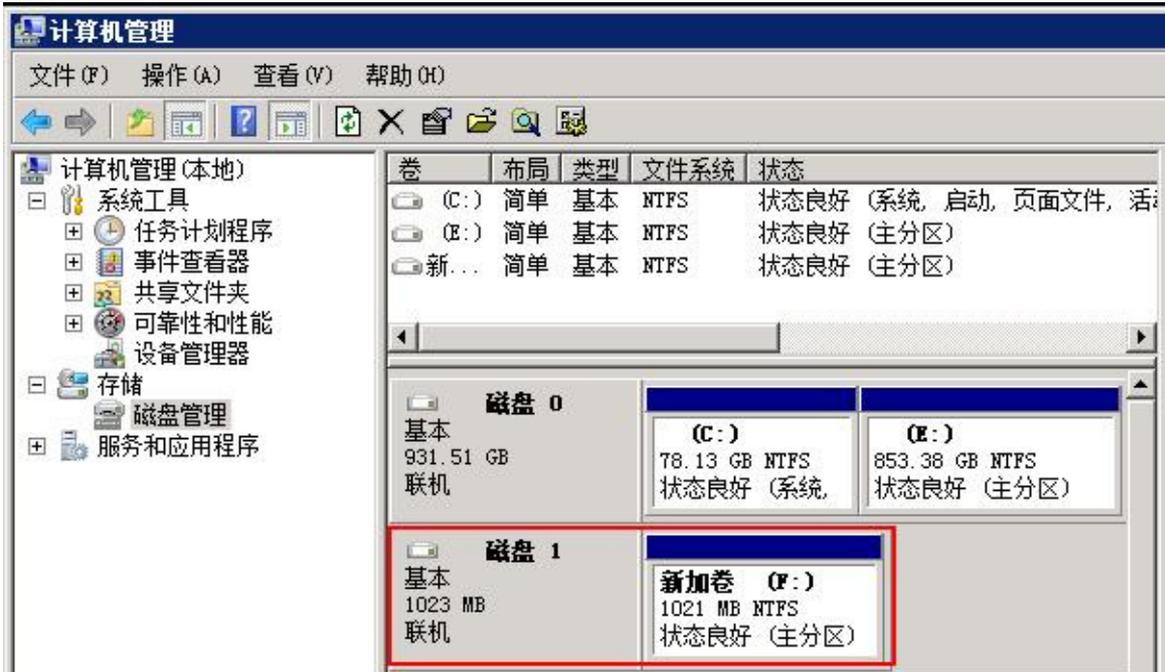


13. 打開“電腦管理>磁盤管理”程式，新磁盤映射成功，但還未分配。如圖：



14. 選擇該磁盤並按右鍵，創建“新建簡單卷”，按一下“下一步”直至創建完成。

如圖：



共享磁盤並設置保護

15. 選中該磁盤並右鍵查看“屬性”，將該磁盤設置為共享。

16. 打開Curtain管理員，設置該磁盤為受保護網路磁盤。

17. 重新運行Curtain用戶端並映射網路磁盤，使用資源管理器進入該網路磁盤，並嘗試新建資料夾，如果創建失敗，說明磁盤已被Curtain保護。

備註: 原來NAS共享文件夾許可權需要重新在Windows伺服器上手動設置。

8.3 - 啟動或停止Curtain除錯日誌

請按以下步驟啟動或停止Curtain除錯日誌:

1. 啟動Command Prompt (於 "開始> 程式> 附屬應用程式" 下)
2. 輸入"regedit"啟動Registry Editor
3. 選擇 \HKEY_LOCAL_MACHINE\SOFTWARE\Coworkshop\Curtain 3
4. 啟動或停止Curtain除錯日誌:
 - 啟動日誌 · 設定DebugLog = a
5. 重現問題
6. 將錯誤日誌文件復制壓縮后發送給Curtain技術支援中心。

Vista以上系統除錯日誌的位置:

- \\installation path\Coworkshop\Curtain 3\cbin\log
- \\Users\username\CurtainLog

Vista以下系統除錯日誌的位置:

- \\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位操作系統)
 C:\Users\tester\CurtainLog

備註 : 對於64位操作系統 · 請發送在 "Program Files"和"Program Files (x86)"下日誌。

7. 操作完成后 · 請記得停止除錯日誌 :
 停止日誌 · 設定DebugLog = 0

備註: 請緊記在使用除錯日誌後將它停止 · 因為除錯日誌會佔用硬盤不少空間。

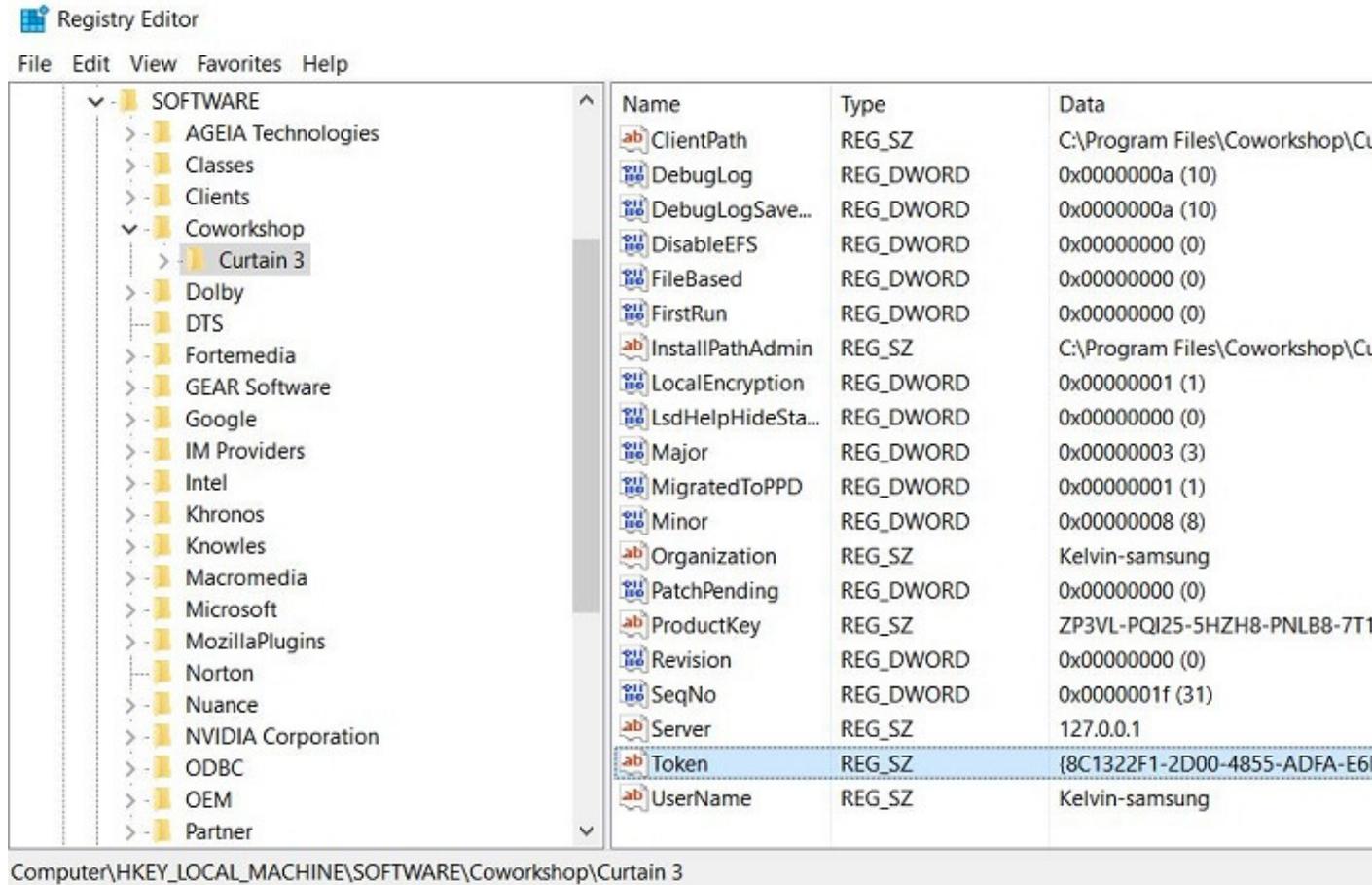
8.4 - 針對克隆的Curtain客戶端生成唯一令牌

Curtain客戶端安裝後會生成一個獨一無二的令牌 (GUID全局唯一標識符) · 由於克隆的系統會保持令牌不變 · 故需使用ReGenToken.exe工具重新生成。

請按以下步驟自動生成Token:

1. 在安裝Curtain客戶端的工作站中 · 雙擊運行ReGenToken.exe工具。
2. 系統會提示 "生成令牌並設置成功" 。
3. 請到Curtain客戶端和Curtain管理端檢查令牌是否被改變。

檢查Curtain客戶端：



檢查Curtain管理端：



備註：該工具ReGenToken.exe分為3272版本和3273版本，請根據安裝的Curtain客戶端版本決定。

下載鏈接：

[ReGenToken.exe tool](#)

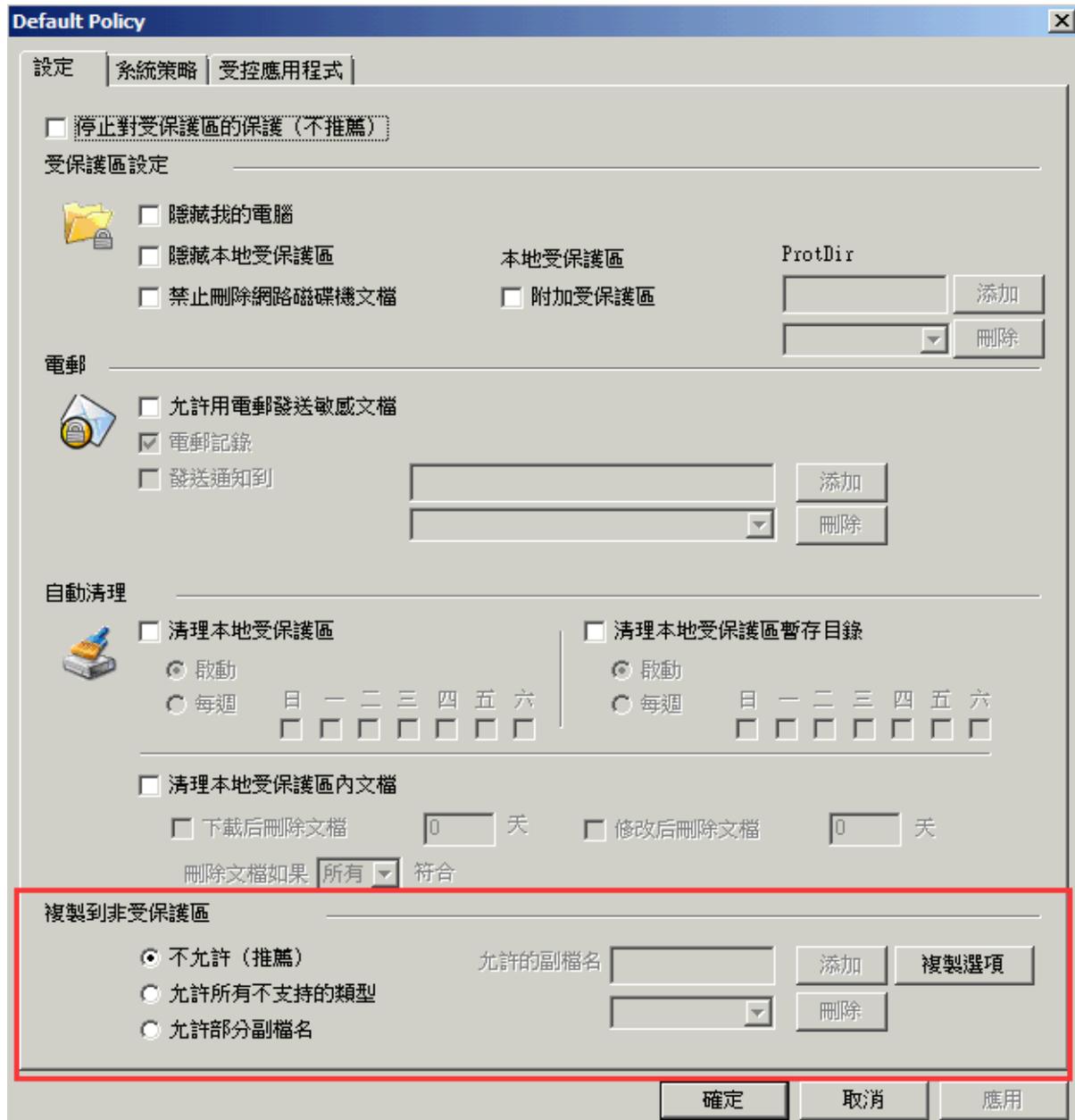
<http://www.coworkshop.com/download/ReGenToken.zip>

9 - 最佳實踐

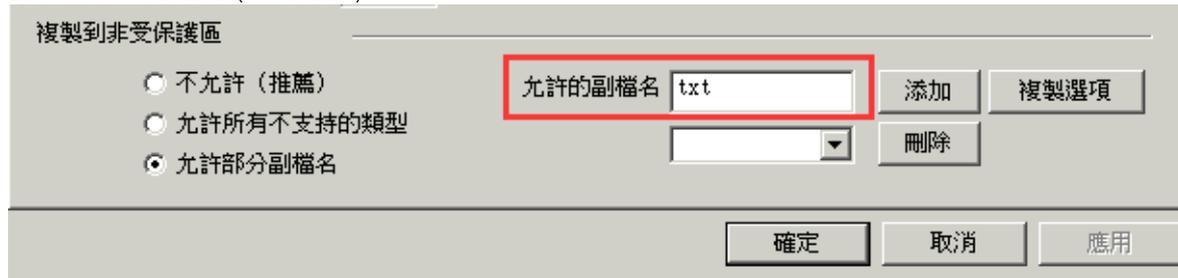
9.1 - 允許受保護文件從安全區復制/發送出去

授權用戶從安全區復制/發送文件到非受保護區的步驟：

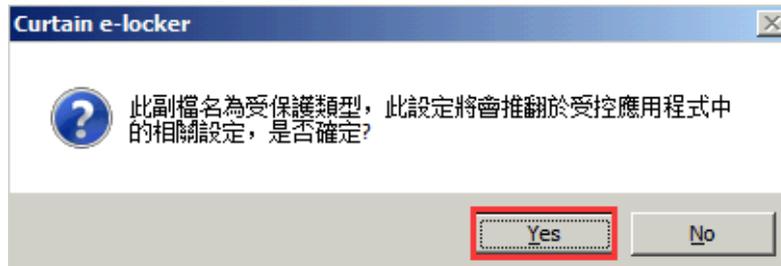
1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵，並選擇"內容">"復制到非受保護區"。



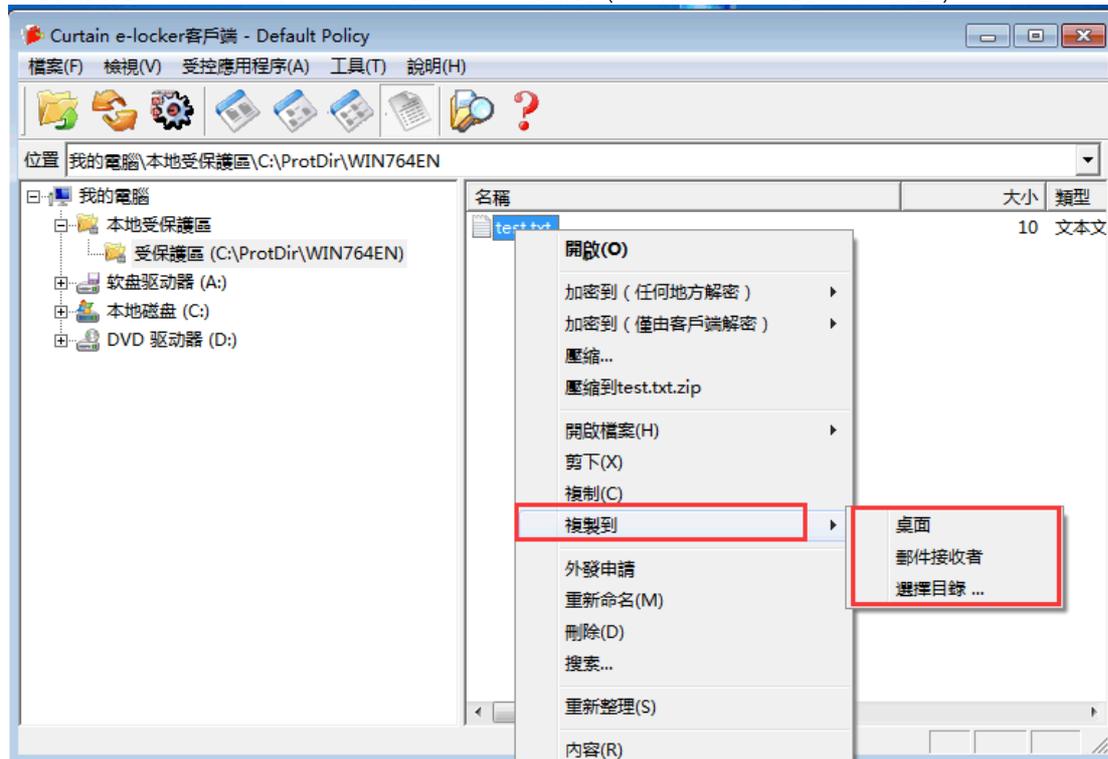
2. 添加允許的副檔名 (例如:TXT) 。



3. 單擊“添加”按钮，再確認。



4. Curtain客戶端表現：用戶右鍵單擊txt文件 -> 復制到 (此時文件可複製到非受保護區) 。



備註：請記住，此設置將覆蓋應用程序控制中的設置。例如，如果您不允許該組在MS Excel中保存/複製文件，但允許複製XLS文件，則後者設置將覆蓋前者的設置。

9.2 - 如何設置對 SolidWorks Enterprise PDM的保護？

對 SolidWorks EPDM 設置保護的大概步驟：

1. 於Curtain 管理員，添加 EPDM 伺服器為受保護區。
2. 於用戶電腦，通過受保護的EPDM View Setup把Local File Vault位置設定到本地受保護區下的文件夾。
3. 完成

詳細設置步驟：

步驟 1：在 Curtain 管理員，添加 EPDM 伺服器為受保護區。

1.1. 在 Curtain 管理員，於功能表上選擇“文件 > 設置”。

1.2. 在“伺服器信息”頁，按“添加”按鈕來新增 EPDM 伺服器。

伺服器位址：EPDM 伺服器的電腦名稱或 IP 位址。

埠：預設的埠是 8443（用作 Curtain 管理員和 Curtain 伺服器插件之間的溝通）。



1.3. 按確定鍵確認。

1.4. 保護EPDM 伺服器的網路埠。

- 於“受保護網路埠”，點選“允許保護”。
- 按“添加”按鈕，系統會彈出對話框（如圖）。

設定



位址 - 選擇 EPDM 伺服器（電腦名稱或 IP 位址）

埠 - 輸入 3030（EPDM 的預設值是 3030）

協議 - 選擇 TCP（EPDM 的預設協議是 TCP）

1.5. 按確定鍵確認。

步驟 2. 於用戶電腦，通過受保護的 EPDM View Setup 把 Local File Vault 位置設定到本地受保護區下的文件夾。

- 如果你的電腦會跟其他 EPDM 用戶共同使用，你需要使用附加安全區，因為用戶甲不能訪問用戶乙的本地受保護區。請繼續按步驟 2.1。
- 如果你的電腦不會有多個用戶共同使用 EPDM，請跳到步驟 2.4 繼續。

2.1. 在Curtain管理員，點選一個安全策略，按滑鼠右鍵，並選擇“內容”。

2.2. 於“設定”頁:

- 選擇“附加受保護區”，並輸入路徑。
- 按“添加”按鈕確定。



2.3. Curtain管理員添加完成以後，客戶端在下次啟動，附加保護區就會顯示在客戶端內，如下圖所示：



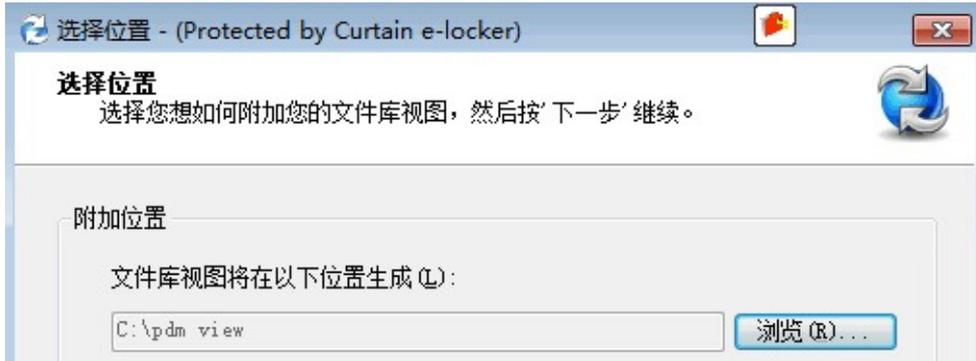
2.4. 於“開始”菜單，選擇“所有程式 > Coworkshop Curtain e-locker > Secure Applications”。



2.5. 開啟Secure EPDM View Setup。



2.6. 把Local File Vault位置設定到本地受保護區下的文件夾。



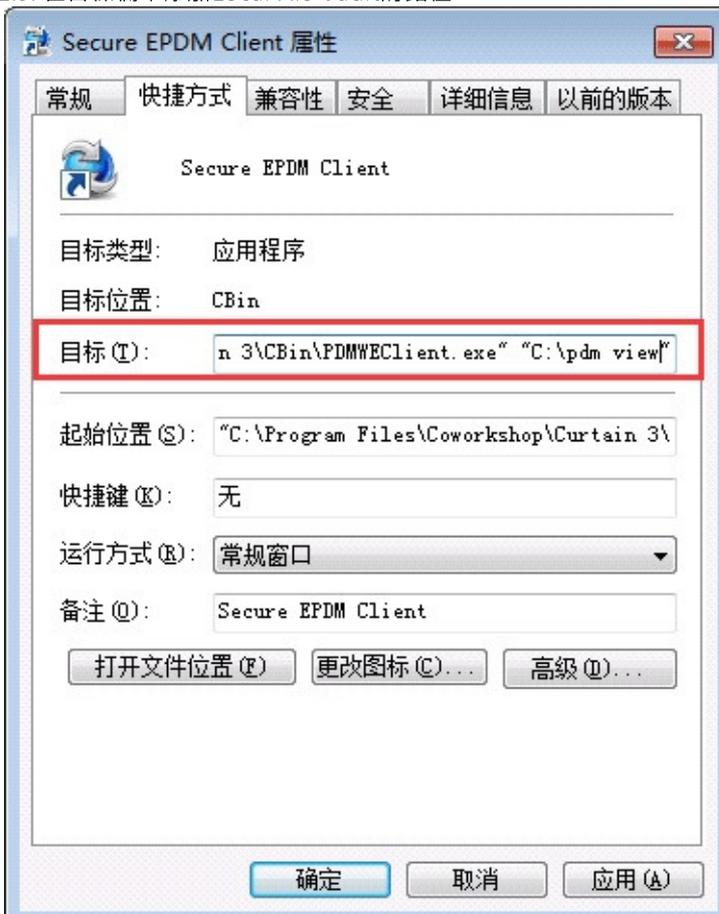
備註：如果你的電腦會跟其他 EPDM 用戶共同使用，你需要把Local File Vault位置設定到附加安全區。

2.7. 於“開始”菜單，選擇“所有程式 > Coworkshop Curtain e-locker > Secure Applications”。

2.8. 右鍵點選Secure EPDM Client快捷方式，選擇“屬性”。



2.9. 在目標欄中添加Local File Vault的路徑。



備註：

- 請確保你已經用 Secure EPDM View Setup 把此路徑設定為 Local File Vault。

2.10. 通過 Secure EPDM Client 來使用 EPDM 系統。

