

# Curtain<sup>™</sup> 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)的一切條文及細側,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/用户到合適的安全策略	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

<u> </u>	urtain o-lockor ( 見 4 ) 5 0 _ 安 恭 论 印書	iv
	8.3 - 啟動或停止 Curtain 除錯日志	126
	8.2 - 使用易鎖通過 i SCSI 來保護 NAS	114
	8.1 - 如何避免和殺軟沖突?	114



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,這方面正正就是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。

版	共用	安全性	自訂			
詳組。	或使用者名	名稱(G):				
808	Administra normal (V) SYSTEM	ttors (VM-X M-XPTC\nc	PTC\Adm ormal)	inistrators)		
1	Users (VM	-XPTC\Use	rs)			
			-			
				新增(D)		<u>R)</u>
Jsers	的權限的	)		新增( <u>D</u> ) た許	」 <u>移</u> 除( 拒絕	<u>R</u> )
Jsers 完:	的權限(型 全控制	)		新增(D)	」 <u>移除(</u> 拒絕	<u>R)</u>
Jsers 完: 修i	的權限(P) 全控制 改	)		新增(D)		
Jsers 完: 修i 讀」	的權限(P) 全控制 改 取及執行	)		新增 <u>(D)</u> <u> </u>		<u>R</u> )
Jsers 完: 修讀 清:	的權限( <u>P</u> ) 全控制 改 取及執行 單資料夾(	) <b>入</b> 容		新增(D)		<u>R</u> )
Jsers 完修讀 清 讀	的權限( <u>P</u> ) 全控制 改 取及執行 單資料夾( 取	) <b></b> 內容		新增(D)		R)
Jsers 完修讀 清讀 寫	的權限(P) 全控制 改 取及執行 單資料灭( 取 入	) 內容		新増(D) た許 □ マ マ		
Jsers 完修讀 清 讀 寫 時	的權限(2) 全控制 改取及執行 單資料夾「 單資料夾「 取 入	) 內容		新増(D) た許 □ □ マ □ □		
Jsers 完修讀 清讀 寫 時 殊	的權限(2) 全控制 改及及執行 取及及執行 取入 社都限 又 社都限 或進	) 內容 皆設定請拔	:〔進階]。	新増D		

### 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
- 複制粘貼
- 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。



### 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。



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-安装前的準備

# 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,將文檔內容複制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"複制到"選項。你可以使用此功能 將文檔複制到受保護區之外。

文檔被複制到受保護區之外後:

- 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

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防火墻>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】。

💣 新建入站规则向导		×
<b>規则类型</b> 选择要创建的防火墙规则类型		
步骤:         ● 規则类型         ● 协议和端口         ● 操作         ● 配置文件         ● 名称	要创建的规则类型 • <b>和存</b> , 控制程序连接的规则。 • <b>端口(0)</b> 控制 TCT 或 UDT 端口连接的规则。 • <b>存定文(C)</b> 如TTS 对等缓存 控制 Windows 体验功能连接的规则。 • <b>自定</b> 义规则。	
	< 上一步 (B) 【下 <b>一步 (X)</b> >	]

3. 在"特定本地端口"內輸入 "24821",點擊【下一步】。

💣 新建入站规则向导		×
<b>协议和端口</b> 指定此规则匹配的协议和端		
<b>步骤</b> : ・ 規则类型 ・ 协议和端口 ・ 操作 ・ 配置文件 ・ 名称	<ul> <li>该规则应用于 TCP 还是 WDP?</li> <li>C TCP</li> <li>UDP</li> <li>该规则应用于所有本地端口还是特定本地端口?</li> <li>所有本地端口(A)</li> <li>特定本地端口(S): 24821 元例: 80. 443, 8080</li> </ul>	
	<u>了解协议和端口的详细信息</u>	
	< 上一步 (B) 【下一步 (N) >	>

4. 選擇"允許連接",點擊【下一步】。

💣 新建入站规则向导		x
<b>操作</b> 指定在连接与规则中指定的	的条件相匹酉时要执行的操作。	
步骤:         • 规则类型         • 协议和端口         • 操作         • 配置文件         • 名称	<ul> <li>连接符合指定条件时应该进行什么操作?</li> <li>6 允许在我(A)</li> <li>优许使用 IPsec 保护以及未保护的连接。</li> <li>7 <b>9.7公子公子在名(7)</b></li> <li>四方注使用 IPsec 进行身份验证以及完整性保护的连接。使用 IPsec 属性中的设置以及连接安全规则节点中的规则的连接将受到保护。</li> <li>「 等代用 IPsec 萬行身份验证及隐私。</li> <li>「 零代用 IPsec 制约 最近 及隐私。</li> <li>「 零代用 IPsec 制约 最近 及隐私。</li> <li>「 常代用 IPsec 制约 最近 及隐私。</li> <li>「 常代用 IPsec 制约 最近 及隐私。</li> <li>「 常代用 IPsec 制约 最近 及隐私。</li> <li>「 常代 用 IPsec 制约 最近 及隐私。</li> <li>「 常代 用 IPsec 制约 最近 及隐私。</li> <li>「 都代 用 IPsec 制约 是一个人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人</li></ul>	
	< 上一步 (8) 下一步 (8) 入 取消	

5. 如圖所示默認勾選上"域", "專用", "公用", 點擊【下一步】。

💣 新建入站规则向导		×
<b>配置文件</b> 指定此规则应用的配置文件	ŧ×	
步骤:         • 规则类型         • 协议和端口         • 操作         • 配置文件         • 名称	<ul> <li>何时应用该规则?</li> <li>戶 何()</li> <li>近 前机连接到其企业域时应用。</li> <li>戶 有用()</li> <li>近 有用()</li> <li>计算机连接到公用网络位置时应用。</li> <li>1</li> <li>1</li></ul>	
	<_	上一步 (8) 下一步 (8) > 取消

### 6. 在名稱內輸入"Curtain",點擊【完成】。

🌧 新建入站规则向导		X
<b>名称</b> 指完业规则的复数和描述。		
指定式规则的名称中相通还。 <b>步骤:</b> <ul> <li>规则类型</li> <li>协议和端口</li> <li>操作</li> <li>配置文件</li> </ul>	名称(M): Curtain	
✓ - 益利/i	描述 (可选) (0):	
	< 上一步 (B) 二 完成 (P) 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。

■ 服务器管理器 文件(F) 操作(A) 杏毛(V) 邦	ah an						
	aj (1)						
■ 服务器管理器 (M32₩21X8)	入站规则						
	名称	组 -	配置文件	已启用	操作	替代	程序
田 御 切胞	Curtain		任何日期	是	允许	否	任何日
は 100 100 100 100 100 100 100 100 100 10	🔮 BITS 对等缓存(Conte	BITS 对等缓存	任何日期	否	允许	否	System
□ ■16 目□ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □ □	🔮 BITS 对等缓存(RPC)	BITS 对等缓存	任何日期	否	允许	否	%Syst.
日 🍻 高级安全 Windows 防火t	🔮 BITS 对等缓存 (RPC-E	BITS 对等缓存	任何日期	否	允许	否	%Syst.
11.11、公工	🔮 BITS 对等缓存(WSD-In)	BITS 对等缓存	任何日期	否	允许	否	%Syst.
🕵 出站规则	ⓓ COM+ 网络访问(DCOM-In)	COM+ 网络访问	任何日期	否	允许	否	%syst.
🔚 连接安全规则	🔮 iSCSI 服务(TCP-In)	iSCSI 服务	任何日期	否	允许	否	%Syst.

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..."

Windows Firew	all	
eneral Exceptions	Advanced	
Vindows Firewall is programs and servic o work better but mi Programs and Servic	blocking incoming network connections, except for the es selected below. Adding exceptions allows some progr ght increase your security risk.	ams
Name	~~	^
<ul> <li>✓ curtain24822</li> <li>✓ curtain24821</li> <li>✓ curtain24821</li> <li>✓ curtain24821</li> <li>✓ File and Printer</li> <li>✓ Kaspersky Adm</li> <li>✓ Kaspersky Adm</li> </ul>	Sharing inistration Kit inistration Kit	100
Kaspersky Adm     Network Diagn     Remote Assista     Remote Desktr	inistration Nit ostics for Windows XP ince	*
Add Program Display a notifica	Add Port       Edit       Delete         tion when Windows Firewall blocks a program         f allowing exceptions?	
		ncel

2. 給此例外輸入名稱、端口為TCP的24821,並按OK確定。

Edit a Port	
Use these settings number and protoc want to use.	to open a port through Windows Firewall. To find the port ol, consult the documentation for the program or service you
Name:	burtain24821
Port number:	24821
What are the risks	of opening a port?
Change scope	OK Cancel

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
- UDP的24822
   UDP的24822
   TCP的24821
   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防火墙>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】。

💣 新建入站规则向导			×
<b>規则类型</b> 选择要创建的防火墙规则类型			
步骤:         ● 规则类型         ● 协议和端口         ● 操作         ● 配置文件         ● 名称	要创建的规则类型 宁 程序(P) 控制程序连接的规则。       守 端口(O) 按制 TCP 或 UDP 端口连接的规则。       伊定义(E):       PITS 对等缓存 控制 Windows 体验功能连接的规则。       合 自定义(C) 自定义规则。       了解规则类型的详细信息		Y
		<上一步(B) 下一步(N) >	取消

3. 在"特定本地端口"內輸入 "24822",點擊【下一步】。

💣 新建入站规则向导	×
<b>协议和端口</b> 指定此规则匹配的协议和端口	0
步骤:         • 规则类型         • 协议和端口         • 操作         • 配置文件         • 名称	<ul> <li>该规则应用于 TCF 还是 UDF?</li> <li>● TCP</li> <li>● UDP</li> <li>该规则应用于所有本地端口还是特定本地端口?</li> <li>● 所有本地端口(A)</li> <li>● 特定本地端口(S):</li> <li>124822</li> <li>示例: 80, 443, 8080</li> </ul>
	了解协议和端口的详细信息
	<上一步 (B) 下一步 (B) > 取消

4. 選擇"允許連接",點擊【下一步】。

💣 新建入站规则向导		x
<b>操作</b> 指定在连接与规则中指定的	的条件相匹酉时要执行的操作。	
步骤:         • 规则类型         • 协议和端口         • 操作         • 配置文件         • 名称	<ul> <li>连接符合指定条件时应该进行什么操作?</li> <li>6 允许在我(A)</li> <li>优许使用 IPsec 保护以及未保护的连接。</li> <li>7 <b>9.7公子公子在名(7)</b></li> <li>四方注使用 IPsec 进行身份验证以及完整性保护的连接。使用 IPsec 属性中的设置以及连接安全规则节点中的规则的连接将受到保护。</li> <li>「 等代用 IPsec 萬行身份验证及隐私。</li> <li>「 零代用 IPsec 制约 最近 及隐私。</li> <li>「 零代用 IPsec 制约 最近 及隐私。</li> <li>「 常代用 IPsec 制约 最近 及隐私。</li> <li>「 常代用 IPsec 制约 最近 及隐私。</li> <li>「 常代用 IPsec 制约 最近 及隐私。</li> <li>「 常代 用 IPsec 制约 最近 及隐私。</li> <li>「 常代 用 IPsec 制约 最近 及隐私。</li> <li>「 都代 用 IPsec 制约 是一个人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人人</li></ul>	
	< 上一步 (8) 下一步 (8) 入 取消	

5. 如圖所示默認勾選上"域", "專用", "公用", 點擊【下一步】。

💣 新建入站规则向导		×
<b>配置文件</b> 指定此规则应用的配置文件	ŧ×	
步骤:         • 规则类型         • 协议和端口         • 操作         • 配置文件         • 名称	<ul> <li>何时应用该规则?</li> <li>戶 何()</li> <li>近 前机连接到其企业域时应用。</li> <li>戶 有用()</li> <li>近 有用()</li> <li>计算机连接到公用网络位置时应用。</li> <li>1</li> <li>1</li></ul>	
	<_	上一步 (8) 下一步 (8) > 取消

### 6. 在名稱內輸入"Curtain",點擊【完成】。

💣 新建入站规则向导		×
<b>名称</b> 指定此规则的名称和描述。		
<ul> <li>步骤:</li> <li>规则类型</li> <li>协议和端口</li> <li>操作</li> <li>配置文件</li> <li>名称</li> </ul>	名称 (0): Curtain 描述 (可迭) (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,添加例外端口插件成功。

<b>L</b> 服务器管理器							
文件(F) 操作(A) 查看(V) 帮	助(H)						
🗢 🔿 🔰 🖬 😖 🚺 🖬							
▲ 服务器管理器 (M32₩2K8)	入站规则						
	名称	组 🔺	配置文件	已启用	操作	替代	程序
田 2 切胞	Curtain		任何日期	是	允许	否	任何日
日國國的	💿 BITS 对等缓存(Conte	BITS 对等缓存	任何日期	否	允许	否	System
日 🛄 印묘	🔮 BITS 对等缓存(RPC)	BITS 对等缓存	任何日期	否	允许	否	%Syst.
日 🍑 直级安全 Windows 防火t	🔮 BITS 对等缓存 (RPC-E	BITS 对等缓存	任何日期	否	允许	否	%Syst.
	💿 BITS 对等缓存(WSD-In)	BITS 对等缓存	任何日期	否	允许	否	%Syst.
一 出站规则	🔮 COM+ 网络访问 (DCOM-In)	COM+ 网络访问	任何日期	否	允许	否	%syst.
▲ 连接安全规则	🔮 iSCSI 服务(TCP-In)	iSCSI 服务	任何日期	否	允许	否	%Syst.

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..."

Windows Firewa	ll	
ieneral Exceptions	Advanced	
Windows Firewall is b programs and service to work better but mig Programs and Service	blocking incoming netw sselected below. Addi ght increase your securi	ork connections, except for the ing exceptions allows some programs ity risk.
Name		~
🗹 curtain24822		
🗹 curtain24822		
🗹 curtain24821		
🗹 curtain24821		
File and Printer S	Sharing	
🗹 Kaspersky Admi	nistration Kit	
🗹 Kaspersky Admi	nistration Kit	
🗹 Kaspersky Admi	nistration Kit	ل
Network Diagno	ostics for Windows XP	
Hemote Assistar	nce	~
	n	
Add Program	Add Port	Edit Delete
🗹 Display a notificat	ion when Windows Fire	ewall blocks a program
What are the risks of	allowing exceptions?	
		OK Cancel

2. 給此例外輸入名稱、端口為TCP的24821,並按OK確定。

Edit a Port		
Use these settings to open a port through Windows Firewall. To find the port number and protocol, consult the documentation for the program or service you want to use.		
Name:	curtain24821	
Port number:	24821	
	⊙ TCP O UDP	
What are the risks of opening a port?		
Change scope	OK Cancel	

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沖突,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(更改端口步骤,请参考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)。
```

```
m 管理员: C:\Windows\System32\cmd.exe
C: \Windows\system32>netstat -anolfindstr "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" 改為其他空閒的端口,然后保存。

<<pre><<pre><<pre>server port="8005" shutdown="SHUTDOWN">

//>

/// 

/// 

// 

// 

// 

// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
// 
<p

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,請按以下步驟進作安裝。

#### 安裝Curtain管理員的步驟:

1. 複制適合的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。

Curtain e-locker Central Administrator - InstallShield Wizard 🔀		
٢	從下列選項中選擇安裝語言。	
_	中交 (繁體)	
	中文(繁體) 中文(簡體) 英語	

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。

Curtain Admin - InstallShield Wizar	d and an and the second second second		×
<b>選擇功差</b> 選擇安裝程式將安裝的功能。			
	諸選擇您所要安裝的功能,浸	除不想安装的功能選項。	
	✔ Curtain管理員 ✔ Curtain服務器插件	40872 K 26912 K 36912 K 局的介面不 略。	可以使用Curtain管理 定義主要的控制策
	所需空間 C: 可用空間 C:	67856 K 11535260 K	
InstallShield	< 上一步( <u>B</u> )	ド一步(№) >	取消

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。請按以下步驟進作安裝。

#### 安裝Curtain服務器插件的步驟:

1. 複制適合的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<sup>。</sup>

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。

Curtair	a e-locker Central Administrator - InstallSh	ield Wizard 🔀
ىك	從下列選項中選擇安裝語言。	
	中交 (繁體)	~
	<u>中文(繁體)</u> 中文(簡體) 英語	

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。

Curtain Admin - InstallShield Wi	ard 📃
<b>選擇功能</b> 選擇安裝程式將安裝的功能	
	諸選擇您所要安裝的功能,清除不想安裝的功能選項。 □ Curtain管理員 OK ☑ Curtain服務器描件 26912 K 「Curtain服務器插件進行通 信,並指示服務器插件如何保護 服務器上的資源。
	所需空間 C: 26984 K 可用空間 C: 11535260 K
InstallShield	< 上一步( <u>B</u> ) 下一步( <u>N</u> ) > 取消

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. 複制適合的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。

ٹ	從下列選項中選擇安裝語言。
	中文 (繁體)

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。

Curtain e-locker Client - Inst 授 <b>程合约</b> 諸仔細閱讀下面的授權合約	allShield Wizard	
	END-USER LICENSE AGREEMENT FOR CURTAIN SOFTWARE IMPORTANTREAD CAREFULLY: This End-User License Agreement ("EULA") is a legal agreement between you (either an individual or a single entity) and Coworkshop Solutions Limited for the CURTAIN software that accompanies this EULA, which includes associated media ("Software"). An amendment or addendum to this EULA may accompany the Software. YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY INSTALLING, COPYING, OR USING THE SOFTWARE. IF YOU DO NOT AGREE, DO NOT INSTALL, COPY, OR USE THE SOFTWARE; YOU MAY RETURN IT TO YOUR PLACE OF PURCHASE FOR A FULL REFUND, IF APPLICABLE. 1. GRANT OF LICENSE. Coworkshop Solutions Limited grants you the following rights provided that you comply with all terms and conditions of this EULA: 1.1 Installation and use. You may: (a) install and use a copy of the Software on one personal computer or other device; and (b) install an additional copy of the Software on a second, portable device for the exclusive use of the primary user of the first copy of the Software. 1.2 Alternative Rights for Storage/Network Use. As an alternative to MUDICENTIAL MUDICE	
InstallShield	< 上一步( <u>B</u> ) 下一步( <u>N</u> ) > 取消	

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。

InstallShield Wizard		Strait Batta - more	a could be installed	X
環境檢測 檢測環境是否滿足安裝要求				
	檢測結	\$果如下:		
	ø :	操作系統:	Windows Vista SP2	
	9	通信埠:	符合要求	
	9	MSXML組件:	符合要求	
	Ø :	文件系統:	符合要求	
	9	已安裝的版本:	沒有安裝Curtain客戶端	
	ø	Curtain服務器插件:	沒有安裝Curtain服務器插件	
InstallShield	ľ	< 上一步(B) 下一步	<u> (N) &gt;</u>	取消

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。

Curtain e-locker Client - InstallShield Wizard 🛛 👔 👔				
伺服器位置				
	請輸入管理站	尚的機器名(或者IP地址)。		
	伺服器	L		
InstallShield		< 上一步( <u>B</u> ) 【下一步( <u>N</u> ) >	取消	

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 作產品激活。

#### 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。

Curtai	n e-locker管理員	X
?	用戶機器中的Curtain e-locker軟件未 是否現在激活?	激活 <b>!</b>
	是四一香烟	

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。

和中分15% 請輸入用戶當前版本Cur	tain e-lock	er的軟件序	列號	
用戶注冊資料				
用戶名稱:				
組織名稱:				
L				

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。

Curtain e	-locker軟件激活	
軟件激活		
第一步:! 發	钻撃下面的"生成激活請求文檔"按鈕,生成一( 送此文檔至 雁飛科技有限公司	國激活請求文檔,
第二步: 點	當你獲得確認激活文擋後, 撃"導入確認激活文擋…″,完成激活步驟。	
第一步	生成激活請求文檔	
第二步	導入確認激活文檔	確定 取消

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。

Curtai	in e-locker管理员	×
(į)	Curtain e-locker軟件已	·遗活!
	,明定	

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。

定	伺服器信息	受保護網路磁碟機	受保護網路埠	密碼管理
授擢				
授	霍字符串			****
指注	定新的管理員			
伺服	器選項			
<b>V</b>	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
雷郵	設定			
777	SUTPHENR PR			1 1 1 2 5 1 1 1 2 5 1 1 1 2 5 1 1 2 5 1 2
				2J

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	·) •
-----------------------	-------	------------	--------------------	------

受保護共∬ ☑ 允許	用目錄  123	物理路徑 C:\Users\Administrat	添加(A)	受保護埠	埠 TCP/UDP	
	ADMIN\$	C:\Windows C:\ C:\Windows\SYSVOL C:\Windows\SYSVOL	₩除®)			
	•		例外			
€保護網頭 □ 允許	頁應用 網站					
<b>F</b> .			添加			
			修改			

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。

📫 Curt	ain e-lock	er管理端					
文件(F)	檢視(T)	客 <mark>戶端(C</mark> )	安全策略(P)				
新發	建安全策略	3 <mark>(N)</mark>					
保存	保存安全策略(S)						
備化	備份安全策略(B)						
客月	客戶端補丁(P)						
審批	審批人信息(I)						
水日	水印信息(W)						
設定	E <mark>(E)</mark>						
管理	管理(M)						
活動	活動記錄(T)						
生历	<b>戈授權字</b> 符	F串(G)					
離	引Curtain e	e-locker管理	員(X)				

2. 輸入新建的安全策略名稱,並按確定。

新安全策略	X
輸入新安全策略名	確定
	取消

# 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"。

□ ③ 所有安全策略 ※ Default Po Wait for a	ኛ (9) olicy (1) ssignment (0)
VIP (0)	更新客戶端程式(U) 設定為缺省安全策略(S)
	重新命名(R) 刪除(D)
🦾 🚯 Externa	內容(P)

	□隱藏我的電腦		
	□隱藏本地受保護區	本地受保護區	ProtDir
	□ 禁止刪除網路磁碟機文檔	□ 附加受保護區	添
			~ 刪
動達理			
\$0/A*±	□清理本地受保護區	□清理本地受	受保護區暫存目錄
S		• 啟動	
		E四五六 〇毎週	日一二三四五六
	□清理本地受保護區內文檔	□清理本地到	受保護區內回收站文件
	下載后删除文檔	0 天 🗌 刪除后	ī永久删除 10 天
	──修改后刪除文檔	0 天	
	刑除文档加里 所有 ~	容合	
製到非	受保護區		
	○不允許(推薦)	允許的副檔名	添tn 複製羅頂
	○ 允許所有不支持的類型		74*74 1004025*74
			> 刪除

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"復製出去"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。

受保護軟件       軟件名稱       禁止另存       禁止明送       禁止列印       附加水印       記述         ダ AutoCAD       -       是       是       -       -       是       -	設定 系統策略 受控應用程式	
軟件名額       葉止另存       禁止利印       附加水印       記述         ダ AutoCAD       -	受保護軟件	
toCAD         版本         可供選擇的版本         AutoCAD 2011         AutoCAD 2009         AutoCAD 2009         AutoCAD 2006         AutoCAD 2005         AutoCAD 2006         AutoCAD 2006         AutoCAD 2006         AutoCAD 2006         AutoCAD 2006         AutoCAD 2000         AutoCAD 2000         上移         上移         下移	軟件名稱 ▼ AutoCAD ▼ AutoCAD LT	禁止另存 禁止傳送 禁止列印 附加水印 記録 ▲ - 是 是 - - 是 是 -
協本 可供選擇的版本 AutoCAD 2011 AutoCAD 2009 AutoCAD 2009 AutoCAD 2007 AutoCAD 2006 AutoCAD 2005 AutoCAD 2005 AutoCAD 2005 AutoCAD 2002 AutoCAD 2002 AutoCAD 2000i AutoCAD 2	toCAD	
	可供選擇的版本 可供選擇的版本 <u>AutoCAD 2011</u> AutoCAD 2010 AutoCAD 2009 AutoCAD 2007 AutoCAD 2006 AutoCAD 2005 AutoCAD 2004 AutoCAD 2002 AutoCAD 2000i AutoCAD 2000i AutoCAD 2000 上移 下移	<ul> <li>○ 本小田秋</li> <li>○ 禁止另存</li> <li>◎ 強制儲存到受保護區內</li> <li>◎ 禁止複製出去</li> <li>◎ 禁止列印</li> <li>○ 特止列印</li> <li>○ 常止列印屏幕</li> <li>○ 禁止剪貼板</li> <li>○ 禁止傳送</li> <li>● 経除所有</li> <li>選取所有</li> </ul> 其他 <ul> <li>● 保護文檔初稿</li> <li>取動客戶端進程使用</li> <li>應用程式權限</li> </ul>

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"

🖃 🏠 所有安全策略 (2)	
Wait for assignment #	
**	更新客戶端程式(U)
	設定為缺省安全策略(S)
	重新命名(R)
	刪除(D)
	內容(P)

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。

BAAC	伺服器信息	受保護網路磁	各磁碟機 受保護網路:		磁碟機 受保護網路埠			例外埠
例外的共享	密碼管理	審批人信息	水印	LDAP	第略分配方式			
安全策略分配	2							
○北北海	号公配							
0.124.084	GY) BL							
● 按用月	∋分配							
按用月	印分配							

然後"用戶和組"將顯示在Curtain管理員中。

16 - C	Curtain e-locker	管理員		
文件(F) 檢視(T) 客戶端(C) 安全策略(P)	语言(L) 說明(H)			
🏮 💊 🎸 📥 😂	i 😼 ?			
□ 圓 管理員管理	用戶名 組	策略 域	安全標識符	用戶類型
□ 3 客戶端	Test_01	Sales	S-1-5-21-40282487	本地
	<sup>2</sup> Test_02	Sales	S-1-5-21-40282487	本地
夢 離線 (1)	<sup>2</sup> Test_03	Sales	S-1-5-21-40282487	本地
	& Test_04	Sales	S-1-5-21-40282487	本地
	& Test_05	Sales	S-1-5-21-40282487	本地
	<sup>2</sup> Test_06	Sales	S-1-5-21-40282487	本地
▲ 祖 (U)	<sup>2</sup> Test_07	Sales	S-1-5-21-40282487	本地
■···〈會 加有女主來略 (5) -····〈會 Default Policy (0) -····〈〉 Wait for assignment (0)	& Test_08	N/A	S-1-5-21-40282487	本地

<sup>3.</sup> 完成<sup>。</sup>

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: ٠ "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。

設定	伺服器信	息 受(	呆護網路磁碟機	受保護	網路埠	例外埠	例外的共享
密碼管	翅	審批人信息	息 水日	£p	LDAP	ŝ	策略分配方式
LDAP							
愈用LC	DAP						
LDAP	司服器地址		192.168.10	).154			
LDAP	司服器端口		389				
SSL							
使用LC	DAP安全連接						
LDAP	用戶名		administra	tor			
LDAP	密碼		•••••	••••			
LDAP	叟索庫		dc=sztest,	dc=com			
LDAP	言息緩存時間	間隔	1			:	分鐘
			3	則試連接			
			0	rAdmin	×		
			▲	連接成功。			
				ОК			

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。

ŵ			Curt	ain e-locker	管理員	
文件(F) 檢視(T) 客戶端(C) 安全	策略(P) 語言(L	) 說明(H)				
🚺 🚸 🛷 📥 🌰	s 🍣 🐯	1				
	用戶名	組	策略	域	安全標識符	用戶類型
□	& User_41	Remote Desktop U		SZTEST.COM	S-1-5-21-15577856	域
	& User_40	Remote Desktop U		SZTEST.COM	S-1-5-21-15577856	域
	& User_39	Group_02		SZTEST.COM	S-1-5-21-15577856	域
	& User_38	Group_05;Remote		SZTEST.COM	S-1-5-21-15577856	域
	& User_37	Group_05;Remote		SZTEST.COM	S-1-5-21-15577856	域
	& User_36	Group_05;Remote		SZTEST.COM	S-1-5-21-15577856	域
	& User_35	Group_05;Remote		SZTEST.COM	S-1-5-21-15577856	域
□··· (會 所有女主東哈 (2)	& User_34	Group_05;Group_0		SZTEST.COM	S-1-5-21-15577856	域
Weit for parison and (0)	& User_33	Group_05;Group_0		SZTEST.COM	S-1-5-21-15577856	域
wait for assignment (0	& User 32	Group 04:Remote		SZTEST.COM	S-1-5-21-15577856	域

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。

### 指派用户/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)。

Ø			Curtain	e-locker管理
文件(F) 檢視(T) 客戶端(C) 安全	è策略(P) 語言(L	.) 說明(H)		
📑 🚸 💞 🚣 📤	s 🍣 🐯	1		
□ 『管理員管理	用戶名	組	策略	域
🖻 🍮 客戶端	👗 User_65	Remote Desktop U		SZTEST.COM
	👗 User_64	Remote Desktop U		SZTEST.COM
	User_63	改變安全策略(C	)	SZTEST.COM
	👗 User_62	2000年10月1日 2010年1月1日	-	SZTEST.COM
	& User_61			SZTEST.COM
4月戸(89)	日户(89) User_60 加圳和(K)			SZTEST.COM
·····································	🐫 User_59	Remote Desktop U		SZTEST.COM
□····(會 所有女王束喑 (5)	🐫 User_58	Remote Desktop U		SZTEST.COM
Wait for accimment (0	User_57	Remote Desktop U		SZTEST.COM
Engineers (2)	👗 User_56	Remote Desktop U		SZTEST.COM
Sales (5)	& User_55	Remote Desktop U		SZTEST.COM
HR (6)	& User_54	Remote Desktop U		SZTEST.COM
B(a)	& User 53	Remote Desktop U		SZTEST.COM

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/用户到合適的安全策略

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。

🚺 Curtain e-locker管理員				
檔案(F) 檢視(V) 客戶端(C) 安全第	5略(P) 語言(L)	說明(H)		
🎯 🗞 🎸 📗 🛕	🗞 🗊	, 🚯  ?		
□	客戶端	安全策略	所屬域	狀
	😻 kelvin-Vista	Default Policy	office.coworkshop.com	IE
	📎 VM-2003	<n a=""></n>	WORKGROUP	
·····••• 列·克休暖时 (2)	TEST2003	<n a=""></n>	WORKGROUP	
	🖇 CURTAINCL	IENT <n a=""></n>	WORKGROUP	
□	SERVER01	<n a=""></n>	COWORKSHOP	
Default Policy (1)	S DEV02	<n a=""></n>	COWORKSHOP	
Wait for assignment (0)	DEV01	<n a=""></n>	COWORKSHOP	
Engineers (0)				

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

指派用户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)。

			л / м <u>н</u> «сл+.	ジロ処門へエル
10 A			Curtain	e-locker管理
文件(F) 檢視(T) 客戶端(C) 安全	策略(P) 語言(L)	) 說明(H)		
📑 🌭 🛷 📥 📤	S 🖏	😼 ?		
□ 圓 管理員管理	用戶名	組	策略	域
□ 🛃 客戶端	🐍 User_65	Remote Desktop U		SZTEST.COM
	🚨 User_64	Remote Desktop U		SZTEST.COM
	🐫 User_63	改變安全策略(C)		SZTEST.COM
	🐫 User_62	2000 (E) 2000 (E)	-	SZTEST.COM
回 總 用户机組	& User_61			SZTEST.COM
	🕹 User_60	师J 新丁(R)		SZTEST.COM
○ 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	🐫 User_59	Remote Desktop U		SZTEST.COM
□···(會)所有女主束哈(5)	🐫 User_58	Remote Desktop U		SZTEST.COM
Wait for assignment (0	💐 User_57	Remote Desktop U		SZTEST.COM
Engineers (2)	🐍 User_56	Remote Desktop U		SZTEST.COM
Sales (5)	& User_55	Remote Desktop U		SZTEST.COM
HR (6)	& User_54	Remote Desktop U		SZTEST.COM
Pe tur for	& User 53	Remote Desktop U		SZTEST.COM

3. 選擇好用戶/組后·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、甚至自已開 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"。

💰 Curt	ain e-lock	er管理端	
文件(F)	檢視(T)	客 <mark>戶端(C</mark> )	安全策略(P)
新發 保存 備化	建安全策略 存安全策略 分安全策略	{(N) }(S) }(B)	
客戶 審排 水戶	<sup>≦</sup> 端補丁(F 比人信息(I) P信息 <b>(W)</b>	?) )	
設知 管理	宦(E) 里(M)		
活動	动記錄(T)		
生反 離閉	戈授權字符 <mark>骨Curtain e</mark>	F串(G) e-locker管理	員(X)

2. 於"服務器信息"頁,按"添加"按紐來新增服務器。舉例:如果你想保護兩台Windows文件服器上的共享文件夾和一個應用網站,你需要將那三台服務器添加在此頁。

服務器地址: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服務器插件之間的溝通)。

	10	2010 B	
间服器地址	垣	說明	
dev01 kelvin-vista	8443		
demo.docnet.com kmdemo.dyndns.c update.adobe.cor	添加伺服器 伺服器地址   埠 8443 說明		
		確定	取消

3. 新增服務器上受保護區。

情況1-保護Windows文件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"按紐,系統會彈出對話框。

映射磁碟構	浅 伺服器 192.16	<b>}地址</b> 8.1.18	器徑 Protected		允許DF	5 DFS 路徑	物理路徑 D:\Protected
🙀 修改共	大字						×
	青指定共3 路∕∞・\\	¥目錄	3.1.18	~	Pro	otected	
UNC	EUIT. ((	☑ 允許	映射磁碟	幾		Y:	~
DFS	路徑: \\	□通過	客戶端保調	莄	N		
						確定	取消
<							3
				添加	10	刪除	修改

UNC路徑: \\服務器\分享名稱

- 服務器 選擇服務器(電腦名稱或|P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"按紐,系統會彈出對話框。

<b>_</b>	□ 允許	保護					
伺服者	暑地址	協議	埠				添力0
							刪除
							修改
		http:// ●通i ○通i	kmdemo.dyndn: 過SDK保護 過伺服器插件仍	s.org ∨ R護	: 80		
		受保護上	傳位置:				
		http://	kmdemo.dyndns.	org : /	<protecta< td=""><td>шþ</td><td></td></protecta<>	шþ	
		提示: 需 ~	保護所有網站, PROTECTALL>"。	請於受係	R護網路應用	網站處輸	К
						_	

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 Share Point (如:http://Share Point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>"。

X

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"按紐,系統會彈出對話框。

設定

伺服器地址	協議	埠		添加
				刪除
	🎿 添加	埠	×	修改
	地址	PDM-Server		
	埠	3030	_	
受保護網頁應用	<b>↓</b> 協議			
伺服器地址	-			添加
http://kmdemo.d	у	確定取消		刑服金
				MULENT.
				修改

● 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"。

2. 添加伺服器資訊(IP或者主機名稱)。

伺服器地址	埠	說明				
192.168.1.18	8443					
Kelvin-Samsung	8443					
kmdemo.dyndns.org	8443					
						1
			0,000		10.00	
		添力	bo	刪除		修改

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)。

密碼 <sup>(</sup> 設定 受保	管理 伺服 、護網路	審批人 器信息 磁碟機信	信息 受保調 息	水印 黄網路磁碟	LDAP 機 受付	打 保護網	「印機信息 路埠 例:	本地; 外埠 例	加密磁盤  外的共享
E		允許保護							
映	射磁碟	機 伺服器	8地址	路徑	£	论許DFS	5 DFS 路徑	物理路征	፵
	Na 163	7.共享							×
		請指定共	:享日錄						
	UN	C路徑:\	192.1	68.1.18	~	· \ p	ro\pro1		
_			□允	許映射磁碟 過客戶端保	!機 !誰		Z:	$\sim$	
		s 路徑: \	1		-02	1			
							確宁	BOSH	
							UEAL	47/14	
_									
<									>
				1	沃加		冊旧全	伯名	:20
					<i>(11)</i>		DELEVIS.	15	~~~
						確定	ZE	消	應用

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。

受保護	網路磁和	<b>紫</b> 機 信 烏							
	一分子	午保護	5						
₩ 射	遊碟機	伺服器	地址	路徑	允許DFS	DFS 器徑	物理路徑	通過客戶	
		192.168 192.168 192.168	0.1.18 0.1.18 0.1.18	pro\pro1 pro\pro2			E:\pro\pro1 E:\pro\pro2		
		192.168	.1.18	pro\pro3			E:\pro\pro3		
2	》 您是 『	否要將設 ● 192.1( ● Kelvin	定應用 68.1.11 -Sams	月到下列伺月 8 sung	<b>服器?</b>			是	]
2	您是 【	er"官理員 否要將設 ▶ 192.10 ▶ Kelvin	定應用 68.1.11 -Sams	月到下列伺月 8 sung	服器?			是	]
?	》 您是	r"官理員 否要將設 ▶ 192.10 ▶ Kelvin	記定應用 68.1.11 -Sams	月到下列伺月 8 sung	服器?			是	]
<	》 您是	er"官理員 否要將設 ▶ 192.10 ▶ Kelvin	定應用 68.1.11 -Sams	月到下列伺月 8 sung	服器?			是	]
<	》 您是 『	er"官理員 否要將設 ▶ 192.1( ▶ Kelvin	定應用 68.1.11 -Sams	月到下列何月 8 sung	<b>服器?</b> 添加		刪除	是	
<	》 您是	er'官'理員 否要將設 ▶ 192.1( ▶ Kelvin	2定應用 68.1.11 -Sams	月到下列何月 8 sung	<b>服器?</b> 添力u		刪除	是 修改	
<	》 您是 『	er"官理員 否要將設 ▶ 192.1( ▶ Kelvin	定應用 68.1.11 -Sams	月到下列伺月 8 sung	服器 <b>?</b> 添力u		刪除	<u>是</u> 修改	

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 來),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,那么 可以設置 "例外規則"來實現這一需求。



没有安装Curtain客户端的计算机只可以使用非机密资料

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,并且設置了"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并且可以自 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:相當于停止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。

.	全部() 全部()	₹ していていていていています。 その話			_		_	_	•
址-	全部7 只對歹 除列表	∇保護 別表中 長之外	的保護 全部例	ŧ Riți					
地均	<u>E</u>						類型		
	业一地均	全部( 全部) 全部 全部 只對列 除列 地址	全部保護 全部保護 全部保護 全部不保護 只對列表中 除列表之外 地址	全部保護 全部保護 全部不保護 只對列表中的保護 除列表之外全部低 地址	全部保護 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 地址	全部保護         全部保護         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         地址	全部保護         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         地址	全部保護       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       地址	全部保護       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       地址

### 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"。

受 保護共日	3日約 —		
了九許	共用目錄 □ ADMIN\$ □ C\$	物理         ▲ 保護規則         ×           C:\Wir         C:\Wir         ▲           C:\Wir         ●         ●	
受保護網頭 「 九許 【 <b>兄</b> 許	ī應用 /網站		
そ保護網頭 「九許	網站		

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。

⊷ 保護	<b>嬳規則</b>	×
類型	只對列表中的保護	•
一地址	£	
-	保護規則	1
Г	IP地址	
	厂 IP地址範圍	
	確定 取消	
	添加 刪除 修改	
	確定 取消	

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:

<b>F</b> .•	授權字符串	******						
<b>そ保護共用</b>	用目錄 一			受保護埠				0
7 允許	共用目錄	物理路徑		□ 允許	埠	TCP/UDP		[ _
	ADMIN\$	C:\Windows	添加( <u>A</u> )	_ <u>_</u>				
		C:\ C:\protected	刪除(R)					
			修改(M)					
	•	•	例外					
<del>6</del> 2,			刪除 修改					
通信埠						1	2	

注意:當第三步 "關閉" 時會提示 "是否需要重啟插件服務器" ·在這里可以點擊 "NO" 選擇不重啟。

Curtain	e-locker	×
i	您是否願意重新開機使這些修改生效 <b>?</b>	
	<u>是</u> W 否W	

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" 。

設定 🧃	条統策略   受控應用程式		
☑ 停止	對受保護區的保護(不推薦) 設定		
	▶ 隱藏我的電腦		
	▶ 隱藏本地受保護區	本地受保護區	ProtDir
	▶ 禁止刪除網路磁碟機文檔	▶ 附加受保護區	添加
			▼刪除

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。





# 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)。

軟件名稱	禁止另存	禁止傳送	禁止列印	強制儲存到受保; ^	
Microsoft Excel	-	是	是	是	
Microsoft Internet Explorer	-	是	是	是	
rosoft Excel					
版本		存取權限			
可供選擇的版本		■ 禁止另存			
Microsoft Excel 2003 Microsoft Excel XP Microsoft Excel 2000 Microsoft Excel 97		<ul> <li>✓ 禁止利</li> <li>✓ 禁止列印</li> <li>✓ 禁止列印</li> <li>✓ 禁止列印</li> <li>✓ 禁止剪貼</li> <li>✓ 禁止傳送</li> <li>● 發除所有</li> <li>其他</li> </ul>	all j yj (mas all j yj (mas) all j yj (ma	所有	
<u>上移</u> 下移		▶□际護×幅	進程使用	應用程式權限	

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文擋只可以保存到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制到保護區之內才能打開, 可以用複制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。

Default Policy								
設定	系統策略	受控應用程式	局部設置					
在線/	在線/離線 模式							
● 工作站可以在離線模式下使用								
### 6.3 - 自動清理

"自動清理"是一個自動清除用户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

对 🗌 清理本地受保護區	□ 清理本地受保護區暫存目錄
◎ 啟動 ○每週 日 一 二 三 四 五 六 □ □ □ □ □ □ □ □ □ □	<ul> <li>         ・         ・         ・</li></ul>
□ 清理本地受保護區內文檔	□ 清理本地受保護區內回收站文件
□下載后刪除文檔 0 天	□刪除后永久刪除 10 天
◎修改后刪除文檔 0 天	
刪除文檔如 所有 ~ 符合	
"注册本地采得举定" 加思深挥此深语 大地采得举回力的行行	与 <u>文</u> 搅 哆 浊 则 除 。

"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很聰明地處理複製貼上這個功能:

- 在受保護區的文檔之間複製貼上是容許的;
- 從受保護區以外複製資料並貼到受控文檔內也是容許的;
- 但是,從受控文檔內複製資料並貼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,而又不會構成 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格式的同時,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。

Default Policy	
設定 系統策略 受控應用程式	
受保護軟件	767
軟件名稱	禁止另存 禁止傳送 禁止列印 強制儲存到受保 ^
Microsoft Word	· 是 是 是
Votepad	· 是 是 是 []
Microsoft Word	×
版本	存取權限
可供選擇的版本	🔤 禁止另存
Microsoft Word 2007 Microsoft Word 2003	☑ 強制儲存到受保護區內
Microsoft Word XP	▼ 禁止複製出去
Microsoft Word 2000 Microsoft Word 97	( 禁止列印
	▼ 禁止列印屏幕
	☑ 禁止剪貼板
	☑ 禁止傳送
	移除所有 選取所有
	其他
13	酌動客戶端進程使用   應用程式權限   ▼
下移	
	確定 取消
	確定 取消 應用

先容許用戶打印Word文檔

Print			? 💌
Printer <u>N</u> ame:	Adobe PDF		▼ Properties
Status: Type: Where: Comment:	Idle Adobe PDF Converter ProDir		Fin <u>d</u> Printer
Page range All Current p Pages: Enter page r separated b	page Selection numbers and/or page ranges y commas. For example, 1,3,5–12	Copies Number of <u>copies</u> : $\begin{array}{c} & & \\ & $	Colla <u>t</u> e
Print <u>w</u> hat: P <u>r</u> int:	Document   All pages in range	Zoom Pages per s <u>h</u> eet: Scale to paper si <u>z</u> e:	1 page   No Scaling
Options		C	OK Cancel

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"。

□·· 〈	(9) slicy (1)
Wait for as	ssignment (0)
	更新客戶端程式(U) 設定為缺省安全策略(S)
	重新命名(R) 刪除(D)
💫 Externa	內容(P)

2. 點擊 "複製選項" 按鈕,選擇如下圖所示的第三個選項,單擊 "確定"。

複製選項	
☑ 谷許將已加密的又福從受保護區複製到外面(加密又福可在任何地方解密)	
☑ 容許將已加密的文檔從受保護區複製到外面 (加密文檔只可在Curtain受保護區內解密)	
□ 允許將敏感的資料複製到任何地方	
	確定 取消

#### 與其他人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。

Curtain	開啟(O)		92 KB 92 KB	Microsoft Exce Microsoft Exce
Curtain	加密到(任何地方解密)	>	92 KB	Microsoft Exce
XI代理商	加密到(僅由客戶端解密)	>	桌面	6
	壓縮		郵伯	牛接收者
	壓縮到Curtain e-locker Pricebook - July 2017(HK).xlsx.zip		瀏覽	笔

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"。

「複製選項」		×
容許將已加密的文檔從受保護區複製到外面 (加密文檔可在任何地方解密)		
☑ 容許將已加密的文檔從受保護區複製到外面 (加密文檔只可在Curtain受保護區內解密)		
□ 允許將敏感的資料複製到任何地方		
	確定 取	Ъ

#### 與其他人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。

創建新密碼	×
CURTAIN	Secured e-locker in workstation
請輸入密碼	來保護您的文檔
新密碼:	
確認密碼:	
	確定 取消

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"按紐,或於菜單上選擇"檔案>活動記錄"。接著,系统會顯示活動記錄。

Curtain e-loc	ker管理員				
謠案(F) 檢視(V	/) 客戶端(C) 安全	(笄略(P) 語言	眚(L) 說明(H)		
J 🚯		🖌 😂 (	\$ 🚯 ?		
舌動記錄	Conception of the local division of the loca	D invite	Autor of Annaul An	in the	
數據庫					
文檔	C:\ProgramData\Cur	tain \Data \curta	in.sdb		
搜尋條件					
由:	11/ 1/2010 🔍 🗸		用戶:		… 高級…
到:	11/ 5/2010 🗐 🗸		工作站:		… 清除
關鍵字:			事件:		
う 辞・					
日期/時間	用戶	工作站	事件	結果	描述
<ul> <li>2010-04</li> <li>2010-04</li></ul>	4-20 13:02:31 SYSTEI 4-20 12:52:21 4-20 12:20:36 kelvino 4-20 12:20:36 kelvino 4-20 12:20:36 kelvino 4-20 12:20:36 kelvino 4-20 12:20:35 kelvino	4 kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista	Curtain e-locker 開始 Curtain e-locker 停止 複製出去 複製出去 複製出去 複製出去 加密 加密 加密	成成成成成成成成功功功功功功功功功功功功功功功功功功	複製文檔[C:\ProtDir\KELVINC\0130074 複製文檔[C:\ProtDir\KELVINC\0130074 複製文檔[C:\ProtDir\KELVINC\0230074 複製文檔[C:\ProtDir\KELVINC\0230074 複製文檔[C:\ProtDir\KELVINC\0530074 加密[C:\ProtDir\KELVINC\0130074381e 加密[C:\ProtDir\KELVINC\0130074381e 上
列印	輸出				[關閉(C)

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)。

數據庫					列印		-
文檔	C:\ProgramD	ata\Curta	ain \Data \curtai	n.sdb		皆自	
搜尋條件					日期	4751	2012-01-19
<b>#</b> :	19/ 1/2012			用戶:	時間		14:25:13
피 到:	19/ 1/2012			工作站:	用戶		kelvinc
關鍵字:		9		事件:	電腦名	稱	kelvin-Vista
文檔:	-			結果:	事件		列印
×				ind yie	結果		允許
2012-0 2012-0 2012-0 2012-0 2012-0 2012-0	1-19 14:25:13 1-19 14:24:52 1-19 14:24:40 1-19 14:22:58 1-19 14:22:25	kelvinc kelvinc kelvinc kelvinc kelvinc	kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista	列印 敬動 敬動 列印 敬動	<ul> <li>文件名</li> <li>頁數:</li> <li>打印機</li> </ul>		Microsoft PowerPoint - Curtain e-locker 3 Adobe PDF
<ul> <li>         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         2012-0         300         2012-0         300</li></ul>	1-19 14:22:06 1-19 13:10:10 1-19 13:10:03 1-19 13:09:56 1-19 13:09:49 已錄	kelvinc kelvinc kelvinc kelvinc m	kelvin-Vista kelvin-Vista kelvin-Vista kelvin-Vista	散動 複製出去 散動 散動	打印序 第1頁 第2頁 第3頁	]容 ——	

### 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仕使用,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仕使用而不受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"按紐來新增審批人。

- 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)

	PHR 10		収口工	况明	
tester	tester@cow	M32XP\admini	tester	1234	
漆加軍	主人				×
<b>±</b> *	トート 10-1-10-1-10-1-1-1-1-1-1-1-1-1-1-1-1-1-				
#1					-
Ices	ter				
中的新	<b>ä</b> *				
	•				-
tes	cer@coworksnop.c	:om			
Win	dows用白名*(t	由脑名\田白名 戓 セ	が用白名)		
	tain)tester		MAUN HI		-
	canticoscor				
职任	<u>۲</u> *				
tec	-				-
lesi					
说即	Ħ				
tes	- ter1234				
163	(G) 1204j			-	

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"。

名称	
Book1	.xls
🗳 testi	ng. doc
	打开(0)
	加密到(只由客戶端解密) ♪ 压缩
	压缩到 testing.doc.zip
	剪切(X)
	复制(C)
(	外发申请
	重新命名(11)
	删除(2)
	搜索
	刷新 ( <u>S</u> )
	属性 (B)

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。

外发申请				
申请文件				
C:\ProtDir\ADM	INISTRATOR\test	ting.doc		
申请人 *				
Lily				
申请人邮箱*				
lily@coworkshop	o.com			
申请原因				
外发				< >
, 选择审批人*				
审批人姓名	邮箱	Windows用	职位	说明
tester	tester@co	M32XP\adm	tester	1234
<u> &lt;</u>				>
		ОК		ancel

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。

🎓 申请外发文件(Li	ly <lily@coworkshop.com>) - 邮件 (纯文本)</lily@coworkshop.com>
:文件(亚)编辑(亚) 礼	观图(火) 插入(生) 格式(2) 工具(生) 动作(4) 帮助(4)
	🚵 🖉   💷 🍢   📍 💐   🌹   🖹 选项 (2)   🎯 🍟 📜
该邮件尚未发送。	
	.ester@coworkshop.com
主题(J): 🛛 🖪	申请外发文件(Lily〈lily@coworkshop.com〉)
附加	SendFile.curtain2 (7 KB)
申请人: Lily 申请文件: C:\ProtDir\A 申请原因: 外发	DMINISTRATOR\testing.doc

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)。

71及甲胍				
—申请信息—				
审批人	tester (tester@coworkshop.co	m)		1
申请人	Lily (lily@coworkshop.com)			
申请时间	2012/05/02 14:23:07			
申请原因				
外发				~
				M
一文件列表—				
		全部允许	全部拒绝	
	文件路径	允许	拒绝	
testing.doc		e	C	^
<			6	
<u>、</u> 一批注			2	
<ul> <li>批注</li> <li>Pass</li> </ul>			3	
・ 批注 Pass			2	
く 批注 Pass				

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。

💼 审批结果(tester <tester@coworkshop.com>) - 邮件(纯文本)</tester@coworkshop.com>
: 文件(E) 编辑(E) 视图(Y) 插入(E) 格式(2) 工具(E) 动作(A) 帮助(H)
: 🔜 🎿   🔏   🗟 🖉   🔛 &   📍 💺   🌪   🖹 选项 🕑   🕢 🦉 📜
该邮件尚未发送。
收件人 (X) lilv@coworkshop.com
抄送 (C)
主题(J): 审批结果 (tester <tester@coworkshop.com>)</tester@coworkshop.com>
附加 (I Approverd. zip (6 KB)
审批人姓名: tester
通过审批的文件: C:\ProtDir\ADMINISTRATOR\testing.doc
未通过审批的文件:
批注:
Pass

# 6.10 - 附加水印

如果你想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"。
```

設定	×
設定 伺服器信息 受保護網路磁碟機 受保護網路埠 例外埠	
例外的共享   密碼管理   審批人信息 水印   LDAP	
▶ 啟用文字水印	
文字水印	
上邊界  10 % 左邊界  10 %	
下邊界 10 % 右邊界 10 %	
字體顏色	
字體 Aharoni ▼ 字體外觀 空心 ▼ □ 半透明	
水印內容水印參數	
[DateTime] Sensitive information Protected by Curtain e-locker User: [UserName] Host: [HostName] Printer: [PrinterName]	
☑ 啟用圖片水印	
圖片 注意:如需打印透明圖片水印請加載透明FNG格式圖片!	
圖片位置     10     %     □     水平店中	
● 垂直位置 10 % □ 垂直居中	
預驗	
確定 取消應用	

2. 完成後按"確定" <sup>。</sup>

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。

otepad	
版本 可供選擇的版本	存取權限
Notepad 10 Notepad 6 Notepad 5	<ul><li>☑ 強制儲存到受保護區內</li><li>☑ 禁止複製出去</li></ul>
	<ul> <li>✓ 禁止列印</li> <li>□ 附加水印</li> <li>□ おおお印の穴</li> </ul>
	<ul> <li>✓ 茶止傳送</li> <li>移除所有 描 選取所有 ☐</li> </ul>
<u>上移</u> 下移	□ 保護文檔初稿
	散動客戶端進程使用     應用程式權限     ▼
	確定取消

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"。

Notepad	X
版本 可供選擇的版本 Notepad 10 Notepad 6 Notepad 5	存取權限 <ul> <li>禁止另存</li> <li>禁止易存</li> <li>受強制儲存到受保護區內</li> <li>禁止複製出去</li> <li>禁止列印</li> <li>禁止列印</li> <li>一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一一</li></ul>
下移	殷動客戶端進程使用     應用程式權限     ▼           確定          取消

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。

🚺 Vaternark. txt – ji	2事本 - (受Curtain e-locker)	所保护)	
文件(E) 编辑(E) 格式(D)	查看(Y) 帮助(H)		
Test print	打印 常规 选择打印机 添加打印机 Adobe FDF Fox: Reader 状态: 准备就绪 位置: 备注:	■	
	<ul> <li>页面范围</li> <li>● 全部 ①</li> <li>○ 选定范围 ①</li> <li>○ 页码 ④:</li> </ul>	份数 (C): 1 □ 自动分页 (C) 1 2 3 3 打印 (C) 取消 应用 (	



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。

新建快捷方式		×
這個精靈是用来	幫你創建受控應用程序的快捷方式。	
受控應用程序:		瀏覽
位置:	C:\Users\User\Desktop	瀏覽
命名:		
參數:		
	創建	取消

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。

芝炸用贝包定			
受控應用程			^
	Microsoft Office		
	Microsoft Acces	S	
	Microsoft Excel		
	Microsoft Office	Convert	
	Microsoft Office	Docume	
	Microsoft Office	Picture	
	Microsoft Power	Point	
	Microsoft Word	Func	
	Microsoft Windows		
	Others		
	PDF Tools		
	E PTC		~
	<	>	
[	確認	取消	1

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

設定

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。

内資料	以將現有的本地受 科的安全性・在局	授保護區升級至本地加 收用本地加密磁盤後,	密磁盤,通過加 管理員需要對相	密可以大大增3 應的客戶端進4	强存放在本地 行加密磁盤配	受保護區 習置(文件	
=>本	.地加密磁盘配置, 加密磁盘,請在西	)。確定配置後,存放行 2置前確保已將現有資	王本地受保護區P 料備份・	内的資料會被加	K久删隙,亚	生成新酌	
啟用	本地加密磁盤後,	不能取消。					
✓ 啟	用本地加密磁盤						
一加密	方式						
	VeraCrypt	⊖ BitL	ocker		⊖ TrueCry	pt	

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。

90

菜單上多了一個"本地加密磁盤配置"選項

■Curtain e-locker管理員				2			_
文件(F) 檢視(T) 客戶端(C) 安全策	略(P) 語言(L	.) 說明(H)					
新建安全策略(N) 保存安全策略(S)	s 😂 (	Ş 🛃	?				
備份安全策略(B)	客戶端	安全策略	所屬域	狀態	版本	最后上線時間	網
客戶端補丁(P) 審批人信息(I) 水印信息(W)	😻 harry-PC	Default Policy	shenzhen.coworkshop.com	正常	3272.18	2010-06-08 21:02:16	N/A
設定(E) 管理(M) 本地加密磁盤配置(D)							
活動記錄(T) 離開Curtain e-locker管理員(X)							
□ 🏠 所有安全策略 (2) 							
□ 案 客戶端的保護區 本地受保護區 (2) 本地加密磁盤 (0)							
J							
						NU	IM

## 左手邊新增客戶端的保護區"視窗

■Curtain e-locker管理員								_
文件(F) 檢視(T) 客戶端(C) 安全策	略(P) 語言(L	) 說明(H)						_
] 🧊 🚸 💞 🖾 🔬	s 😂 (	Ş 🚯	?					
□	客戶端	安全策略	所屬域	狀態	版本	最后上線時間	網路驅動	城本   標記
─────────────────────────────────────	💕 tester-PC	Default Policy		正常	3272.19	2010-06-08 21:34:12	3272	{1C8
□ 🍫 所有安全策略 (2)								
Default Policy (1)								
Wait for assignment (1)								
□ 蘆 各戶騙的係護區								
本地加密磁盤 (0)								
								NUM

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		
	操作系統:		19
	本地加密磁盤狀態:	全部	<u> </u>
MB~ MB	本地磁盤剩餘空間:	全部 未獲取設置 早難取設置	清
MB~ MB	本地加密磁盤剩餘空間:	13%(設置 創建失敗 創建成功 掛載失敗 掛載成功 待删除 删除	
		制除成功	
		操作未就:         小B         MB~         MB         MB~         MB         本地磁盤剩餘空間:         MB~         MB         本地加密磁盤剩餘空間:         MB         本地加密磁盤剩餘空間:         MB         本地加密磁盤射餘空間:         本地磁盤空間	操作未就:          本地加密磁盤狀態:         MB~       MB         本地加密磁盤剩餘空間:       未獲取設置         創建成功       掛載成功         排載,以功       特刪除,成功         中除,失敗       刪除成功         本地磁盤空間       本地加密磁盤狀態       操作系統       版本         本地磁盤空間       本地加密磁盤狀態       操作系統       版本

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)。
  - 删除成功: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。

		0.5.1 -	 -/33	 	 
then Sold Sold T	TE				
	÷1				
7.540 EEE EEE					

加密密碼一經設定	定,便不能修改。	
密碼:	•••	
確認密碼:	•••	
導入	確認	取消

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。

X

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)。

9=井米石开门。	A ++ 10x 22/1	2=#16	C +++µ+hoster∺A2		
未護領空:			○ 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:	全部	7
本地磁盤總空間:		MB~ MB	本地磁盤剩餘空間:	MB~	MB
本地加密磁盤總空間:		MB~ MB	本地加密磁盤剩餘空間:	MB~	MB
¥月·瑞列表 客戶端名稱 本地磁盤	本地磁盤空間	1 本地加密磁盤空	间 本地加密磁盤狀態 操作	系統 版本 失敗原因	
TESTER-PC C:	C:(51.9/59	,	Wind	o 3	
TESTER-PC C:	C:(51.9/59		Wind	o 3	
TESTER-PC C:	C:(51.9/59		Wind	o 3	
TESTER-PC C:	C:(51.9/59		Wind	o 3	

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。

Curtain e-I	ocker管理端	×
?	當創建默認本地加密磁盤的時候,會永久性刪除所有客戶端受保 護區內已經存在的文件,是否繼續?	
	<u>Y</u> es <u>N</u> o	

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	×
┌加密磁盤	
默認加密磁盤大小(單位:GB):	1
默認映射盤符名称(A-Z):	F: 💌
映射文件默認保存盤符:	C:
映射盤符被佔用時的處理:	⊙ 自動選擇一個空閒的盤符
	○ 停止處理并報告錯誤
磁盤空間不足時的處理:	● 自動匹配一個不小於1GB的加密磁盤
	○ 停止處理并報告錯誤
	確定 取消

"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。
- 默認映射盤符名稱(A-Z):用作映射本地加密磁盤的盤符。
- 映射文件默認保存檔符:用作儲存本地加密磁盤的加密文件的默認盤符。
- 映射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
- 默認映射盤符名稱(A-Z):F:
- 映射文件默認保存檔符:C:
- 映射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	们密磁盤。	
--------------------	-------	--

客戶端詳細信息
客戶端信息
客戶端名稱: TESTER-PC
┌本地磁盤信息
盤符 磁盤總空間 磁盤剩餘空間
C: 59.8GB 35.1GB
本地加密磁盤信息
默認 1.0GB 掛載成功 1.0GB 自動匹配一個不小於 自動選擇一個空間的盤符
編輯失敗狀態的加密磁盤配置

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。

Curtain e-l	ocker	×
?	管理員已經配置當前電腦使用增強性加密磁盤,是否現在 <mark>啟</mark> 用?	
	Yes No	

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。

Curtain e-l	ocker	×
4	还沒有創建默認的加密磁盤	
	ОК	

4. 按 "OK" 繼續,系統會立即創建本地加密磁盤。

🟓 創建本地加密磁盤	
還有創建加密磁盤的推送設置未處理,正在創建加密磁盤,請稍後	
創建加密磁盤 F:	
正在創建	
速度	22.3 MB/s
當前進度	26.09%
	1
總進度	26.09%

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。

r

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作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。

⊖⊖ ⊽ 📜 ► Compute	er 🕨 🤜 🔀 Search Computer
Organize 🔻 Propertie	s System properties Uninstall or change a program Map network drive » 📓 🖛
<ul> <li>★ Favorites</li> <li>■ Desktop</li> <li>● Downloads</li> <li>● Recent Places</li> </ul>	Hard Disk Drives (3)     Local Disk (C:)     49.9 GB free of 59.8 GB
<ul> <li>Libraries</li> <li>Documents</li> <li>Music</li> <li>Pictures</li> </ul>	Local Disk (G:)  Location is not available
Videos	F:\ is not accessible. Access is denied.
Network ™	ОК

#### 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"。

叟索條件				
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:		搜尋
本地磁盤:		本地加密磁盤狀態:	全部 ~	
本地磁盤總空間:	MB~ MB	本地磁盤剩餘空間:	全部 未獲取設置 只獲取設置	清陵
本地加密磁鏡線空間:		本地加密磁盤剩餘空間:	創建失敗	
		一个G/B 品 做 正 利 時 王 1917	掛載失敗	
			待删除	
			刪除失敗	
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	间 本地加密磁盤狀態 操作	制除失敗 制除成功 下系統版本 失敗原因	
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	间 本地加密磁盤狀態 操作	刑除失敗 刑除成功 下系統 版本 失敗原因	

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。

;戶端詳細信息	
削建擴展加密磁盤	×
┌加密磁盤────	
默認加密磁盤大小(單位:GB):	1
默認映射盤符名称(A-Z):	F:
映射文件默認保存盤符:	C:
映射盤符被佔用時的處理:	◎ 自動選擇一個空閒的盤符
	○ 停止處理并報告錯誤
磁盤空間不足時的處理:	ⓒ 自動匹配→個不小於1GB的加密磁盤
	○ 停止處理并報告錯誤
	確定 取消
捕展 1.0GB 掛載成功	1.0GB 自動匹配一個イット於 自動選擇一個空間的整符
/ / / / / / / / / / / / / / / / / / /	1.0GB 自動控配一個不小於 自動選擇一個空間的盛行
THE LOOP PLACE IN THE	
編輯失敗狀態的加密磁盤配置	
	刷閉

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。

	○ 本地受保護區		④ 本地加密磁盤			
各戶端名稱:			採作 <del>杀</del> 税:	I		
本地磁盤:			本地加密磁盤狀態:	全部		•
本地磁盤總空間:	MB~	MB	本地磁盤剩餘空間:		MB~	MB
本地加密磁盤總空間:	MB~	МВ	本地加密磁盤剩餘空間		MB~	MB
				,		
客戶端列表						
客戶端名稱 本地磁盤	本地磁盤空間 本	地加密磁盤空间	本地加密磁盤狀態 操作	F系統 版本	失敗原因	
TESTED DC CI		(a. a. (d. a. a. a.) . a.				
ILSILKTO G	C:(49.9/59 F:	(0.9/1.0GB),G:	F:掛載成切,G: Win	do 3		
	C:(49.9/59 F:	(0.9/1.0GB),G:	F:掛載成切,G: Win	do 3		
ILSIEKTC C.	C:(49.9/59 F:	(0.9/1.0GB),G:	F:掛載成功,G: Win	do 3		
	C:(49.9/59 F:	(0.9/1.0GB),G:	F:掛載成功,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:掛載成功,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:排載成功,G: Win	do 3		
	C:(49.9/59 F:	(0.9/1.0GB),G:	F:掛載成功,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:掛載成功,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:掛載成以刀,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:掛載成功,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:掛載成U刀,G: Win	do 3		
	C:(49.9/59 F:	(U.9/1.0GB),G:	F:掛載成以刀,G: Win	do 3		
提示:雙聲相應的客戶端(	C:(49,9/59 F: 条目可以查看更多的	(0.9/1.0GB),G:	F:掛載成功,G: Win	do 3 密磁盤信息。		搜索

#### 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。

舌動記錄										]
數據庫										
文檔	C:\Program	Data\Curta	ain (Data (curt	ain.sdb						
─搜尋條件──										
由:	6/ 9/2010	-		用戶:				i	高級	
到:	6/ 9/2010	•		工作站:					<b></b> 諸除	
關鍵字:	, 			事件:						
文檔 <b>:</b>	,			結果:					搜 <b>帮(S)</b>	
-結果		ШŔ		<b></b>		(± E)	4#14			
	-00.00+30+20		tester_PC		i	<u>結未  </u> 成11		設置為均	非裁列の般	
2010-06	-09 00:30:29	TESTER	tester-PC	11年20日 創建加密磁盤		のスコノリ 市式I力	11 戰[加密磁盤, 創建[擴展]加密磁盤。	axiel (明): 1024M。	新取到G:盘 映射到G:盘	
2010-06	-09 00:28:55	SYSTEM	tester-PC	接收并保存加密磁线	。 盤設置	成功	創建[擴展]加密磁盤,	1024M,	映射到G:盘	
2010-06	-09 00:27:55	tester	tester-PC	むした いっし いっし いっし いっし いっし むり いっし		成功	加載應用程式["C:\Pro	gram File	s\Coworks	
2010-06	-09 00:27:50	TESTER	tester-PC	掛載加密磁盤	J	成功	掛載[[狀認]加密磁盤,	設置為排	扑載到F:盤	
2010-06	-09 00:27:49	TESTER	tester-PC	創建加密磁盤	J	成功	創建[[狀認]加密磁盤,	1024M,	映射到F:盤	
2010-06	-09 00:23:50	SYSTEM	tester-PC	Curtain e-locker 停止	E .	成功				
•									Þ	
找到7條記錄										
列印	輸出								關閉( <u>C</u> )	
# 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。

IXAC [9]	服器信息	受保調	蒦網路磁碟相	幾 受保護	護網路埠	例外埠	例外的共3
密碼管理	審批人會	信息	水印	LDAP	打印機	信息	本地加密磁盤
客戶端密碼	馬管理						
一登錄密碼	5						
<b>●</b> 無	密碼						
()客	戶端						
	自定義密碼	ç.					
	USB令牌						
	000 11/11						
卸載密碼	5						
密	碼保護						
-							
-							
管理端密码	馬管理						
管理端密₩ □密	馬管理 碼保護						
管理端密制	碼保護						
管理端密制	<b>馬管理</b> 碼保護 重設密碼						
	<b>馬管理</b> 碼保護 重設密碼						
管理端密₩ □密 插件端密₩	<b>馬管理</b> 碼保護 重設密碼 馬管理						
管理端密碼 □密 插件端密碼 ● 無	<b>新管理</b> 碼保護 重設密碼 新管理 密碼						
管理端密碼 □整 □描件端密碼 ● 無 ○ 插	馬管理 碼保護 重設密碼 馬管理 密碼 件端						
管理端密 □ 整 - 插件端密 ● 無 ○ 插	馬管理 碼保護 重設密碼 馬管理 密碼 件端						
管理端密碼 □密 插件端密碼 ● 無 ○ 插	馬管理 碼保護 重設密碼 馬管理 密碼 件端						
管理端密碼 □整 □插件端密碼 ◎ 無 ○ 插	馬管理 碼保護 重設密碼 馬管理 密碼 件端						
管理端密碼 □密 插件端密碼 ●無 ○插	馬管理 碼保護 重設密碼 馬管理 密碼 件端						
管理端密朝 □密 □描件端密朝 ● 無 ○ 插	馬管理 碼保護 重設密碼 馬管理 密碼 件端						

3. 輸入密碼後按確定鍵確認。

創建新密碼	×
CURTAIN	Secured e-locker in workstation
請輸入新密碼。	
新密碼:	
確認密碼:	密碼由6-16位字符組成,區分大小 寫(不能包括空格)。
	確定 取消

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証書的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。

選擇認證方式	×
CURTAIN	Secured e-locker in workstation
請選擇認證方式。	
◎ 自定義密碼	
C USB令牌	
	確定 取消

# 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"。

登入 CURTAIN	Secured e-locker in workstation
域名/電腦名: 密碼:	server2008x86en
	<u>修改密碼</u> 忘記密碼
	確定取消

"密碼設置" 窗框會如下圖顯示。

CURTAIN		Secured ir	le-locker workstation
舊密碼:	忘記密	<u>碼</u>	
新密碼:			
確認密碼:			
	_		

2. 輸入舊密碼和新密碼。

3. 按確定鍵確認<sup>。</sup>

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		Х
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。

- 按"更新 Curta 檔案(F)	程式"按鈕 ain e-locker 檢視(V)	或選"檔案> 管理員 客戶端(C)	客戶端更新" 安全策略(P)	語言(L)	說明(H		
客戶端更 已安朝	」 「新 麦的升級檔						×
版本 3.8. 3.8. 3.8. 3.8. 3.8. 3.8. 3.8.	x 3263.4 3263.2 3263.1 3263.1 3263.0 3260.0						
新增升	₩₩₩	更新過濾 >>			確定	取消	

# 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 比文件夾位於 C:\Program Data

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|P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。



6. 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。

7. 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:

- 1. 安裝一台新電腦,並使用不一樣的電腦名稱與|P地址。
- 2. 在該台新電腦上,安裝Curtain管理員(詳細步驟請參考相關資料)。

3. 激活剛安裝好的Curtain管理員(詳細步驟請參考相關資料)。

4. 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。

5. 在現時的Curtain管理員,於菜單上選擇"檔案>設定"。

E		10 64	Brit . month	AND DESCRIPTION OF THE OWNER.
设定	伺服器信息	受保護網路磁碟機	受保護網路埠	密碼管理
授林	權			
授	權字符串	_		
t≌	定新的管理員		NewAdmin	

6. 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。

管理員				
客戶端(	C) 安全策略(P)	語言(	L) 說明(	(H)
<b>8</b>	S 🛆 🗟		\$ 🔂	?
客戶端	安全策略	所	狀態	版本
🔔 Moni	ca Default Policy	sh	已轉移	3265.26

7. 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:

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<sup>"</sup>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。



🕒 🍚 🤳 « Program Files 🕨 Coworkshop	p ▶ Cui	tain 3 🕨 Bin 🕨	• <del>\$</del> 9	Search Bin	
File Edit View Tools Help Organize ▼ Include in library ▼ Share	e with 💌	Burn New folder			911
Favorites	Â	Name		Date modified	T
Downloads		ServerStore.enx.bak2029		2014/12/12 15:27 2014/12/3 18:15 2014/12/4 10:52	B
Creative Cloud Files	н	ServerStore.enx.bak2030		2014/12/4 10:32	B
Documents		ServerStore.enx.bak2035		2014/12/9 18:20	B
Music		ServerStore.enx.bak2036		2014/12/10 18:07 2014/12/11 19:11	B
<ul> <li>Pictures</li> <li>Videos</li> </ul>		ServerStore.enx.bak2038		2014/12/12 15:22 2014/11/19 18:01	B

#### 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),卡巴斯基(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|SCS| Target

1. i	從DSM系統上進入主功能表	<sup>,</sup> 打開"存儲空間管理員"	,如圖:		
	11				₽搜索
			raocacon	EST ANY POSSIBLE	
				$\sim$	
		<b>DSM</b> 说明	套件中心	资源监控	存储空间 管理员
				~	
		日志中心	MyDS Center	安全顾问	存储空间分析
2.3	進入"存儲空間管理員"介面	ā,選擇"ISCSI LUN"。	如圖:		
	<b>4</b> 8 <b>1</b>				

10		存储空间管理员
至系統概況	新增	
🚓 存储空间		
111 磁盘群组		
HDD/SSD		
😂 iscsi lun		
iSCSI Target		

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

	iSCSI LUN 创建向导	×
选择 LUN 种类		
<ul> <li>iSCSI LUN (一般文件)</li> <li>此形式的 iSCSI LUN 不仅提供</li> <li>iSCSI LUN (段落分块) - 使用/</li> </ul>	弹性且动态的容量管理,且具备 Thin Provisioning 所有硬盘容量的 LUN	」功能。
此形式的 ISCSI LUN 能提供最 名称: iSCSI Target 链接:	性的访问性能。 LUN-2 新增一个 iSCSI target ←	
<ul> <li>ISCSI LUN (股格分块) - 可弹1</li> <li>此形式的 iSCSI LUN 创建在磁 名称:</li> <li>iSCSI Target 链接:</li> </ul>	生使用部份磁盘群组谷重的 LUN 盘群组上,提供动态调整容量的弹性与优化的访问性 LUN-2 新增一个 iSCSI target ▼	台 日 上 =
	×→#	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:

	iSCSI LUN 创建向导	×
设置 iSCSI LUN 属性		
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 🔹 👻	
iSCSI Target 链接:	新增一个 iSCSI target 🔹	
上一步	下→步	取消

5. 勾選"啟用CHAP", 並輸入名稱和密碼, 按一下"下一步"。如圖:

所增一个 iSCSI target		
;称:	Target-1	
QN:	iqn.2000-01.com.synology:NAS01.	
✔ 启用 CHAP		
名称:	Target1	
密码:		
确认密码:	•••••	
启用相互 CHAP		
名称:		
密码:		
确认密码:		

6. 再次檢查設置, 如果確認沒有問題, 按一下"下一步"。如圖:

 宜
CSI LUN
JN-2
储空间 1 (可用容量: 484 GB)
(GB)
irget-2 (新增)
n.2000-01.com.synology:NAS01.Target-2.489975a9d1
HAP

7. 在"存儲空間管理員"介面上,你可以看到創建好的iSCSILUN。如圖:

上一步

1	存储空间管理	员
■ 系统概况	新增 删除 编辑	
	<b></b> LUN-1 - 正常	
<b>4</b> 存储空间	iscsi LUN (一般文件)	
dbdh	状态	正常
Ⅲ 磁盘群组	已报告	512 GB
	已用	103.50 MB
	Thin Provisioning	是
	位置	存储空间 1
🥃 iscsi lun	iSCSI Target 链接	
	名称	状态
iscsI Target	Target-1	已就绪

取消

8	存储空间管理员	
■ 系統概況	新增 删除 编辑 停用 iSN	S
📥 存储空间	Target-1 - 已就绪	
111 磁盘群组	名称 IQN	Target-1 iqn.2000-
HDD/SSD	服务状态	1.489975a9d1 已就绪
S ISCSI LUN	认证 多重联机	CHAP 停用
🌐 iSCSI Target	标头摘要 数据摘要	停用 停用
	最大接收片段字节 最大发送片段字节	262144 Bytes 4096 Bytes
	已链接的 iSCSI LUN	
	名称	容量
	LUN-1	512 GB
	掩码	
	启动器 IQN	权限
	默认权限	可读写

## 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>iSCS|發起程式", 如果是第一次啟用iSCS|服務, 將 會彈出對話方塊, 按一下 "是"即可。如圖:

icrosoft iSCSI		
Microsoft iSCSI 服务尚未运行。 服务。您想启动该服务并让它在每	要使 iSCSI 正常工作,必须 次启动计算机时自动运行吗	须启动该 }?
	是(1)	否例

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:

iSCSI	发起程序	属性		×
常规	发现	目标	收藏的目标   卷和词	设备   RADIUS
	标门户(T)	1.200	1.15 - 288	( 141) ]
<u>t</u>	也址		道能器	<u>  IP 地址  </u>
	添加门户0	9	冊修余 (R)	刷新(E)
[ iSl	NS 服务器	a) —		
4	当称			
	·	1	mito an I	Plat as 1
	жлµш.	<u> </u>	前序 (01)	
			确定	取消 应用(A)
SCST	化复建度	屈树		
添加目	标门户	PALL		X
键入到	<b>聚添加门户</b>	的 IP 地址	止或 DNS 名称和端口	号。要选择该门户发
现会说	钻的设置, 1	请单击"语	<b></b> 氯级"。	
TP +łb	北动 nws .	夕称 (1)・	端口で)	
192.1	168. 10. 128		3260	 高级(A)
-				
			确定	1 取消
iSI	NS 服务器	(I) —		
	Concerned States In	enen		1000
4	1   1   1   1   1   1   1   1   1  1			
4	3称			
4	乌称			
	<b>呂称</b>			
	乌称 添加(0).	<u></u> ]	冊修余 (91)	刷新 (r)
	<u>国称</u> 添加(0).	]	冊修余 (91)	刷新 (r)
	<u>国称</u> 添加(0).	]	冊//余 (개)	刷新 (F)

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:

	×
常规 发现 目标 收藏的目标 卷和设备 RADIUS	
要访问目标的存储设备,请选择目标并单击"登录"。	
要查看该目标的会话、连接和设备信息,请单击"详细信息"。	1
目标 (T):	
名称	
iqn.2000-01.com.synology:diskstation.target-1不活 iqn.2000-01.com.synology:nas01.target-2.489975不活	<del>述</del> 力
详细信息 (D)登录 (L) 刷新 (E)	
确定取消应用	] (A)
iSCSI 发起程序 属性	×
登录到目标	×
	_
1qn.2000-01.com.synology:nas01.target-2.489975a9d1	
□ 计算机启动时自动还原此连接(R)	
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(B)</li> <li>▲ 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择</li> </ul>	ŀĽ
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(R)</li> <li>① 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择 选项。</li> </ul>	ut
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(B)</li> <li>① 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择 选项。</li> <li>□ 高级(A)</li> <li>□ 确定 取消</li> </ul>	ж
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(B)</li> <li>① 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择 选项。</li> <li>□ 高级(A)</li> <li>□ 确定 取消</li> <li>ign. 2000-01. com. synology:nas01. target=2.489975 不清:</li> </ul>	此 」 5
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(R)</li> <li>□ 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择选项。</li> <li>□ 高级(A)</li> <li>□ 确定 取消</li> <li>ign. 2000-01. com. synology:nas01. target=2.489975 不清:</li> </ul>	此 
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(R)</li> <li>① 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择选项。</li> <li>□ 高级(A)</li> <li>□ 确定 取消</li> <li>iqn. 2000-01. com. synology:nas01. target-2. 489975 不活:</li> </ul>	此  动
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(R)</li> <li>▲ 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择 选项。</li> <li>高级(A)</li> <li>确定 取消</li> <li>ign. 2000-01. com. synology:nas01. target=2.489975 不活:</li> </ul>	此  动
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(B)</li> <li>▲ 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择选项。</li> <li>高级(A)</li> <li>确定 取消</li> <li>iqn. 2000-01. com. synology:nas01. target-2. 489975 不清:</li> </ul>	此 」 动
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(R)</li> <li>▲ 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择选项。</li> <li>高级(A)</li> <li>确定 取消</li> <li>iqn. 2000-01. com. synology:nas01. target-2. 489975 不清:</li> </ul>	此 动
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(B)</li> <li>① 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择选项。</li> <li>高级(A)</li> <li>确定 取消</li> <li>iqn. 2000-01. com. synology:nas01. target=2.489975</li> <li>不活:</li> <li>详细信息(D)</li> <li>登录(L)</li> <li>刷新(B)</li> </ul>	此 动
<ul> <li>□ 计算机启动时自动还原此连接(R)</li> <li>□ 启用多路径(B)</li> <li>▲ 如果您的计算机上已经安装了 iSCSI 多路径软件,则只选择选项。</li> <li>高级(A)</li> <li>确定 取消</li> <li>iqn. 2000-01. com. synology:nas01. target-2. 489975</li> <li>不活:</li> <li>▲ 详细信息(D)</li> <li>登录(L)</li> <li>刷新(B)</li> </ul>	此 」 う 」

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:

Z地适配器(A):	默认值
亰 IP(I):	默认值
目标门户(T):	默认值
RC/校验和	
□ 数据摘要 (D)	□ 标题摘要 00
マ CHAP 登录信息 (C	1
11111111111111111111111111111111111111	┛ 序之间提供身份验证,CHAP 有助于确保数据安全。要使用它,
通过在目标和发起程 有为此发起程序指定: 用户名(U): Tare	■ 序之间提供身份验证,CHAP 有助于确保数据安全。要使用它, 与配置在该目标上的相同的目标 CHAP 机密。 get1
■过在目标和发起程 青为此发起程序指定 用户名(V): 「Targ 目标机密(S): ●●	■ 序之间提供身份验证,CHAP 有助于确保数据安全。要使用它, 与配置在该目标上的相同的目标 CHAP 机密。 et1

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:

CSI	发起程序	属性				×
常规	发现	目标	☆ 藏的目标   巻	和设备丨R	ADIUS	
要认	防问目标的存	字储设备,请	选择目标并单击	<b>:"</b> 登录"	۰	
要望	<b>逐看该目标的</b>	内会话、连接	和设备信息,词	事单击"详	细信息"。	
目标	ī, (T) ;					
名	称				状态	
iq	n. 2000-01.	com. synolo;	gy:diskstation	. target-1	1 不活	动
iq	n. 2000-01.	com.synolo	gy:nas01.targe	t-2. 48991	75 已连	接
						F
2					- Seaton and and	
	详细	信息(0)	登录(L)		刷新(E)	
		THE CASE OF A DECK			Contraction of the second s	

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:

🛃 计算机管理			
文件(F) 操作(A) 查看(V)	帮助(H)		
🗢 🧼 🖄 📅 🚺 🖬 😰	😭 🛃		
<ul> <li>計算机管理(本地)</li> <li>○ 12 系统工具</li> <li>● ④ 任务计划程序</li> <li>● ● 任务计划程序</li> <li>● ● 日子音器</li> <li>● ● 中空看器</li> <li>● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ● ●</li></ul>	<ul> <li>巻 布局 类型</li> <li>○ (C:) 简单 基本</li> <li>○ (C:) 简单 基本</li> <li>○ (C:) 简单 基本</li> </ul>	│ <u>文件系统</u> │状态 │NTFS 状态良: │NTFS 状态良:	好(系统,启动,页面文件 好(主分区) ▲
■ 磁盘管理 ■ 晶 服务和应用程序	基本 931.51 GB 联机	(C:) 78.13 GB NTFS 状态良好(系统	()E:) 853.38 GB NTIFS 状态良好(主分区)
	□ 磁盘 1 基本 1023 MB 联机	1023 MB 未分配;	

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:

🛃 计算机管理			
文件()》操作(A) 查看(V) 素	紧助 (H)		
🗢 🔿 🖄 🗊 🚺 🖬	X 📽 🖻 🍳 😼		
🛃 计算机管理(本地)	卷 布局 类型	文件系统 状态	
□ 👔 系统工具 □ 🖓 任务计划程序	□ (C:) 简单 基本 □ (P·) 简单 基本	NTFS 状态良好 NTFS 状态良好	(系统, 启动, 页面文件, 活; (主分区)
□ 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2	□ 新 简单 基本	NTFS 状态良好	(主分区)
田 @ 可靠性和性能     公备管理器     公备管理器	•		Þ
🖸 📇 存储	□ 磁盘 0		
■ 1995年1995日1月1日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日日	基本 931.51 GB 联机	(C:) 78.13 GB NTFS 状态良好(系统,	(22:) 853.38 GB NTFS 状态良好(主分区)
	□ <b>磁盘 1</b> 基本 1023 MB 联机	<b>新加卷 (F:)</b> 1021 MB NTFS 状态良好 (主分区)	

#### 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除錯日志

### 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.將錯誤日志文件復制壓縮后發送給Curtain技術支援中心。

Vista以上系統除錯日志的位置:

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

Vista以下系统除錯日志的位置:

- \\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,請記得停止除錯日志: 停止日志,设定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三的令牌(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:

E Registry Editor
-------------------

File Edit View Favorites Help

V 📕 SOFT	WARE	^	Name	Туре	Data
> -]_ A	GEIA Technologies		ab ClientPath	REG_SZ	C:\Program Files\Coworkshop\Cu
> - ] C	lasses		100 DebugLog	REG_DWORD	0x0000000a (10)
>- <u></u> C	lients		BebugLogSave	REG_DWORD	0x0000000a (10)
✓ - C	oworkshop	100	11 DisableEFS	REG_DWORD	0x00000000 (0)
	Curtain 3		W FileBased	REG_DWORD	0x00000000 (0)
	oldy		10 FirstRun	REG_DWORD	0x00000000 (0)
	ntemedia		ab InstallPathAdmin	REG_SZ	C:\Program Files\Coworkshop\Cu
5 G	FAR Software		100 LocalEncryption	REG_DWORD	0x00000001 (1)
S G	ooale		LsdHelpHideSta	REG DWORD	0x00000000 (0)
> -1 IN	A Providers		11 Major	REG DWORD	0x0000003 (3)
> - 📕 Ir	itel		WigratedToPPD	REG DWORD	0x00000001 (1)
> -]_ K	hronos		110 Minor	REG DWORD	0x0000008 (8)
> 📜 K	nowles		ab Organization	REG SZ	Kelvin-samsung
> - 🧵 N	lacromedia		111 PatchPending	REG DWORD	0x00000000 (0)
> - 📒 N	licrosoft		ab ProductKey	REG SZ	ZP3VI-POI25-5HZH8-PNI.B8-7T1
> - 1 N	lozillaPlugins		111 Revision	REG DWORD	0x0000000 (0)
N	orton		SegNo	REG DWORD	0x0000001f (31)
> _ N	uance		ab Server	REG SZ	127.0.01
	VIDIA Corporation		ab Token	REG_SZ	(8C1322E1_2D00_4855_ADEA_E6)
	DBC		ab UserName	REG_SZ	Kelvin-campung
>-1 P	artner	~	C UserName	NE0_32	Retvill-sallisung

Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Coworkshop\Curtain 3

## 檢查Curtain管理端:

🔁 Curtain e-locker管理端	the second second	-					
文件(F) 查看(V) 客户端(C) 安全	策略(P) 语言(L) 帮助(H)	)					
📑 🗞 💞 📥 🕭	s 😂 🗊 😼	?					
□…□ 管理员管理	客户端	安全策略	域	状态	版本	最后上线时间	网络驱
白	S DESKTOP-9CPFDUR	Default Policy		正常	3273.2	2016-11-23 15:32:29	3273
逐 在线 (2) 逐 离线 (3) 	S Marsc-PC	test		正常	3273.2	2016-11-23 15:28:06	3273

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"。

Default Poli	cy		X
設定 务	A統策略   受控應用程式		
□ 停止到 受保護區	时受保護區的保護(不推薦)」 設定		
1	□ 隱藏我的電腦		
	🗌 隱藏本地受保護區	本地受保護區	ProtDir
	□ 禁止刪除網路磁碟機文檔	□ 附加受保護區	添加
<b>75</b> -50			_ 刪除
	<ul> <li>□ 九許用電郵發送敏感文檔</li> <li>☑ 電郵記錄</li> <li>□ 發送通知到</li> </ul>		添加 一 刪除
自動清理	□ 清理本地受保護區	□ 清理本地受保護	護區暫存目錄
	◎ 散動 ○ 毎週 日 - 二 三 □ □ □ □ □	○ 四五六 ○ 每週 日 □□□□□	
	▶ 下載后刪除文檔		描 0 天
	刪除文檔如果 所有 💌	符合	
複製到非	受保護區		
	● 不允許(推薦)	允許的副檔名	添加 複製選項
	○ 允許所有不支持的類型		
	<ul> <li>○ 元計部分副福名</li> </ul>	,	
		確定	取消 應用

2. 添加允許的副档名(例如:TXT)。



3. 單擊"添加"按钮,再確認。

Curtain e-	locker		×
?	此副檔名為受保護類型, 的相關設定,是否確定?	此設定將會推翻於受控照	應用程式中
		Yes	No

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)。

設定	伺服器信息	受保護網路	各磁碟機	受保護網路埠	例外埠	例外的共享	密碼管理
伺服器	Z						
伺	服器地址	埠	說明				
		添加伺服	民器		×		
		伺服器	地址				
		埠					_
-		0443					
		說明					
		_		確定	取消		_
				添加	刪除	修改	

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

伺服器地址	協議	埠			添加
		动埠	>	×	
	414.	102 169 1 19			刪除
	161	192.108.1.18	~		1/23/17
	埠	3030			194
	協調	、 ● TCP			
		_			

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 Vlew Setup把Loacl 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。		
設定 条統策略 受控應用程式		
□ 停止對受保護區的保護(不推薦) 受保護區設定		
🔀 🖂 臆藏我的電腦		
└────────────────────────────────────	本地受保護區	ProtDir
		C:\ndm view 法tm
業止刪時網路磁碟機×幅	▶ 附加文休護區	
102000		▼ 刪除

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。

常规 快捷方	式 兼容性 安全 详细信息 以前的版本
훥 Se	cure EPDM Client
目标类型:	应用程序
目标位置:	CBin
目标(I):	n 3\CBin\PDMWEClient.exe″ "C:\pdm view
起始位置(S):	"C:\Program Files\Coworkshop\Curtain 3
快捷键(K):	无
运行方式(图):	常规窗口
备注 @):	Secure EPDM Client
打开文件位	置 (E) 更改图标 (C) 高级 (D)

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。



Secure EPDM Client Shortcut 2.11 KB

😋 🔵 🗢 🔁 🕨 pdm v	riew ► test			• •j	提雲 pdm viev	<b>*</b>	×
组织▼ 检入 薪	取最新版本 历5	も记载 査阅文	件新文件夹			8≡ ◄ (	?
☆ 政憲実	🔁 操作 ▼ 修改	( ▼ 显示 ▼ 工具	•			•	
下载	名称	检出者	大小	文件类型	状态	已修改	检
三 桌面	double dire	Admin	1.09 MB	Toolbox Part		2010-06-13 12:	<w< td=""></w<>
最近访问的位置	single row	Admin	667.7 KB	Toolbox Part		2010-06-13 12:	< M
[] 库	T thrust ball b	Admin	922.13 KB	Toolbox Part		2010-06-13 12:	<w< td=""></w<>
📑 视频							
🔛 图片							
💽 文档							
👌 音乐							
🖳 计算机	•		ш				Þ
0. 54	分预览 国数据	屠卡 🗐 版本 1/1	🛅 材料明细表	品包含 習使用	月处		
♥♥ 网络		-		3 o Ho	Default		
🐊 pdm view		- 11. P		· 变量		数值	-
				Date			
				Descriptio	on		
				Heat Trea	at		
				Material			
		P					F