AUTHORIZED DOCUMENTATION

管理主控台說明

August 1, 2008

Novell®
ZENworks Endpoint Security Management

3.5

www.novell.com

法律聲明

Novell, Inc. 不對本文件的內容或使用做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時修訂本說明文件或更改內容，而無義務向個人或團體告知這類修訂或變更。

此外，Novell, Inc. 不對軟體做任何表示或保證，且特別聲明不對任何特定用途的適銷性或適用性提供任何明示或默示的保證。此外，Novell, Inc. 有權隨時變更部份或全部 Novell 軟體，而無義務向個人或團體告知這類變更。

此合約下提到的任何產品或技術資訊可能受美國出口管制法與其他國家 / 地區的貿易法的限制。您同意遵守所有出口管制規定，並同意取得出口、再出口或進口產品所需的一切授權或類別。您同意不出口或再出口至目前美國出口排除清單上所列之實體，或是任何美國出口法所指定之禁運或恐怖主義國家。您同意不將交付產品用在禁止的核武、飛彈或生化武器等用途上。請參閱 Novell 國際貿易服務網頁 (http://www.novell.com/info/exports/)，以取得有關出口 Novell 軟體的詳細資訊。Novell 無需承擔您無法取得任何必要的出口核准之責任。

對於本文件中所述及之所有產品內附技術，Novell, Inc. 皆具有其智慧財產權。特別是 (但不限於) 這些智慧財產權可能包含 Novell 法律專利網頁 (http://www.novell.com/company/legal/patents/) 中所列的一或多項美國專利，以及在美國與其他國家 / 地區的一或多項其他專利或申請中的專利。

Novell, Inc.
404 Wyman Street, Suite 500
Waltham, MA 02451
U.S.A.
www.novell.com

*線上文件：*如需存取 Novell 此產品與其他產品的最新線上文件，請參閱 Novell 文件網頁 (http://www.novell.com/documentation)。

Novell 商標

若要查看 Novell 商標，請參閱 Novell 商標和服務標誌清單 (http://www.novell.com/company/legal/trademarks/tmlist.html)。

協力廠商資料

所有的協力廠商商標均爲其各別擁有廠商的財產。

目錄

1 使用 ZENworks Endpoint Security 管理主控台

「管理主控台」爲「Novell® ZENworks® Endpoint Security 管理服務」的集中式存取與控制。

若要啓動「管理主控台」登入視窗，請按一下「*開始*」>「*程式集*」>「*Novell*」>「*ESM 管理主控台*」>「*管理主控台*」。指定管理員名稱及密碼，即可登入「主控台」。輸入的使用者名稱必須是「管理服務」上的授權使用者 (請參閱 「使用許可設定 許可設定」(第 9 頁))。

附註：我們建議您關閉或最小化未使用的主控台。

1.1 使用任務列

您可以在左側的任務列中存取「管理主控台」。如果未顯示任務列，請按一下主控台左側的「*任務*」按鈕。

以下幾節中所包含的資訊可讓您瞭解如何使用任務列來執行各種任務：

- 「規則任務」(第 8 頁)
- 「資源」(第 8 頁)
- 「組態」(第 8 頁)
- 「端點稽核」(第 8 頁)

1.1.1 規則任務

管理主控台的主要功能爲建立安全性規則並將其套用至受管理的端點設備。規則任務可在建立及編輯安全性規則的過程中逐步引導管理員，而 ZENworks® Security Client 便會使用此規則將集中管理之安全性套用至各端點設備。

規則任務包括以下項目：

- **使用中的規則：**顯示目前可供檢閱與編輯的規則清單。按一下規則以將其開啓。
- **建立規則：**啓動「新規則精靈」以建立新的安全性規則。
- **輸入規則：**顯示「輸入規則」對話方塊，使您能夠輸入使用其他管理服務所建立的規則。如需詳細資訊，請參閱 「輸入規則」(第 100 頁)。

當您按一下任何一個規則任務時，任務列將會最小化。按一下左側的「*任務*」按鈕以將其重新開啓。

請參閱 第 2 章 「建立並配送 安全性規則」(第 43 頁)，來瞭解規則任務，以及如何建立和管理安全性規則。

1.1.2 資源

「資源」任務清單會顯示可用的技術支援和說明資源：

- **聯絡支援：**啓動瀏覽器並顯示 Novell® Contact and Offices 頁面。
- **線上技術支援：**啓動瀏覽器並顯示 Novell Training and Support 頁面。
- **管理主控台說明：**啓動 ZENworks® Endpoint Security Management 線上說明。

1.1.3 組態

「管理服務組態」視窗可提供對於 ZENworks® Endpoint Security Management 伺服器基礎架構的控制，以及對於監視其他企業目錄服務的控制。如需詳細資訊，請參閱 「使用組態視窗」(第 13 頁)。當執行「獨立」管理主控台時，無法使用此控制。如需詳細資訊，請參閱《*ZENworks Endpoint Security Management 安裝指南*》。

1.1.4 端點稽核

您可以使用「端點稽核」視窗來存取 ZENworks® Endpoint Security Management 的報告和警示功能。

報告：「報告」在存取和實作強大安全性規則時相當重要。按一下「*報告*」，即可透過「管理主控台」存取報告。所收集和回報的端點安全性資訊也是完全可設定，而且可依領域、群組或個別使用者來收集。如需詳細資訊，請參閱 「使用報告」(第 28 頁)。

警告：警告監視可確保「管理主控台」中會報告任何破壞公司安全性規則的嘗試。警告可通知 ZENworks Endpoint Security Management 管理員潛在的問題，並讓管理員執行任何適當的修復動作。您可以在「警告」儀表板上進行完整的設定，使您能夠控制觸發警告的時間和頻率。如需詳細資訊，請參閱 「使用警告監視」(第 25 頁)。

1.2 使用功能表列

ZENworks® Endpoint Security Management 功能表列可讓您存取 「管理主控台」的所有功能。

下列選項可供使用：

- **檔案：**使用 「檔案」功能表來建立並管理安全性規則。
  - **建立新規則：**啓動 「新規則精靈」以建立新的安全性規則。
  - **重新整理規則清單：**更新 「規則」清單，以顯示所有使用中的規則。
  - **刪除規則：**刪除選定的規則。
  - **輸入規則：**讓您將規則輸入 「管理主控台」。
  - **輸出規則：**讓您將規則和所需的 setup.sen 檔案輸出至 「管理服務」資料庫外部的指定位置。
  - **結束：** 關閉 「管理主控台」軟體，並登出使用者。
- **工具：**使用 「工具」功能表來控制 「管理服務」的組態、加密鑰與權限。
  - **組態：**開啓 「組態」視窗。
  - **輸出加密鑰：**開啓 「輸出加密鑰」對話方塊，您可在此指定要輸出的金鑰以及密碼。
  - **輸入加密鑰：**開啓 「輸入加密鑰」對話方塊，您可在此指定要輸入的金鑰以及密碼。
  - **產生新金鑰：**產生要使用的新加密鑰以強制執行資料保護。
  - **許可：**開啓 「許可」視窗。
- **檢視：**使用 「檢視」功能表，可讓您不必透過任務列來執行金鑰規則任務。
  - **規則：**當規則開啓時，將檢視窗切換至該規則。
  - **使用中的規則：**顯示規則清單。
  - **警告：**顯示 「警告」儀表板。
  - **報告：**顯示 「報告」儀表板。
- **說明：**顯示 「管理主控台說明」工具和 「關於」對話方塊：
  - **說明：**啓動 「管理主控台」線上說明以引導您執行規則建立和所有的 「管理主控台」任務。您也可以按一下鍵盤上的 F1 來使用 「說明」。
  - **關於管理主控台：**啓動 「關於」視窗，會顯示安裝類型 (ZENworks Endpoint Security Management 或 UWS)，以及 「管理主控台」目前的版本號碼。此視窗也是在安裝之後才購買產品時輸入授權金鑰的地方。

1.3 使用許可設定 許可設定

您可以在 「工具」功能表中找到 「許可設定」，而且只有 「管理服務」的主要管理員，和 / 或已由該管理員授予 「許可」存取的管理員可以存取。當執行 「獨立」管理主控台時，無法使用此控制。

許可設定可定義哪些使用者或使用者群組可存取「管理主控台」、「管理許可」或「發行至」設定。

在「管理伺服器」安裝期間，將管理員或資源使用者的「資源帳戶」名稱輸入組態表格中 (請參閱《*ZENworks Endpoint Security Management 安裝指南*》)。一旦測試已成功執行並儲存使用者資訊之後，系統會將所有的許可自動授予該使用者。

在安裝「管理主控台」後，資源使用者是唯一具有完整許可的使用者，不過系統會將「管理主控台」的存取權授予領域中的所有使用者群組。針對不需要存取權的群組或使用者，資源使用者可移除其存取權。資源使用者可針對指定的使用者設定其他許可。

當「管理主控台」啓動時，系統會從「許可」表格取回許可。這些許可會告訴主控台，該使用者是否有權限可以登入主控台、建立或刪除規則、變更許可設定，以及他們是否可發行規則及允許他們將之發行給誰。

所提供的存取設定包括：

- **管理主控台存取：**使用者可檢視規則和元件，並編輯現有的規則。僅獲得此權限的使用者將不得新增或刪除規則；且無法使用發行和許可選項。
- **發行規則：**使用者只能將規則發行給指定的使用者或群組。
- **變更許可：**使用者可存取和變更已定義之其他使用者的許可設定，並將許可授予新的使用者。
- **建立規則：**使用者可在管理主控台中建立新規則。
- **刪除規則：**使用者可刪除管理主控台中的任何規則。

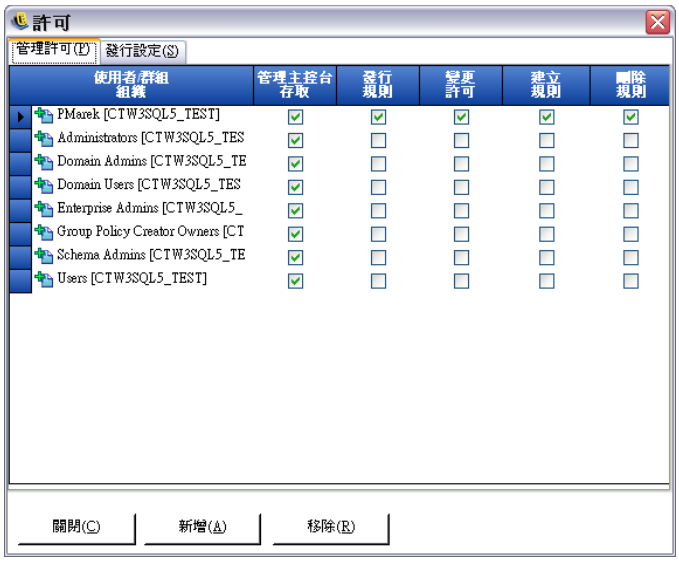
附註：基於安全性目的，建議您只將「變更許可」和「刪除規則」許可授予資源使用者或少數的管理員。

1.3.1 管理許可

若要設定管理許可：

1 按一下「*工具*」>「*許可*」。

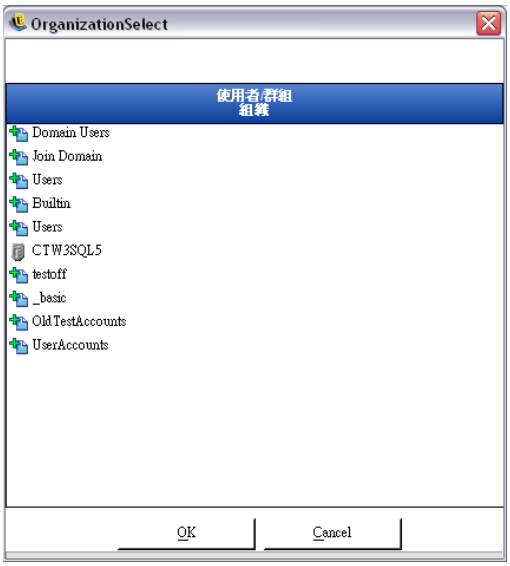
與此領域相關聯的群組即會顯示。



附註：雖然所有群組都將無法執行規則任務，但依照預設值都會授予「管理主控台」的存取權。您可以藉由取消勾選許可來移除對於主控台的存取權。

2 若要將使用者或群組載入此清單：

2a 按一下畫面底端的「*新增*」按鈕。



2b 從清單中選取適當的使用者或群組。若要選取多位使用者，可按住 CTRL 鍵個別選取，或者先選取第一個選項，然後按住 SHIFT 鍵，接著選取最後一個選項，即可選取一系列的使用者。

2c 在選取所有使用者或群組之後，按一下「*確定*」按鈕。

3 將任何 (或全部) 許可指定給可用的使用者或群組。

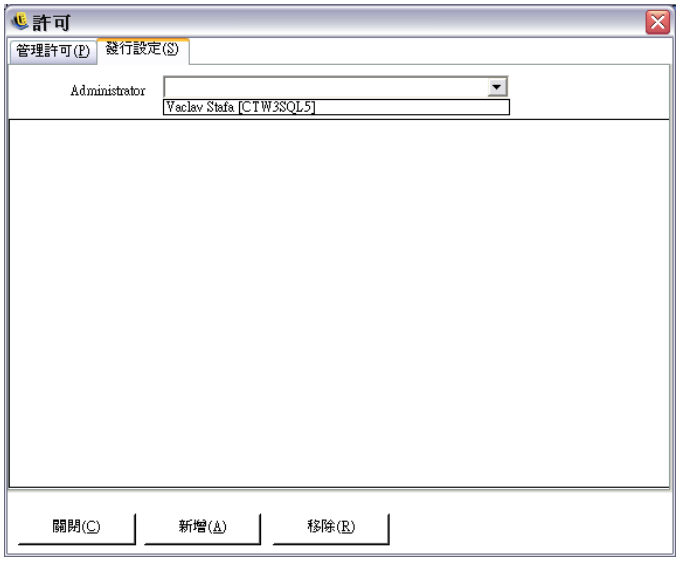
若要移除選取的使用者或群組，請將名稱反白後按一下「*移除*」。選取的名稱將移回組織表中。

1.3.2 發行至設定

已勾選「*發行規則*」的使用者或群組必須指定要發行的使用者或群組。

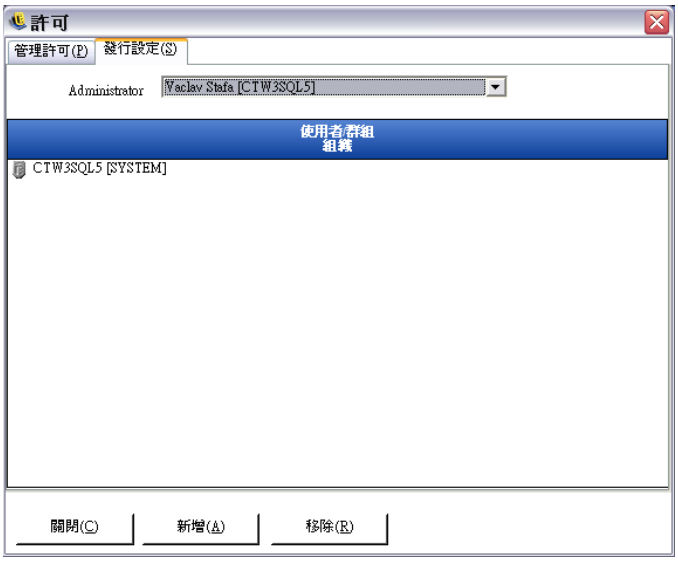
若要設定「發行至」設定：

1. 按一下「*發行至設定*」索引標籤。
2. 從下拉式清單選取已授予「發行」許可的使用者或群組。



3. 將使用者或群組指定給此使用者 / 群組：
   - **3a** 按一下畫面底端的「*新增*」按鈕將，以顯示組織表。
   - **3b** 從清單中選取適當的使用者或群組。您可以使用 Ctrl 和 Shift 鍵選取多個使用者。
   - **3c** 在選取所有的使用者或群組時，請按一下「*確定*」按鈕將使用者和群組新增至所選名稱的

     發行清單。



系統會立即執行許可設定。

4 若要移除選取的使用者 / 群組，請選取清單中的名稱，然後按一下「*移除*」。

5 按一下「*關閉*」以接受這些變更並回到編輯器。

選取的名稱將移回組織表中。

當新增新的目錄服務時 (請參閱 「驗證目錄」(第 15 頁))，輸入的「資源帳戶」將獲得完整的許可設定，如以上所述。

1.4 使用組態視窗

「組態」視窗讓 ZENworks® Endpoint Security Management 管理員可以存取「*基礎結構和編程*」、「*驗證目錄*」及「*伺服器同步*」等控制。按一下主要頁面上的「*組態*」連結，或按一下「*工具*」功能表，然後按一下「*組態*」。「組態」視窗就會顯示。

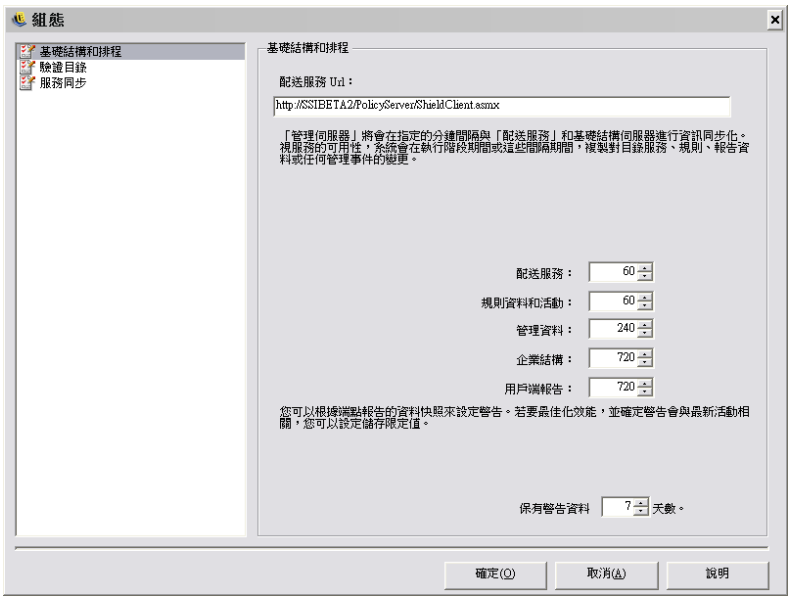
附註：當執行獨立管理主控台時，無法使用此功能。

以下幾節中包含了更詳細的資訊：

- 「基礎結構和編程」(第 13 頁)
- 「驗證目錄」(第 15 頁)
- 「服務同步」(第 24 頁)

1.4.1 基礎結構和編程

基礎結構和編程模組可讓 ZENworks Endpoint Security Management 管理員指定和變更「規則配送服務 URL」，並控制 ZENworks Endpoint Security Management 元件的同步間隔。



以下幾節中包含了更詳細的資訊：

- 「配送服務 URL」(第 14 頁)
- 「編程」(第 14 頁)

配送服務 URL

如果 「規則配送服務」已移至新的伺服器，這將會更新 「管理服務」和所有 ZENworks Security Client 的 「規則配送服務」位置 (而不需重新安裝)。目前伺服器的 URL 會列於文字欄位中。

如果您要變更伺服器，只需要變更伺服器名稱，以指向新的伺服器。請勿變更伺服器名稱之後的任何資訊。

例如，如果目前所列的 URL 爲 http:\\ACME\PolicyServer\ShieldClient.asmx，且 「規則配送服務」已安裝於新的伺服器 (ACME 43) 上，則 URL 應更新爲：
http:\\ACME43\PolicyServer\ShieldClient.asmx

在更新 URL 之後，請按一下 「*確定*」以更新所有的規則並傳送 「規則配送服務」的自動更新。這也會更新 「管理服務」。

當您變更伺服器 URL 時，更新規則的順應性層級到達 100% 之前，您不能終止舊的 「規則配送服務」(請參閱 「使用報告」(第 28 頁))。

編程

「編程」元件允許 ZENworks Endpoint Security Management 管理員指定 「管理服務」將與其他 ZENworks Endpoint Security Management 元件執行同步的時機，可確保所有資料與佇列的工作會符合任何最新的活動，以及爲 SQL 維護工作進行編程。所有的時間增量都以分鐘爲單位。

編程可細分爲以下各項：

- **配送服務：**與 「規則配送服務」的同步編程。

- **規則資料和活動：**與規則更新的同步編程。
- **管理資料：**與「管理服務」的規則同步。
- **企業結構：**與企業目錄服務 (eDirectory™、Active Directory*、NT 領域 * 和 / 或 LDAP) 的同步編程。您可以監視企業目錄服務中的變更，如此即可偵測到使用者規則指定中的對應變更，並將之傳送至「規則配送服務」，以供「用戶端」驗證之用。
- **用戶端報告：**「管理服務」向「規則配送服務」詢問並下載報告資料的頻率。
- **保有警告資料：**您可以根據端點所報告的資料快照來設定警告。您可以設定以天數爲限制的儲存限定值，以獲得最佳效能，並確保警示皆與最新的活動相關。

1.4.2 驗證目錄

安裝 ZENworks® Endpoint Security Management 後，必須建立和設定目錄服務，才能開始管理系統中的設備。

「新增目錄服務組態精靈」讓您建立目錄服務組態，以定義 ZENworks Endpoint Security Management 用戶端安裝的範圍。新組態會使用現有的目錄服務，以定義使用者爲主和電腦爲主的用戶端安裝邏輯邊界。

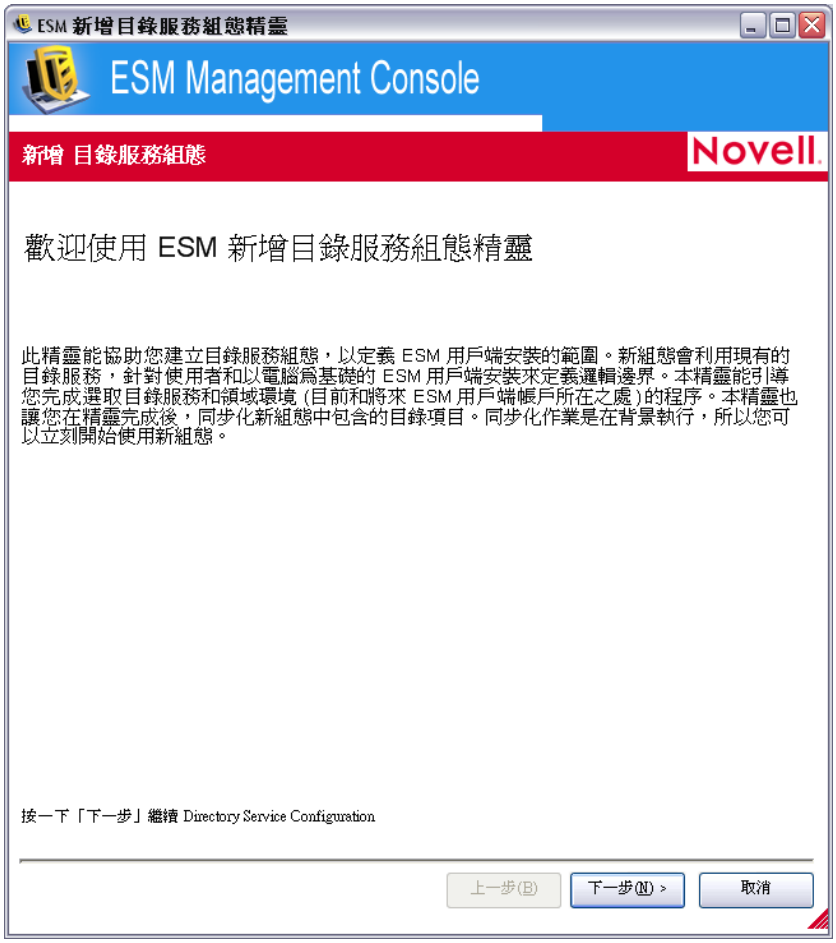
此精靈可引導您完成選取目錄服務和網路位置 (目前與未來用戶端帳戶所在之處) 的程序。

此精靈也讓您同步化新組態中包含的目錄項目。本同步作業在背景執行，所以您可立刻啓用新組態。

安裝 ZENworks Endpoint Security Management 後，就會自動顯示「新增目錄服務組態精靈」。若您剛剛安裝完此產品且已經顯示「歡迎」頁面，請跳至下列程序的 步驟 4。

若要設定目錄服務：

1. 在管理主控台中，按一下「*工具*」>「*組態*」。
2. 按一下「*驗證目錄*」。
3. 按一下「*新增*」以啓動「新增目錄服務組態精靈」。



4 按一下「*下一步*」以顯示「組態伺服器」頁面。

5 填寫下列欄位：

- **服務類型**：從「*服務類型*」下拉式清單選取服務類型：
  - Microsoft 現用目錄
  - Novell eDirectory
- **名稱**：指定易記名稱以描述此目錄服務組態。
- **主機名稱**：指定或瀏覽至此目錄伺服器的 DNS 名稱或 IP 位址。
- **埠**：指定用來連接目錄伺服器的連接埠。

  預設值爲連接埠 389。若您使用其他連接埠連接至目錄伺服器，則可指定該連接埠。

6 按一下「*下一步*」以顯示「提供身分證明」頁面。

7 填寫下列欄位：

- **使用者名稱：**指定帳戶管理員以連結至此目錄。

  此帳戶會成爲目錄服務組態的管理員。擁有該登入名稱的使用者必須具有檢視整個目錄樹狀結構的許可。建議這位使用者由網域管理員或 OU 管理員擔任。請使用 LDAP 格式來設定 eDirectory，例如：cn=admin,o=acmeserver，其中 cn 爲使用者，而 o 爲儲存使用者帳戶的物件。

- **密碼：**指定該帳戶管理員的密碼。

  此帳戶會成爲目錄服務組態的管理員。

  您不能將密碼設有過期期限，且不能停用此帳戶。

- **網域：**指定帳戶管理員所屬的網域。

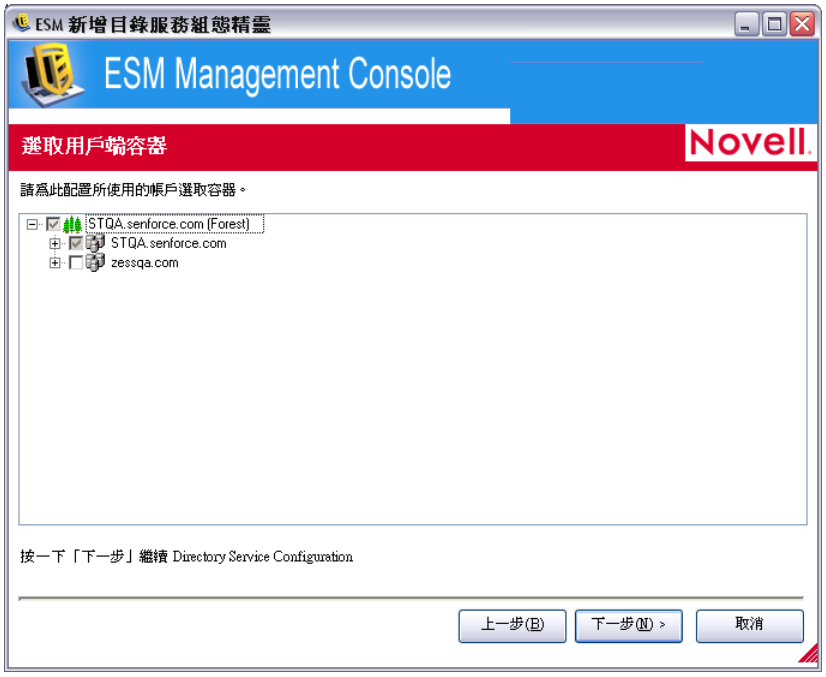
- **使用安全認證連接至此伺服器：**若您不要使用安全認證，請取消選取此選項。依預設值，已啓用此選項。

8 按一下「*下一步*」繼續。

9 若您在 步驟 7 中指定的組態管理員使用者不在此網域中，則會顯示「搜尋帳戶項目」頁面。

指定管理員所在的容器，然後按「*下一步*」。

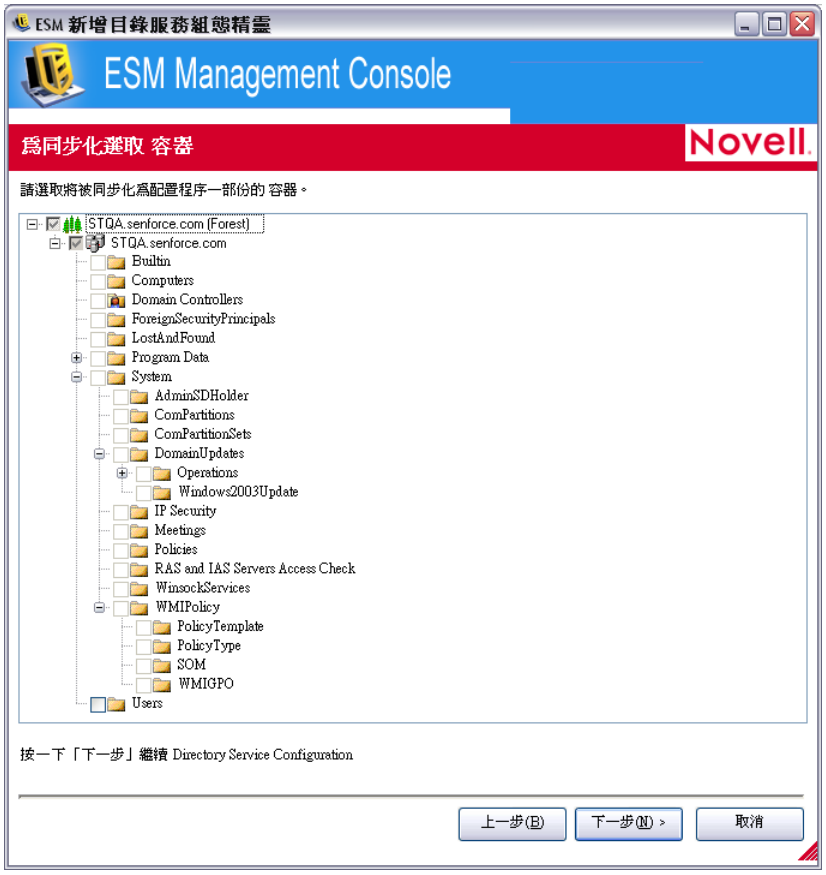
10 在「選取驗證網域」頁面上瀏覽樹狀結構，以選取用來驗證本組態的使用者與電腦的網域。



此時已選取包含您在 步驟 7 中所指定之管理使用者的網域，而且無法取消選擇。

若管理伺服器不是組態中所選取網域的成員，則任何用戶端安裝嘗試簽入此管理伺服器時均會失敗。

11 按一下「 *下一步*」以顯示「選取用戶端容器」頁面，然後選取此組態所用帳戶之容器。

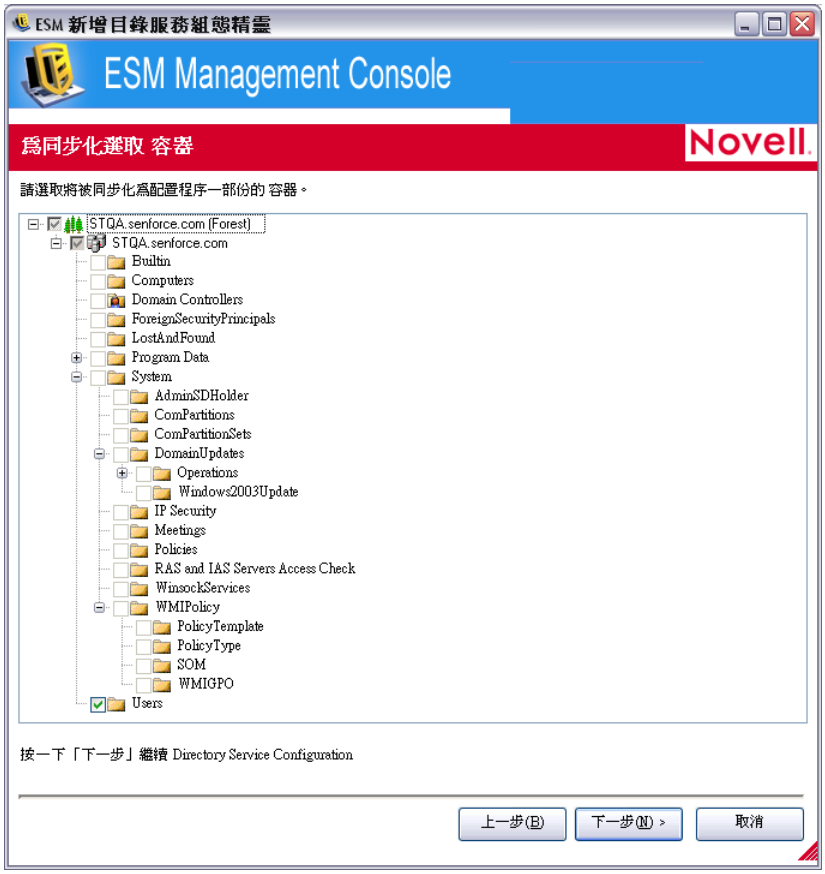


此時已選取包含您在 步驟 7 中所指定之管理使用者的容器，而且無法取消選擇。

「選取用戶端容器」頁面讓您把搜尋範圍縮小到只有包含受管理使用者與電腦的容器，以提昇效能。

若管理伺服器的帳戶不在組態中所選取的其中一個容器內，則任何用戶端安裝如果嘗試簽入此管理伺服器，安裝就會失敗。

12 按一下「*下一步*」以顯示「同步容器」頁面。



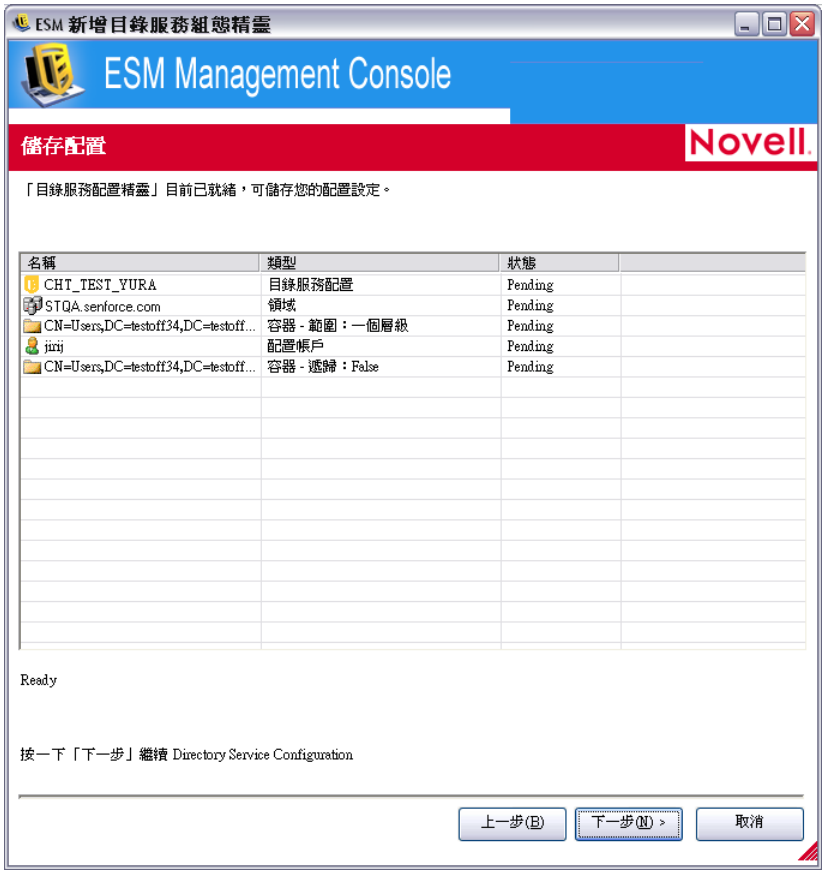
13 (選擇性) 選取組態程序內的欲同步化容器。

本同步作業在背景執行，所以您可立刻啓用新組態。若您要同步化的使用者與電腦極多，則可能需耗費數小時。

若您未指定需同步化的容器，則這些容器中的使用者和電腦在簽入時會填入管理主控台。

同步化容器的動作會將這些使用者與電腦預先填入管理主控台，讓您立刻執行建立安全規則的這類動作。使用者或電腦簽入系統時，就會推送這些規則並予以套用。預先填入管理主控台後，您便可立刻開始建立個別使用者或電腦專屬的規則，而不是建立適用於容器中所有使用者與電腦的規則。若容器不同步化，則必須等到這些使用者和電腦簽入系統後，才能爲不同的使用者或電腦建立獨特規則。

14 按一下「*下一步*」以顯示「儲存組態」頁面。



15 檢閱此資訊，然後按「*下一步*」儲存組態。

必要時可按「*上一步*」變更任何設定。

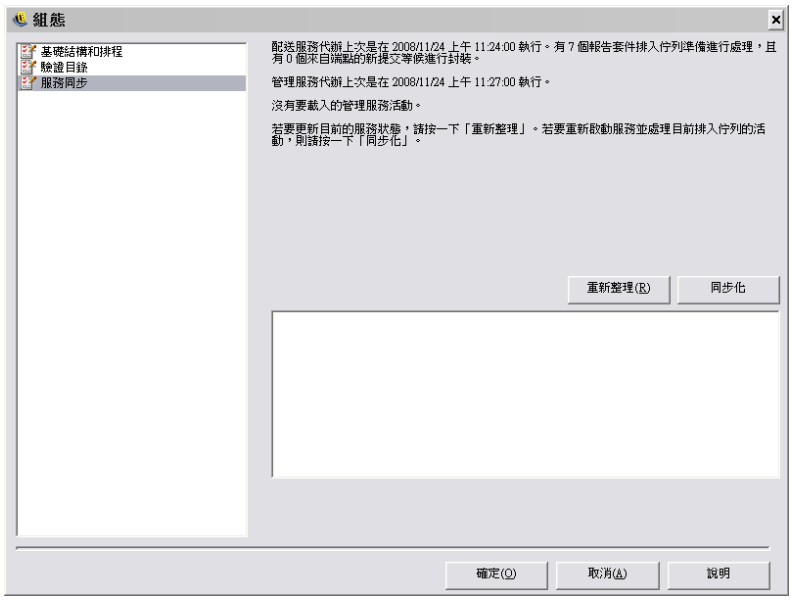
16 按一下「*完成*」。

按一下「*完成*」時，Windows 通知區域中會顯示 圖示並開始同步。您可連按兩下此圖示以顯示「目錄服務同步」對話方塊。

同步會在背景執行。若您離開管理主控台，同步作業就會停止。再度開啓管理主控台時，同步作業就會從原先停止的地方繼續執行。

1.4.3 服務同步

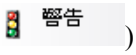
此控制讓您可以強制同步 「管理服務」和 「規則配送服務」。這將會更新所有的警告、報告及規則配送。



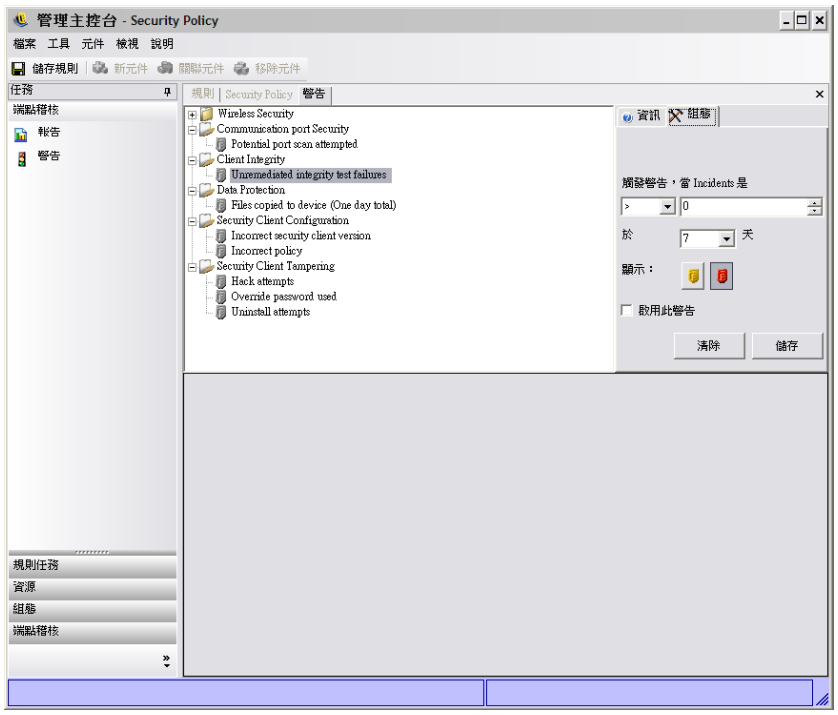
1. 若要更新目前的服務狀態，請按一下「*重新整理*」。
2. 若要重新啓動服務並處理目前佇列的活動，請按一下「*同步化*」。

1.5 使用警告監視

警告監視可讓 ZENworks® Endpoint Security Management 管理員在整個企業中判斷所有 ZENworks Endpoint Security Management 受管理端點的安全性狀態。警告觸發爲完全可設定，且會報告警告或完整的緊急警告。此工具可透過任務列上的「*端點稽核*」或透過「*檢視*」功能表來存取。

1 若要存取「警告」，請按一下「警告」圖示 (

)。



警告監視可用於下列區域中：

- **用戶端完整性：**通知未補救之完整性測試結果。
- **通訊埠安全性：**通知潛在的連接埠掃描嘗試。
- **資料保護：**通知在過去一天內複製到抽取式儲存設備之檔案。
- **安全性用戶端組態：**通知不正確之安全性用戶端版本和不正確之規則。
- **安全性用戶端竄改：**通知使用者入侵嘗試、解除安裝嘗試及置換密碼之使用。
- **無線安全性：**通知不安全之存取點 (包括由使用者偵測到和連接的存取點)。

1.5.1 設定 ZENworks Endpoint Security Management 以提供警告

警告監視要求要定期收集並上載報告資料，以取得目前端點安全性環境的最精確狀況。不受管理的 ZENworks® Security Client 不會提供報告資料，因此不會包含於「警告」監視中。

以下幾節中包含了更詳細的資訊：

- 「啓動報告」(第 26 頁)
- 「最佳化同步服務」(第 27 頁)

啓動報告

「報告」應於每個安全性規則中加以啓動。請參閱 「規範報告」(第 95 頁)，以取得設定安全性規則之報告的詳細資料。請將報告傳送時間調整爲可持續更新端點狀態的間隔。此外，警告沒有報告將無法啓動。任何您希望收到警告的活動，都必須在安全性規則中，具備已指定給它的適當報告。

最佳化同步服務

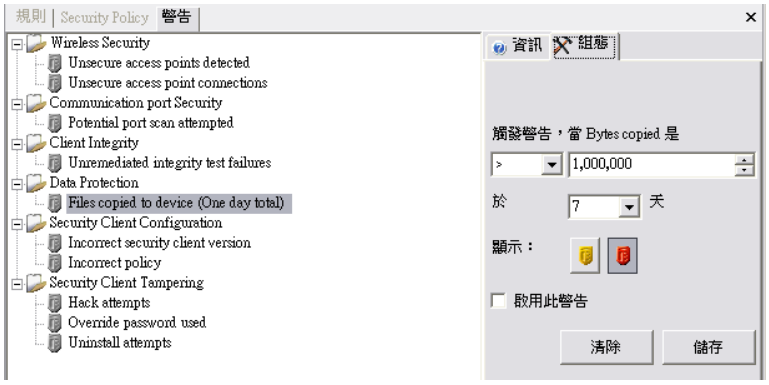
依照預設，「ENworks Endpoint Security Management 報告」服務每隔 12 小時會進行一次同步化。這表示在安裝 ZENworks Endpoint Security Management 後的 12 小時之前，最初的報告和警告資料並未就緒。若要調整這個時間範圍，請開啓「組態」工具 (請參閱 「編程」(第 14 頁))，並將「*用戶端報告*」時間調整符合爲您需求和環境的分鐘數。

立即需要資料時，「組態」工具中的「*服務同步*」選項可立即自行處理「規則配送服務」(其會從端點收集報告資料) 及「報告服務」(其會根據最新收集的資料來更新所有警告)。如需詳細資料，請參閱 「服務同步」(第 24 頁)。

1.5.2 設定警告觸發

警告觸發可調整爲符合貴公司安全性需求的限定值。

1 在清單中選取警告，然後按一下管理主控台右側的「*組態*」索引標籤。



2 在下拉式清單中選取條件以調整觸發限定值。這表示觸發數目爲下列狀況：
- 等於 (=)
- 大於 (<)
- 大於或等於 (<=)
- 小於 (>)
- 小於或等於 (>=)

3 調整觸發數目。此數目會視警告類型而有所不同。

4 選取必須達到此數目的間隔。

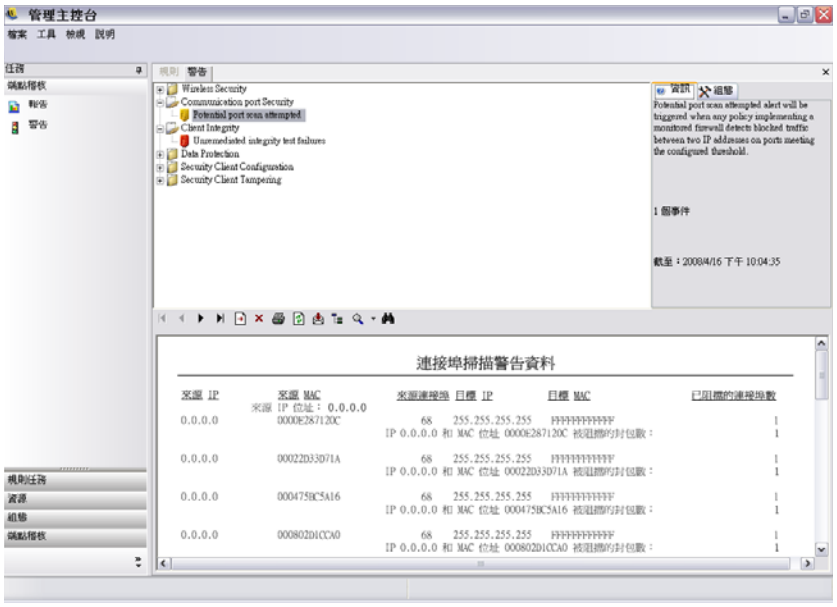
5 選取觸發類型。它可以是一個警告圖示 () 或緊急圖示 ()。

6 確定您已勾選「*啓用此警告*」方塊。

7 按一下「*儲存*」以儲存警告。

1.5.3 管理警告

警告會通知您端點安全性環境內需要補救的問題。一般來說，系統會在個別或群組的基礎上來進行補救。爲了協助識別問題，在選取警告時，即會顯示「警告」報告。



此報告會顯示目前的觸發結果，並且顯示受影響之使用者或設備的資訊。所提供的資料會提供必要資訊，來採取補救動作，以更正任何可能發生的公司安全性問題。可藉由開啓「報告」找到其他資訊。

採取補救動作之後，在下一次報告更新之前，警告都將維持作用中。若要在編程的更新之前清除警告：

1 在清單中選取警告，然後按一下管理主控台右側的「*組態*」索引標籤。

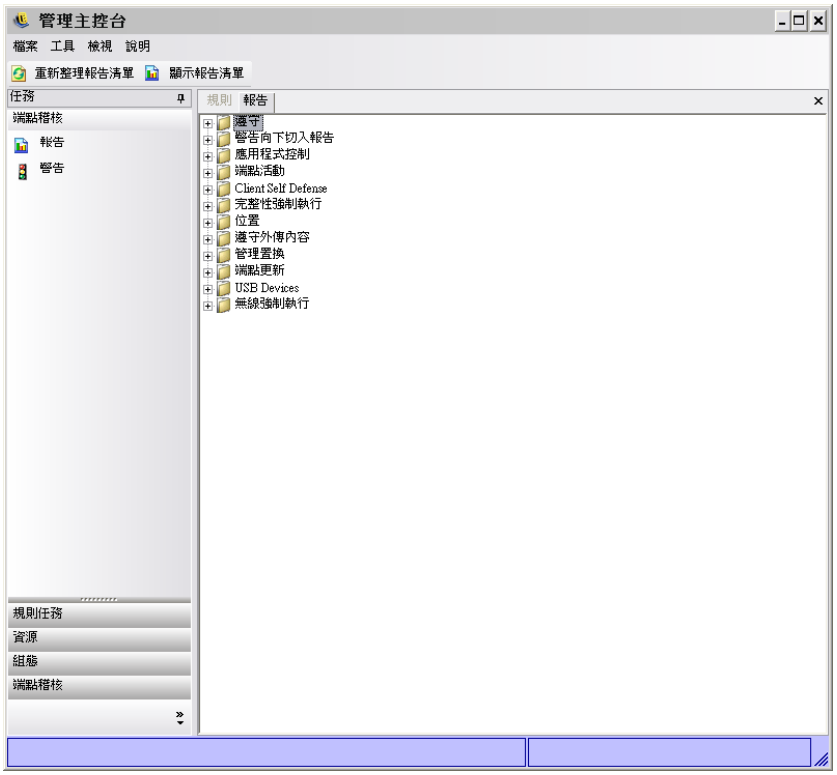
2 按一下「*清除*」。

這會清除警告中的報告資料 (您仍然可以在報告資料庫中使用該資料)。在收到新資料之前，它將不會重新啓用。

1.6 使用報告

「報告服務」可爲企業提供「順應性」和「狀態」報告。可爲目錄和目錄內的使用者群組提供可用資料。Novell® 報告會提供個別規則元件可在企業端點上產生之影響的意見反應。這些報告的申請是設定於「安全性原則」中 (請參閱 「規範報告」(第 95 頁))，而且可以提供有用的資料來判斷規則更新。

請在「*端點稽核*」任務列或「*檢視*」功能表中選取「*報告*」。可用報告清單就會顯示 (按一下每個報告類型旁邊的加號圖示，以展開清單)。



您可藉由識別日期範圍和其他參數 (例如使用者或位置) 來設定報告。若要設定日期，請展開行事曆檢視窗，然後選取月和日。請按一下「日」來變更日期參數。

按一下「*檢視*」以產生報告。

在產生報告之後，您可以透過「管理主控台」的報告工具列來檢視報告、列印報告，並透過電子郵件寄送，或將報告輸出爲 .pdf 檔案。

檢閱報告時，箭頭按鈕可協助您瀏覽報告中的每一頁。報告的第一頁通常會有圖表和圖形，其餘頁面上則會顯示收集的資料，依日期和類型排序。

「*印表機*」按鈕可讓您使用此電腦的預設印表機列印完整報告。

「*輸出*」按鈕會將報告儲存爲 PDF 檔案、Excel* 試算表、Word 文件或 RTF 檔案。

「*群組樹狀結構*」按鈕會將參數清單切換至報告的一側。選取這些參數中的任一個，以便進一步「向下切入」報告。按一下「*群組樹狀結構*」按鈕，以關閉提要欄位。

「*放大鏡*」按鈕可提供下拉式功能表，以調整目前檢視窗的大小。

「*雙筒望遠鏡*」按鈕可開啓搜尋視窗。

例如，當您的滑鼠滑過特定參數 (例如使用者名稱或設備名稱)，滑鼠指標將會變成放大鏡。您可以連按兩下該特定項目，只顯示該物件的新報告。按一下「*關閉*」按鈕，以關閉目前的檢視窗，並返回原始的報告。

若要返回報告清單，可按一下報告視窗上方的「*報告清單*」圖示。

在資料從 ZENworks® Security Client 上載之前，將無法使用報告。依照預設，「ENworks Endpoint Security Management 報告」服務每隔 12 小時會進行一次同步化。這表示在安裝 ZENworks Endpoint Security Management 後的 12 小時之前，最初的報告和警告資料並未就緒。若要調整這個時間範圍，請開啓「組態」工具 (請參閱 「編程」(第 14 頁))，並將「*用戶端報告*」時間調整符合爲您需求和環境的分鐘數。

沒有資料可用的報告，其「*設定*」或「*預覽*」按鈕會呈現黯淡，且下方會出現「沒有資料」的字樣。

下列是可用的報告：

- 「順應性報告」(第 31 頁)
- 「警告向下切入報告」(第 31 頁)
- 「應用程式控制報告」(第 32 頁)
- 「加密解決方案報告」(第 32 頁)
- 「端點活動報告」(第 33 頁)
- 「端點更新報告」(第 33 頁)
- 「用戶端自我防禦報告」(第 33 頁)
- 「完整性強制執行報告」(第 34 頁)
- 「位置報告」(第 34 頁)
- 「外傳內容規範報告」(第 34 頁)
- 「管理置換報告」(第 35 頁)
- 「端點更新報告」(第 35 頁)
- 「無線強制執行報告」(第 36 頁)

1.6.1 順應性報告

「順應性報告」可根據安全性規則配送至受管理使用者的狀態，來提供規範資訊。100% 的順應性分數表示所有受管理的使用者均已 「登入」並接收到目前的規則。

下列是可用的報告：

- **端點登入順應性：**提供企業端點登入後天數與其目前規則期限的摘要。摘要報告中的這些數字都是平均值。此報告不需輸入任何變數。報告將依名稱顯示使用者，並顯示已指定給使用者的規則、使用者上次登入後的天數，以及其規則的期限。
- **端點用戶端版本：**顯示每個端點上用戶端的最新報告版本。請設定日期參數以產生此報告。
- **不曾登入的端點：**列出已向 「管理服務」註冊，但不曾向 「配送服務」檢查規則更新的使用者帳戶。請選取一或多個群組，以產生報告。

  這些可能是 「管理主控台」使用者，但是並未在名下安裝 「安全性用戶端」。
- **群組規則不符規範：**顯示有部分使用者未具備正確規則的群組。您可針對一或多個群組進行選擇，以產生報告。
- **依機器的端點狀態歷程：**顯示受 ZENworks Endpoint Security Management 保護之端點的最新狀態 (在特定日期範圍內)，並依照機器名稱分組。它會顯示登入的使用者名稱、目前規則、ZENworks Endpoint Security Management 用戶端版本和網路位置。此報告需要輸入日期範圍。管理員可連按兩下任何項目來向下切入，以查看特定機器之狀態報告的完整清單。
- **規則指定：**顯示哪些使用者和群組 (帳戶) 已收到指定的規則。請從清單中選取想要的規則，然後按一下 「*檢視*」以執行報告。
- **依使用者的端點狀態歷程：**顯示受 ZENworks Endpoint Security Management 保護之端點的最新狀態 (在特定日期範圍內)，並依照使用者名稱分組。它會顯示機器名稱、目前規則、ZENworks Endpoint Security Management 用戶端版本和網路位置。此報告需要輸入日期範圍。管理員可連按兩下任何項目來向下切入，以查看特定使用者之狀態報告的完整清單。

1.6.2 警告向下切入報告

「警告向下切入」報告可提供其他的警告資訊。這些報告只有在觸發警告時才會顯示資料。清除警告也會清除警告報告，不過，資料仍可於標準報告中取得。

下列是可用的報告：

- **用戶端竄改警告資料：**顯示使用者進行了未經授權之嘗試，以修改或停用 ZENworks Security Client 的執行個體。
- **複製檔案警告資料：**顯示已將資料複製到抽取式儲存設備的帳戶。
- **不正確用戶端版本警告資料：**顯示 「ZENworks Security Client 更新」程序的狀態歷程。
- **不正確用戶端規則警告資料：**顯示沒有正確規則的使用者。
- **完整性失敗警告資料：**回報用戶端完整性檢查成功和失敗之歷程。
- **置換嘗試警告資料：**顯示用戶端自我防禦機制已遭管理員置換的執行個體，在 ZENworks Security Client 上授予有權限的控制。

- **連接埠掃描警告資料**：顯示不同的連接埠數量上已封鎖的封包數量 (大量的連接埠可能表示發生了連接埠掃描)。
- **解除安裝嘗試警告資料**：列出已嘗試解除安裝 ZENworks Security Client 的使用者。
- **不安全存取點警告資料**：列出 ZENworks Security Client 所偵測到的不安全存取點。
- **不安全存取點連接警告資料**：列出 ZENworks Security Client 所連接的不安全存取點。

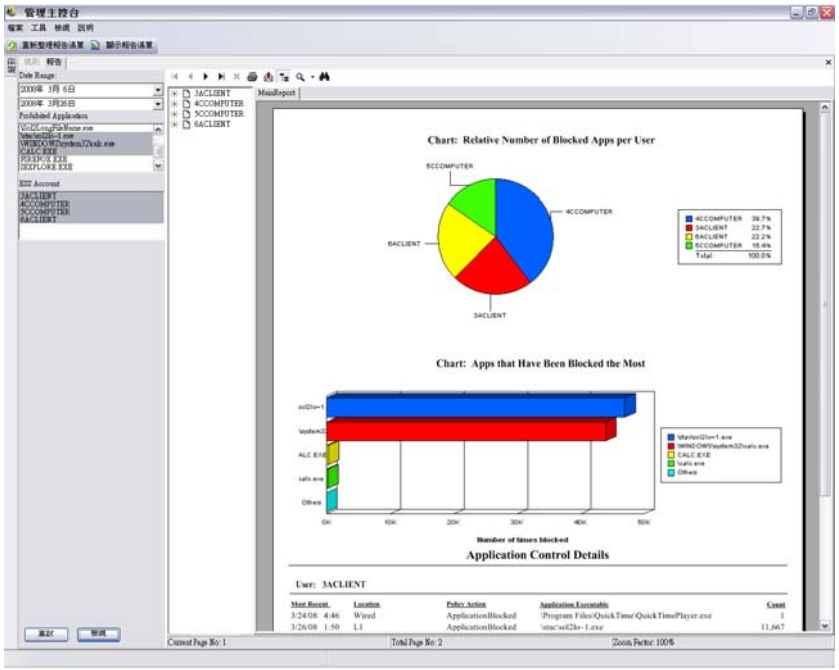
1.6.3 應用程式控制報告

在規則不允許的情況下，應用程式控制報告會顯示已封鎖之應用程式對於存取網路或執行所做的所有未授權嘗試。

下列是可用的報告：

- **應用程式控制詳細資料**：顯示日期、位置、ENworks® Security Client 所採取的動作、嘗試執行的應用程式，以及啓動應用程式的次數。日期會以 UTC 顯示。

請指定日期參數、從清單中選取應用程式名稱、使用者帳戶，然後按一下「*檢視*」以執行報告。



1.6.4 加密解決方案報告

如果端點加密已啓用，加密解決方案報告會顯示移出或移入加密資料夾的檔案。

下列是可用的報告：

- **檔案加密活動**：顯示已套用加密的檔案。

- **加密例外狀況：**顯示來自加密子系統的錯誤 (例如，因爲使用者並未具備正確金鑰，所以無法將受保護的檔案解密)。
- **檔案加密卷冊：** 顯示由 Novell 加密解決方案管理的卷冊 (例如抽取式磁碟或硬碟分割區)。

1.6.5 端點活動報告

端點活動報告可提供個別規則元件的意見反應，以及其在端點操作上的影響。

下列是可用的報告：

- **依 IP 位址的已封鎖封包：**顯示依目的地 IP 篩選的已封鎖封包。日期會以 UTC 顯示。

  請從清單中選取目的地 IP，並設定日期參數。報告會顯示日期、位置、受影響的連接埠，以及已封鎖封包的名稱。
- **依使用者的已封鎖封包：**顯示依使用者篩選的已封鎖封包。日期會以 UTC 顯示。資料基本上會與「依目的地 IP 的已封鎖封包」相同，但是依照使用者分類。
- **依使用者的網路使用率統計資料：**顯示依使用者篩選之傳送、接收或封鎖的封包，及網路錯誤。此報告需要日期範圍。日期會以 UTC 顯示。
- **依介面卡類型的網路使用率統計資料：**列出依介面卡類型篩選之傳送、接收或封鎖的封包，及網路錯誤。此報告需要日期範圍和位置。日期會以 UTC 顯示。

1.6.6 端點更新報告

端點更新報告會顯示 ZENworks Security Client 更新程序的狀態 (請參閱 「ZSC 更新」(第 60 頁))。日期會以 UTC 顯示。

下列是可用的報告：

- **Security Client 更新失敗的圖表百分比：**繪出「ZENworks Security Client 更新」失敗 (且未補救) 的百分比 。不需要任何參數，即可產生此報告。
- **Security Client 更新狀態的歷程：**顯示「ZENworks Security Client 更新」程序的狀態歷程。請選取日期範圍，並按一下「*檢視*」以執行報告。報告會顯示已登入並接收到更新程式的使用者。
- **Security Client 更新失敗的圖表類型：**顯示已失敗且未補救的「ZENworks Security Client 更新」。請選取日期範圍，並按一下「檢視」以執行報告。報告會顯示已登入，但更新安裝失敗的使用者。

1.6.7 用戶端自我防禦報告

用戶端自我防禦報告可讓您知道使用者嘗試修改或停用 ZENworks® Security Client 的時間。

下列是可用的報告：

- **ZENworks Security Client 入侵嘗試：**報告使用者進行未經授權之嘗試以修改或停用 ZENworks Security Client 的執行個體。日期會以 UTC 顯示。

  請輸入日期參數，並按一下「*檢視*」以執行報告。

1.6.8 完整性強制執行報告

完整性強制執行報告可提供防毒 / 防間諜軟體完整性結果的報告。

下列是可用的報告：

- **用戶端完整性歷程：**報告用戶端完整性檢查成功或失敗。日期會以 UTC 顯示。

  選取報告的日期範圍、完整性規則和使用者名稱。
- **依規則的未補救完整性失敗：**報告已失敗且尚未補救的完整性規則和測試。

  請選取完整性規則，然後按一下「*檢視*」以執行報告。
- **依使用者的未補救完整性失敗：**報告完整性測試失敗且尚未補救的使用者。

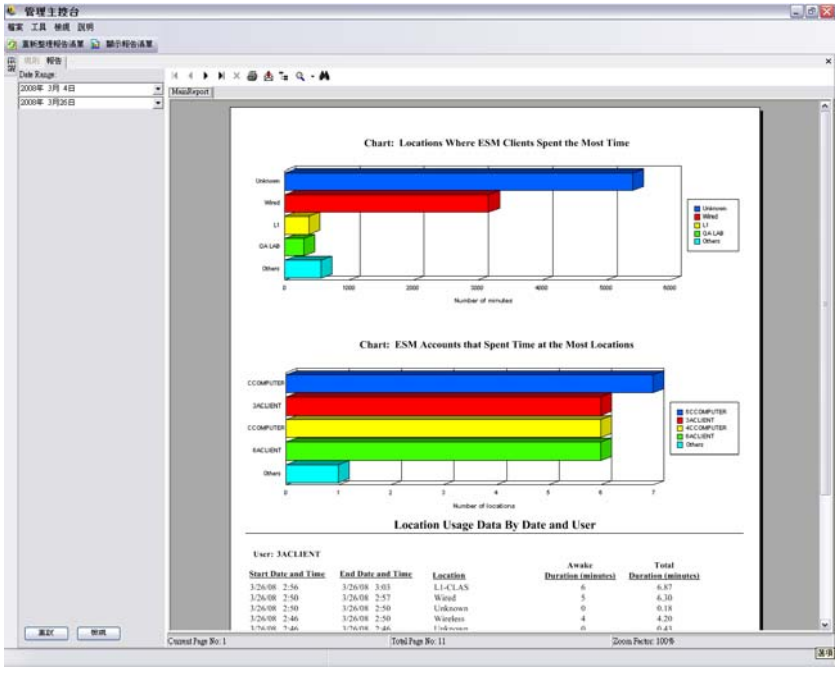
  請選取使用者名稱，然後按一下「*檢視*」以執行報告。

1.6.9 位置報告

位置報告可提供一般位置使用率的資料，例如使用者最常使用的位置。

下列是可用的報告：

依日期和使用者的位置使用率：提供從個別用戶端所收集，關於使用哪些位置及何時使用的資訊。日期會以 UTC 顯示。其中所顯示的是由使用者所使用的位置，未使用的位置則不會顯示。請選取日期範圍以產生報告。

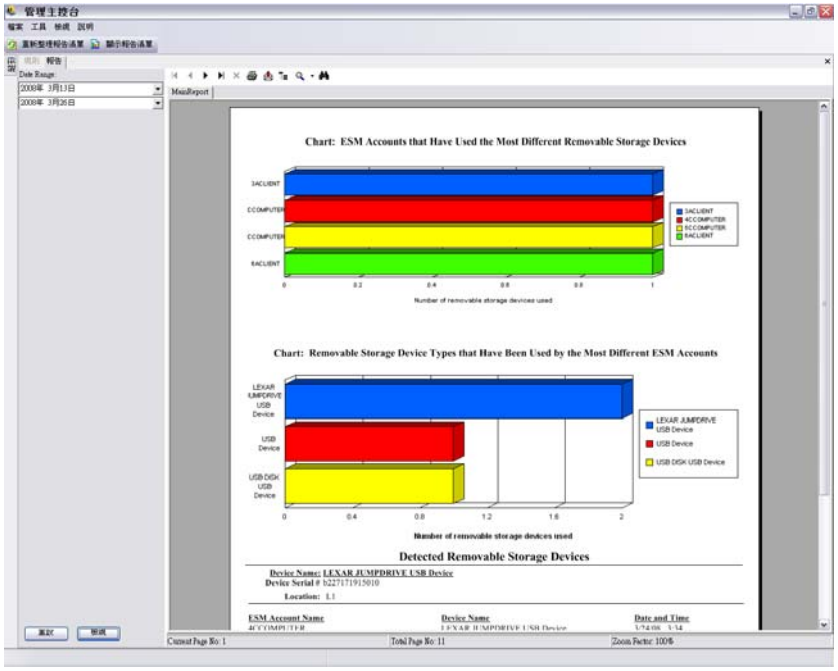


1.6.10 外傳內容規範報告

外傳內容規範報告提供關於抽取式磁碟機之使用資訊，以及識別哪些檔案已上載至這類磁碟機的資訊。

下列是可用的報告：

- **依帳戶的抽取式儲存設備活動：**顯示已將資料複製到抽取式儲存設備的帳戶。不需要任何參數，即可產生此報告。
- **依設備的抽取式儲存設備活動：**顯示已將檔案複製到其上的抽取式儲存設備。請選取日期範圍、使用者名稱和位置以產生報告。
- **依帳戶從抽取式儲存設備複製：**顯示從抽取式儲存設備複製到受管理設備的檔案。
- **偵測到的抽取式儲存設備：**顯示在端點上偵測到的抽取式儲存設備。請選取日期範圍、使用者名稱和位置以產生報告。



- **依帳戶來繪製抽取式儲存設備活動的 7 日圖表：** 顯示最近將資料複製到抽取式儲存設備的帳戶圖表。請輸入日期範圍，以產生此報告。

1.6.11 管理置換報告

管理置換報告會顯示用戶端自我防禦機制已遭管理員置換，在 ZENworks® Security Client 上授予有權限的控制之執行個體。

下列是可用的報告：

- **ZENworks Security Client 置換：**依使用者和日期顯示成功的置換嘗試。日期會以 UTC 顯示。

  請選取使用者和日期範圍，並按一下「*檢視*」以執行報告。

1.6.12 端點更新報告

端點更新報告會顯示 ZENworks® Security Client 更新程序的狀態 (請參閱 「ZSC 更新」(第 60 頁))。日期會以 UTC 顯示。

下列是可用的報告：

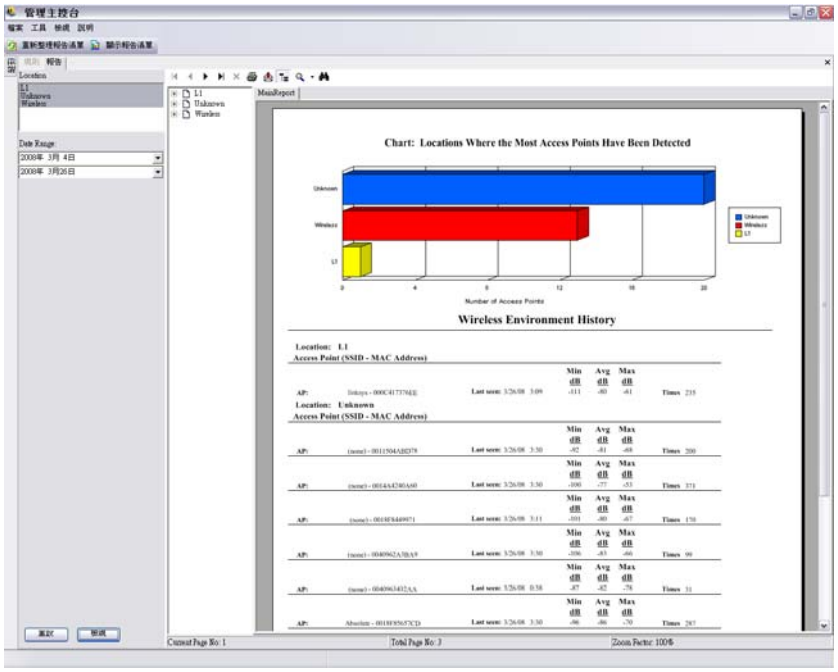
- **安全性更新失敗的圖表百分比**：繪出「ZENworks Security Client 更新」失敗且未補救的百分比 。不需要任何參數，即可產生此報告。
- **Security Client 更新狀態的歷程**：顯示「ZENworks Security Client 更新」程序的狀態歷程。請選取日期範圍，然後按一下「*檢視*」以執行報告。報告會顯示已登入並接收到更新程式的使用者。
- **Security Client 更新失敗的圖表類型**：顯示已失敗且未補救的 「ZENworks Security Client 更新」。請選取日期範圍，然後按一下「*檢視*」以執行報告。報告會顯示已登入，但更新安裝失敗的使用者。

1.6.13 無線強制執行報告

無線強制執行報告可提供端點所處 Wi-Fi 環境的相關報告。

下列是可用的報告：

- **無線連接可用性**：依規則和位置顯示可用於連接的存取點。包括通道、SSID、MAC 位址及存取點是否已加密。
- **無線連接嘗試**：提供設備嘗試連接的存取點清單 (依位置和帳戶)。
- **無線環境歷程**：提供所有偵測到的存取點調查 (無論擁有權爲何)。包括頻率、訊號強度及存取點是否已加密。日期會以 UTC 顯示。請選取想要的位置及日期範圍，以產生此報告。



1.7 使用 ZENworks 儲存設備加密解決方案

ZENworks® 儲存設備加密解決方案 (ZENworks® Storage Encryption Solution) 可爲所有行動資料提供完整且集中式的安全性管理，作法是在端點本身上主動強制執行公司的加密規則。

ZENworks 儲存設備加密解決方案可讓您：

- 在所有端點和抽取式儲存設備上，集中建立、配送、強制執行及稽核加密規則。
- 在硬碟的所有固定磁碟分割區上，將儲存至 (或複製到) 特定目錄的所有檔案加密。
- 加密所有複製到抽取式儲存設備的檔案 .
- 封鎖對檔案的未授權存取，同時在組織中任意共享檔案 .
- 透過可用的解密公用程式，與組織外部的人們共享受密碼保護的加密檔案 .
- 透過規則輕易更新、備份及復原金鑰，而不會遺失資料。

1.7.1 瞭解 ZENworks 儲存設備加密解決方案

透過資料加密安全性規則的建立和配送，即會強制執行資料加密。端點上的機密資料可儲存於加密資料夾中。使用者可以在加密資料夾外部存取和複製這項資料，並共享檔案，不過在該資料夾中，資料將維持加密。所有未經該機器授權的使用者，對於讀取資料的嘗試將不會成功。當規則啓動時，加密的「安全庇護」資料夾將會新增至端點上非系統卷冊的根目錄。

放置於隨身碟或其他抽取式媒體設備上的機密資料將會被立即加密，而且只可在相同規則群組中的機器上加以讀取。您可另行啓動共享資料夾，允許使用者透過密碼，與其規則群組外的人們共享檔案 (請參閱 「資料加密」(第 58 頁))。

1.7.2 共享加密的檔案

相同規則群組內的使用者 (已收到相同安全性規則的使用者) 將會擁有金鑰，其可用來存取存放於端點上、及移動至隨身碟和其他抽取式設備上之資料。

其他規則群組內的使用者 (已啓動加密) 將能夠利用存取密碼，存取放置於「共享檔案」資料夾中的加密檔案。這些使用者將無法讀取「共享檔案」資料夾之外的加密檔案。

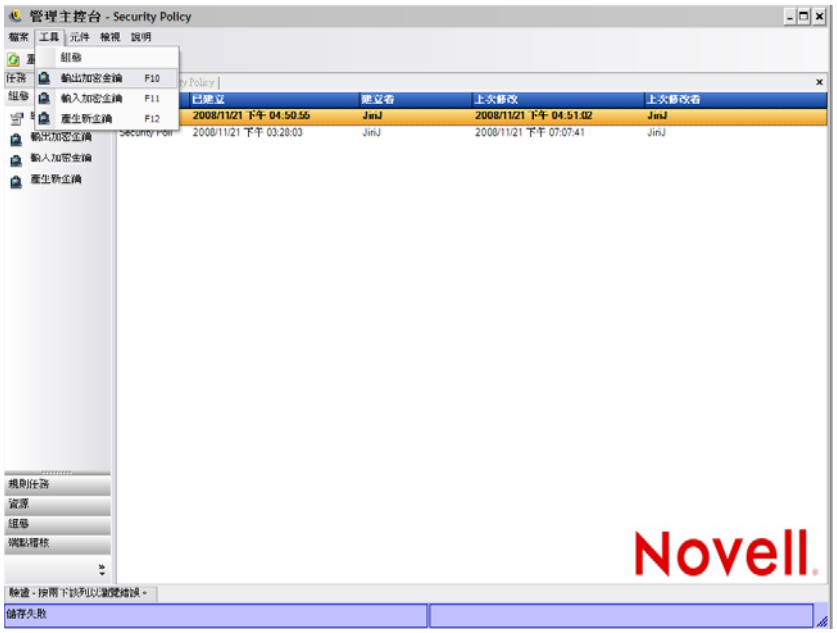
未在規則中啓用加密的使用者，以及未於電腦中安裝 ZENworks Security Client 的使用者 (例如外部承包商) 皆無法讀取「共享檔案」資料夾以外的檔案。他們需要 ZENworks® 檔案解密公用程式來讀取密碼存取的檔案。如需詳細資訊，請參閱 「使用 ZENworks 檔案解密公用程式」(第 39 頁)。

1.8 使用金鑰管理

金鑰管理允許您備份、輸入及更新加密鑰。建議您將加密鑰輸出並儲存，以確保可在系統失敗或不小心變更規則的情況下仍能對資料解密。

通用金鑰爲預設的加密鑰，可用於所有資料加密代理程式。您可以在加密鑰洩露時進行更新，或者做爲安全性預警。產生新的通用金鑰，在受管理的內容重新加密時，將導致暫時的效能衰退。

您可以透過管理主控台的「*工具*」功能表存取「加密鑰」控制。



1.8.1 輸出加密鑰

基於備份，或者爲了將金鑰傳送至其他 「管理服務」執行個體，您可將目前的加密鑰組輸出至指定的檔案位置。

1. 按一下 「*工具*」>「*輸出加密鑰*」。
2. 指定含檔案名稱的路徑，或按一下 「*瀏覽*」按鈕以瀏覽並選取檔案位置。
3. 指定密碼。沒有此密碼，金鑰便無法輸入。
4. 按一下 「*確定*」。

資料庫中的所有金鑰檔案都包含於輸出的檔案中。

1.8.2 輸入加密鑰

您可以從備份或其他 「管理服務」執行個體輸入金鑰。這允許受此 「管理服務」所管理的端點，讀取由其他 ZENworks Endpoint Security Management 安裝所保護的檔案。系統會在在輸入金鑰時忽略副本。輸入的金鑰會變成金鑰組的一部分，而且不會取代目前的通用金鑰。發行新的規則時，所有金鑰都將傳承下來。

1. 按一下 「*工具*」>「*輸入加密鑰*」。
2. 指定包含檔案位置的檔案名稱，或按一下 「*瀏覽*」按鈕來瀏覽並選取金鑰檔案。
3. 指定加密鑰的密碼。
4. 按一下 「*確定*」將金鑰輸入資料庫。

1.8.3 產生新的金鑰

1. 按一下 「*工具*」>「*產生新金鑰*」。

所有之前的金鑰都會儲存在規則中。

1.9 使用 ZENworks 檔案解密公用程式

「ZENworks® 檔案解密公用程式」可用於從加密的抽取式儲存設備上之「共享檔案」資料夾，將受保護的資料解壓縮。您可以將此簡易工具提供給協力廠商，使他們能夠在「共享檔案」資料夾中存取檔案，不過您不能將該工具置於抽取式儲存設備中。

- 「使用 檔案解密公用程式」(第 39 頁)
- 「設定檔案解密公用程式」(第 39 頁)

以下幾節中包含了更詳細的資訊：

1.9.1 使用 檔案解密公用程式

若要使用「檔案解密公用程式」：

1. 將儲存設備插入電腦上的適當連接埠。
2. 開啓檔案解密公用程式。
3. 瀏覽至儲存設備的「共享檔案」目錄，並選取想要的檔案。
4. 若要解壓縮目錄 (資料夾) 而非檔案，可以按一下「*進階設定*」按鈕並選取「*目錄*」，然後瀏覽至適當的目錄 (按一下「*基本設定*」以返回預設檢視窗)。
5. 瀏覽並選取本機上的電腦路徑以儲存這些檔案。
6. 按一下「*解壓縮*」。

可按一下「*顯示進度*」按鈕，即可監視異動。

1.9.2 設定檔案解密公用程式

您也可利用目前的金鑰組，將「檔案解密公用程式」設定爲管理員模式，並可從加密的儲存設備將所有資料解壓縮。我們不建議您使用此組態，因爲它會對於 ZENworks 儲存設備加密解決方案目前所使用的全部金鑰造成潛在的威脅；不過如果資料是無法復原的，則您可能必須使用此組態。

若要設定工具的組態：

1. 在其目前的目錄內，建立「檔案解密公用程式」的捷徑。
2. 在捷徑上按一下滑鼠右鍵，然後按一下「*內容*」。
3. 在目標名稱的結尾，以及引號之後，輸入 -k (例如："C:\Admin Tools\stdecrypt.exe" -k)。
4. 按一下「*套用*」>「*確定*」。
5. 使用捷徑開啓工具，然後按一下「*進階設定*」。
6. 按一下「*載入金鑰*」按鈕以開啓「輸入金鑰」對話方塊。
7. 瀏覽金鑰檔案，然後指定金鑰的密碼。

所有利用這些金鑰加密的檔案，現在均可解壓縮。

1.10 使用置換密碼金鑰產生器

強制執行 ZENworks® Security Client 安全性規則可能對連接性、軟體執行或抽取式儲存設備存取等造成限制，並可能對使用者的生產力造成中斷。變更位置或防火牆設定通常可以解除這些限制，並恢復已中斷的功能。不過在某些情況中，限制會在所有位置和防火牆設定中執行，或者該使用者無法變更位置或防火牆設定。

發生此情況時，在修改規則之前，目前規則中的限制可透過密碼置換來解除，以允許產能。此功能允許管理員爲指定的使用者和功能設定密碼保護的置換，以暫時允許必要的活動。

密碼置換會停用目前的安全性規則，並且在預先定義的時間內恢復預設的「全部開啓」規則。在時間限制過期之後，系統會恢復目前或更新的規則。規則的密碼是在安全性規則的「全域規則」設定中所設定的。

密碼置換會執行下列動作：

- 可置換應用程式封鎖
- 允許使用者變更位置
- 允許使用者變更防火牆設定
- 置換硬體控制 (隨身碟、CD-ROM 等)

不可將輸入規則中的密碼發給使用者。您可以使用「置換密碼金鑰產生器」來產生短期使用的金鑰。

若要產生置換金鑰：

1. 開啓「置換密碼金鑰產生器」(「*開始*」>「*程式集*」>「*Novell*>「*ESM 管理主控台*」>「*置換密碼產生器*」)。
2. 在「*管理員密碼*」欄位中指定規則密碼，並在下一個欄位中確定該密碼。
3. 指定最終使用者用來進行登入的使用者名稱。
4. 指定停用規則的期間。
5. 按一下「*產生金鑰*」按鈕來產生置換金鑰。

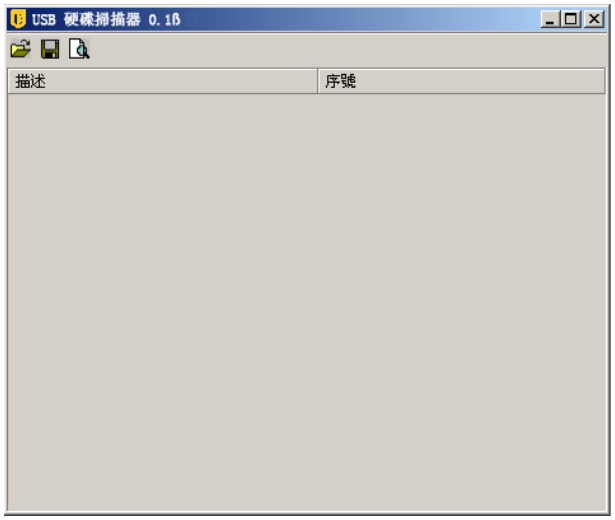
使用者可在服務台呼叫期間讀取該金鑰，或者您也可以將其複製並貼至電子郵件中。然後使用者可將金鑰輸入 ENworks Security Client 的管理視窗 (請參閱 《*ZENworks Endpoint Security Management Security Client 使用者指南*》)。此金鑰僅適用於該使用者的規則，並且只能在指定的時間內使用。金鑰一旦使用過後就不能再使用。

附註：如果使用者在密碼置換期間內登出或重新開機，密碼將會過期，且需要再發出一個新的金鑰。

如果在時間限制過期之前寫入新的規則，則必須要求使用者檢查規則更新，而不是按一下 ZENworks Security Client 關於方塊中的「*載入規則*」。

1.11 USB Drive Scanner

您可選擇使用 USB Drive Scanner 工具 (包含在安裝套件中) 產生已授權的 USB 設備清單，並將其輸入規則中。



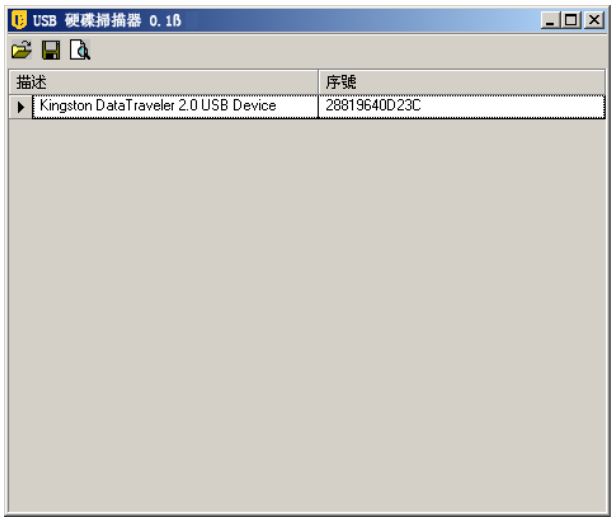
若要產生已授權的設備清單：

1 開啓 USB Drive Scanner 應用程式 .

附註：這是與「管理服務」和「管理主控台」分開的個別安裝。桌面會顯示此工具的捷徑。

2 將 USB 設備插入電腦的 USB 連接埠中。此設備必須有一個序號。

3 按一下「*掃描*」圖示 ( )。設備名稱與其序號會顯示在適當的欄位中。



4 重複步驟 步驟 2 和步驟 步驟 3，直到所有的設備都已輸入清單爲止。

5 按一下「儲存」圖示 ( )。

請參閱 「偏好的設備」(第 52 頁) 以瞭解如何將清單輸入規則中。

若要編輯已儲存的檔案，請按一下「*瀏覽*」圖示 ( ) 以開啓檔案。

建立並配送 安全性規則

2

ZENworks® Security Client 會使用安全性規則將位置安全性套用在行動使用者上。每個位置的管理員會決定網路連接埠可用性、網路應用程式可用性、檔案儲存設備存取，以及有線與 Wi-Fi 連接性。

您可以針對企業、個別使用者群組或個別使用者 / 機器建立自訂的安全性規則。安全性規則可確保完整的員工生產力並同時保護端點，或者可限制員工只能執行某些應用程式，並且只能使用已授權的硬體。

以下幾節中包含了更詳細的資訊：

- 「瀏覽管理主控台」(第 43 頁)
- 「建立安全性規則」(第 45 頁)
- 「輸入及輸出規則」(第 99 頁)

2.1 瀏覽管理主控台

若要開始建立安全性規則：

1. 在管理主控台中，按一下「*檔案*」>「*建立新規則*」。
2. 指定新規則的名稱，然後按一下「*建立*」以顯示管理主控台，其中並顯示「規則」工具列和規則索引標籤。

以下幾節將描述管理主控台的使用者介面，使您瞭解如何透過 ZENworks® Endpoint Security Management 建立並配送安全性規則。

- 「使用規則索引標籤和樹狀結構」(第 43 頁)
- 「使用規則工具列」(第 44 頁)

2.1.1 使用規則索引標籤和樹狀結構

您可以瀏覽位於「管理主控台」上方的可用索引標籤，並使用左窗格中的「*全域設定*」樹狀結構來寫入或編輯安全性規則。

可用索引標籤包括以下項目：

- **全域規則設定：**「全域規則設定」將依預設套用至整個規則中，因此並不是特定位置的設定。

  「全域規則設定」可讓您進行以下設定：

  - 規則設定
  - 無線控制
  - 通訊硬體
  - 儲存設備控制
  - USB 連接性
  - 資料加密

- ZENworks Security Client
- VPN 強制執行

- **位置：**這些規則會套用在特定類型的位置之中，無論是指定爲單一網路，或是咖啡店或機場等網路類型。
- **完整性和補救規則：**這些規則可確保基本軟體 (例如防毒軟體和間諜軟體) 在設備上的執行並維持更新。
- **規範報告：**指示是否收集此特定規則的報告資料 (包括資料類型)。
- **發行：**將完成的規則發行至個別使用者、目錄服務使用者群組和個別機器。

「規則樹」會顯示索引標籤式種類的可用子集元件。例如，「*全域規則設定*」包含「*規則設定*」、「*無線控制*」、「*通訊硬體*」和「*儲存設備控制*」的子集。只有包含在主要子集頁面的項目才是定義種類時所必須，其餘的子集都是選擇性元件。

2.1.2 使用規則工具列

規則工具列可提供六種控制。您可以在整個規則建立過程中使用「*儲存規則*」控制，但只能在「*位置*」和「*完整性和補救*」索引標籤下使用元件控制。

以下將提供工具的說明：

- **儲存 規則：**以目前的狀態儲存規則 .

  重要：當您完成每個元件子集時，我們強烈建議您按一下「*規則*」工具列上的「*儲存*」圖示。如果輸入元件中的資料不完整或不正確，將會顯示錯誤通知畫面 (請參閱「錯誤通知」(第 99 頁) 取得詳細資料)。

- **新元件：**在「位置」或「完整性」子集中建立新元件。一旦儲存規則後，就可使用新元件以建立與其他規則的關聯。
- **關聯元件：**開啓目前子集的「選取元件」畫面。可用的元件包括已包含在安裝中的任何預先定義元件，以及在其他規則中建立的所有元件。

重要：變更關聯元件將會影響該元件的其他執行個體。

例如，您可以建立一個稱爲「Work」的單一「位置」元件，它可定義當端點進入該環境時所套用的公司網路環境和安全性設定。此元件現在可套用至所有安全性規則。您可以在一個規則中變更元件的環境或安全性設定更新，如此就可以在與其相關聯的所有規則中更新相同的元件。

使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

- **移除元件：**移除規則中的元件。不過您仍可在此規則或其他規則中建立元件的關聯性。
- **重新整理規則清單：**重新整理規則清單。
- **報告清單：**顯示報告的清單。

2.2 建立安全性規則

1. 在管理主控台中，按一下「*檔案*」>「*建立新規則*」。
2. 指定新規則的名稱，然後按一下「*建立*」以顯示管理主控台，其中並顯示「規則」工具列和規則索引標籤。
3. 使用以下各節的資訊進行規則設定：

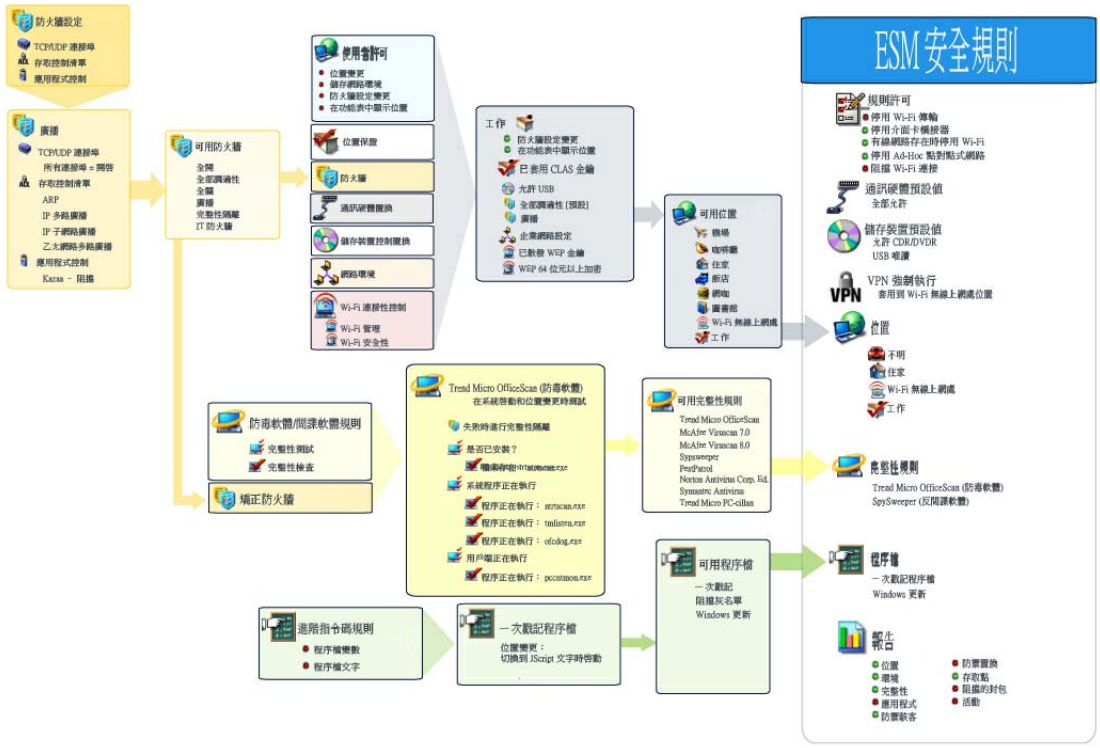
- 「全域規則設定」(第 46 頁)
- 「位置」(第 65 頁)
- 「完整性和補救規則」(第 88 頁)
- 「規範報告」(第 95 頁)

- 「發行」(第 97 頁)
- 「錯誤通知」(第 99 頁)
- 「顯示使用率」(第 99 頁)

安全性規則的建立方法：定義所有的全域設定 (預設行爲)，然後爲該規則建立並聯結，如位置、防火牆和完整性規則等現有元件，最後建立規則的規範報告。

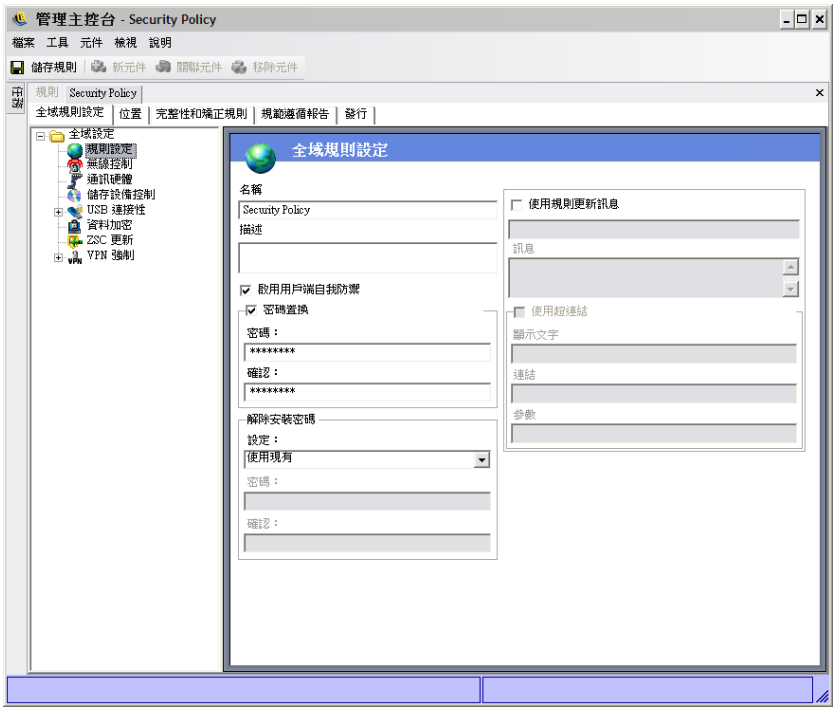
您可以在虛擬的規則中或建立與其他規則的關聯來建立元件。假設在前幾個規則中，您將會爲企業建立所有的唯一位置、防火牆設定和完整性規則。這些元件將會儲存在 「管理服務」的資料庫中以供其他規則於稍後使用。

以下圖表顯示每個層次的元件，並顯示從選定項目所產生的規則。



2.2.1 全域規則設定

全域規則設定會套用爲規則的基本預設。若要存取此控制，請移至 「管理主控台」，然後按一下 「*全域規則設定*」索引標籤。



以下幾節將詳細描述您可以在全域進行的設定。

- 「規則設定」(第 47 頁)
- 「無線控制」(第 48 頁)
- 「通訊硬體」(第 49 頁)
- 「儲存設備控制」(第 50 頁)
- 「USB 連接性」(第 53 頁)
- 「資料加密」(第 58 頁)
- 「ZSC 更新」(第 60 頁)
- 「VPN 強制執行」(第 61 頁)
- 「自訂使用者訊息」(第 64 頁)
- 「超連結」(第 64 頁)

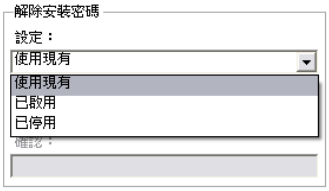
規則設定

主義的全域設定包括：

- **名稱和描述：**規則名稱是在規則建立程序開始時指定的。您可以編輯名稱或提供規則的描述。
- **啓用用戶端自我防禦：**規則可啓用或停用用戶端自我防禦。核取此方塊可啓用「用戶端自我防禦」。取消選取此方塊將會停用所有使用此規則的端點用戶端自我防禦。
- **密碼置換：**此功能可讓管理員設定密碼置換，能夠在指定的期間內暫時停用規則。選取「*密碼置換*」方塊並在提供的欄位中指定密碼。在確認欄位中再次輸入密碼。在「置換密碼產生器」中輸入此密碼以產生此規則的密碼金鑰。如需詳細資訊，請參閱 「使用置換密碼金鑰產生器」(第 40 頁)。

警告：我們強烈建議您不要將此密碼提供給使用者。您可以使用「置換密碼產生器」產生可供他們使用的暫時金鑰。

- **解除安裝密碼：**我們建議您透過解除安裝密碼來安裝 ZENworks* Security Client，以避免使用者將軟體解除安裝。此密碼通常會在安裝時進行設定，不過您可以透過規則來更新、啓用或停用密碼。



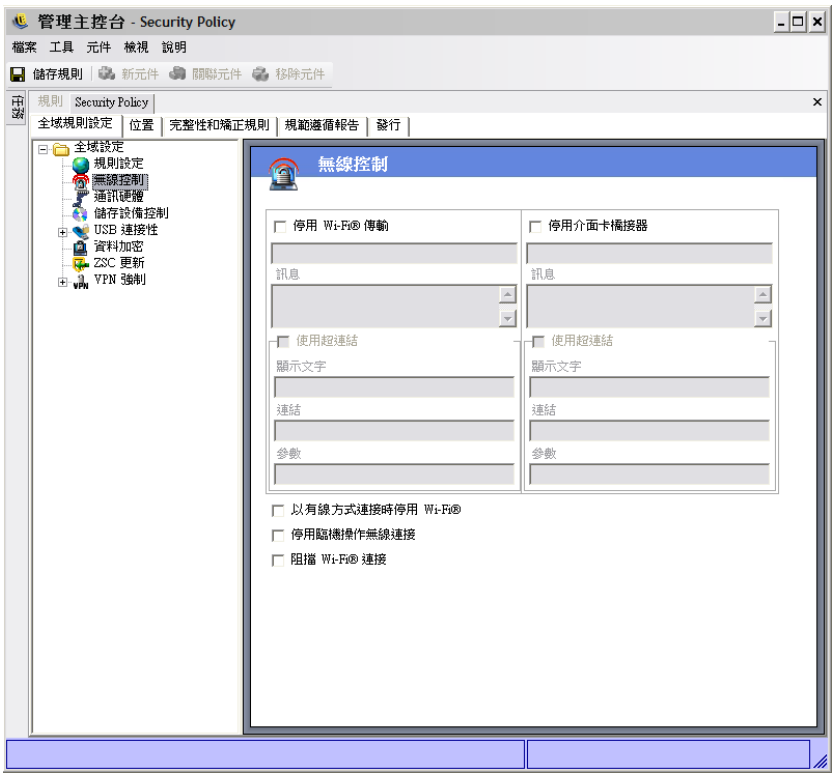
您可以在下拉式清單中選取以下其中一個設定：

- **使用現有設定：**此爲預設值。這會保留目前的密碼。
- **已啓用：**啓用或變更解除安裝密碼。指定新密碼並進行確認。
- **停用：**停用解除安裝密碼需求。

- **使用規則更新訊息：**您可以在更新規則時顯示自訂使用者訊息。按一下核取方塊，然後在提供的欄位中指定訊息資訊。
- **使用超連結：**訊息中可包含指向附加資訊、公司規則等超連結 (請參閱 「超連結」(第 64 頁))。

無線控制

「無線控制」會可全域設定介面卡連接性參數以保護端點和網路。若要存取此控制，請按一下「*全域規則設定*」索引標籤，並按一下左邊規則樹中的「*無線控制*」圖示。



無線控制設定包含以下項目：

- **停用 Wi-Fi 傳輸**：在全域中停用所有 Wi-Fi 介面卡，包含內建 Wi-Fi radio 的完全靜音。

  您可以選擇在使用者嘗試啓用 Wi-Fi 連接時顯示自訂使用者訊息和超連結。如需相關資訊，請參閱「自訂使用者訊息」(第 64 頁)。
- **停用介面卡橋接**：在全域中停用包含在 Windows* XP 中的網路橋接功能，它可讓使用者橋接多個介面卡，並做爲網路上的中樞器。

  您可以選擇在使用者嘗試使用 Wi-Fi 連接時顯示自訂使用者訊息和超連結。如需相關資訊，請參閱「自訂使用者訊息」(第 64 頁)。
- **進行有線連接時停用 Wi-Fi**：當使用者進行有線連接時 (透過 NIC 的 LAN) 在全域中停用所有 Wi-Fi 介面卡。
- **停用臨機操作網路**：在全域中停用會在網路上強制執行 Wi-Fi 連接的特別連接 (例如透過存取點)，並限制所有此類型的對等式網路。
- **封鎖 Wi-Fi 連接**：在全域中封鎖 Wi-Fi 連接但不執行 Wi-Fi radio 的靜音。當您要停用 Wi-Fi 連接但仍須使用存取點進行位置偵測時，可使用此設定。如需相關資訊，請參閱「位置」(第 65 頁)。

通訊硬體

按位置的通訊硬體設定可控制要在此網路環境中允許哪個硬體類型的連接。

附註：您可以透過「*全域規則設定*」標籤設定全域的通訊硬體控制，或者透過「*位置*」索引標籤進行個別位置的設定。

若要設定全域的通訊硬體控制，請按一下「*全域規則設定*」索引標籤，在樹狀結構中展開「*全域設定*」，然後按一下「*通訊硬體*」。

若要設定個別位置的通訊硬體控制，請按一下「*位置*」索引標籤，在樹狀結構中展開想要的位置，然後按一下「*通訊硬體*」。請參閱 「通訊硬體」(第 68 頁) 以瞭解如何進行個別位置的通訊硬體設定。

爲每個列出的通訊硬體設備選擇要啓用或停用全域設定：

- **1394 (FireWire)**：控制端點上的 FireWire* 存取連接埠。
- **IrDA**：控制端點上的紅外線存取連接埠。
- **藍牙**：控制端點上的藍牙* 存取連接埠。
- **序列 / 平行**：控制端點上的序列和平行連接埠存取。

儲存設備控制

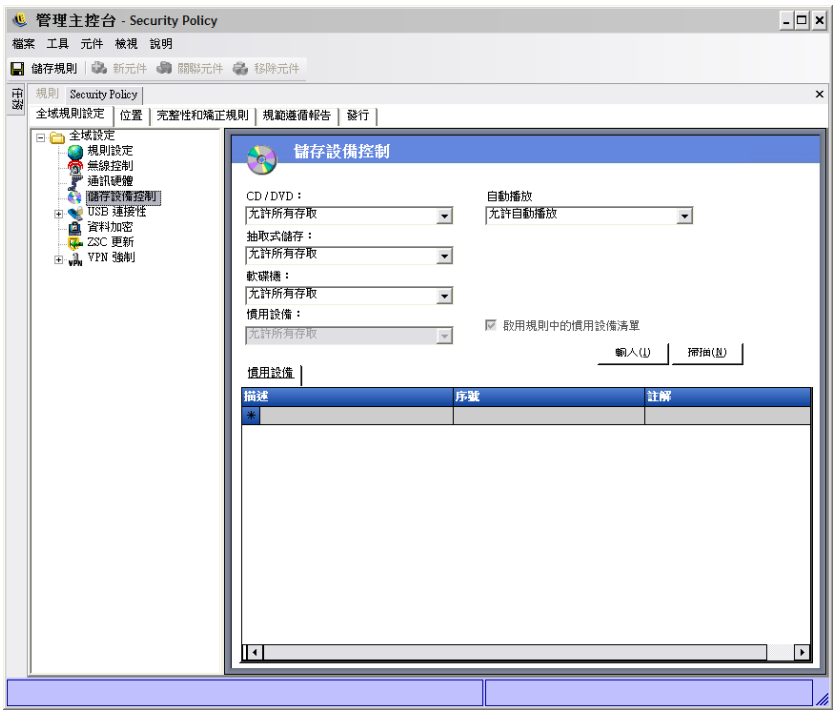
儲存設備控制可進行規則的預設儲存設備設定。這包括可指定是否允許外部儲存設備讀取或寫入檔案、在唯讀狀態中操作，或完全停用。這些設備在停用時將無法從端點取回任何資料，而硬碟和所有的網路磁碟機仍可進行存取與操作。

當啓動「儲存加密解決方案」時將不允許「ZENworks Endpoint Security Management 儲存設備控制」。

附註：您可以透過「*全域規則設定*」標籤設定全域的儲存設備控制，或者透過「*位置*」索引標籤進行個別位置的設定。

若要設定全域的儲存設備控制，請按一下「*全域規則設定*」索引標籤，在樹狀結構中展開「*全域設定*」，然後按一下「*儲存設備控制*」。

若要設定個別位置的儲存設備控制，請按一下「*位置*」索引標籤，在樹狀結構中展開想要的位置，然後按一下「*儲存設備控制*」。如需詳細資訊，請參閱 「通訊硬體」(第 68 頁)。



儲存設備控制可區分爲以下種類：

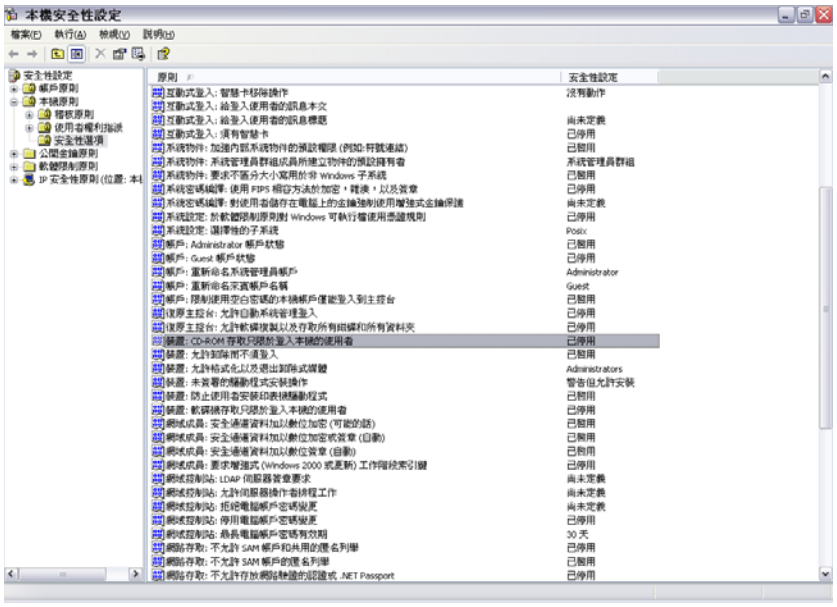
- **CD/DVD**：控制列於 Windows 裝置管理員 *DVD/CD-ROM 光碟機* 中的所有設備。
- **抽取式儲存設備**：控制 Windows 裝置管理員的*磁碟機*中報告爲抽取式儲存設備的所有設備。
- **軟碟機**：控制列於 Windows 裝置管理員*軟碟*中的所有設備。
- **偏好的設備**：僅允許列於「儲存設備控制」視窗中的抽取式儲存設備。不允許所有報告爲抽取式儲存設備的其他設備。

一律允許固定儲存設備 (硬碟) 和網路磁碟機 (如可用時)。

若要設定儲存設備的規則預設值，請在下拉式清單中選取兩種類型的全域設定：

- **啓用**：依照預設值，允許使用此設備類型。
- **停用**：不允許使用此設備類型。當使用者嘗試在已定義的儲存設備中存取檔案時，他們會從作業系統收到存取動作失敗的錯誤訊息，或者從嘗試存取本地儲存設備的應用程式收到該訊息。
- **唯讀**： 設備類型設爲「唯讀」。當使用者嘗試寫入此設備時，他們會從作業系統收到寫入動作失敗的錯誤訊息，或者從嘗試存取本地儲存設備的應用程式收到該訊息。

附註：如果您要在一組端點上停用 CD-ROM 或軟碟，或者將其設爲「唯讀」，您必須將兩種「本地安全性設定」(透過目錄服務群組規則物件傳送)「*設備：限制僅本地登入的使用者可存取 CD-ROM*」和「*設備：限制僅本地登入的使用者可存取軟碟*」設爲停用。若要進行驗證，請開啓群組規則物件，或開啓機器上的「管理工具」。檢視「本地安全性設定 - 安全性選項」，並確認兩種設備都已停用。預設值爲停用。



以下幾節中包含了更詳細的資訊：

- 「偏好的設備」(第 52 頁)
- 「輸入裝置清單」(第 52 頁)

偏好的設備

當您在位置上使用全域設定時，可以將偏好的抽取式儲存設備選擇性地新增至僅允許授權設備存取的清單中。新增至清單中的設備必須具有序號。

若要列出偏好的設備：

1 將設備插入機器 (已安裝 「管理主控台」) 的 USB 連接埠中。

2 待設備就緒之後，按一下 「*掃描*」按鈕。如果設備具有序號，其 「描述」和 「序號」將會顯示在清單中。

3 在下拉式清單中選取設定 (「*全域抽取式設備*」設定將不會套用在此規則中)：

- **已啓用**：偏好清單中的設備將允許完整的讀取 / 寫入功能，而其他的 USB 和外部儲存設備都會停用。
- **唯讀**： 偏好清單中的設備將允許唯讀功能，而其他的 USB 和外部儲存設備都會停用 。

您可以爲此規則所允許的每個設備重複這些步驟。所有設備都會套用相同的設定。

附註：以位置爲基礎的 「儲存設備控制」設定將會置換全域設定。例如，您可能會在工作位置上允許所有的外部儲存裝置，而在其他位置上僅允許全域預設值，以限制使用者只能存取偏好清單上的裝置。

輸入裝置清單

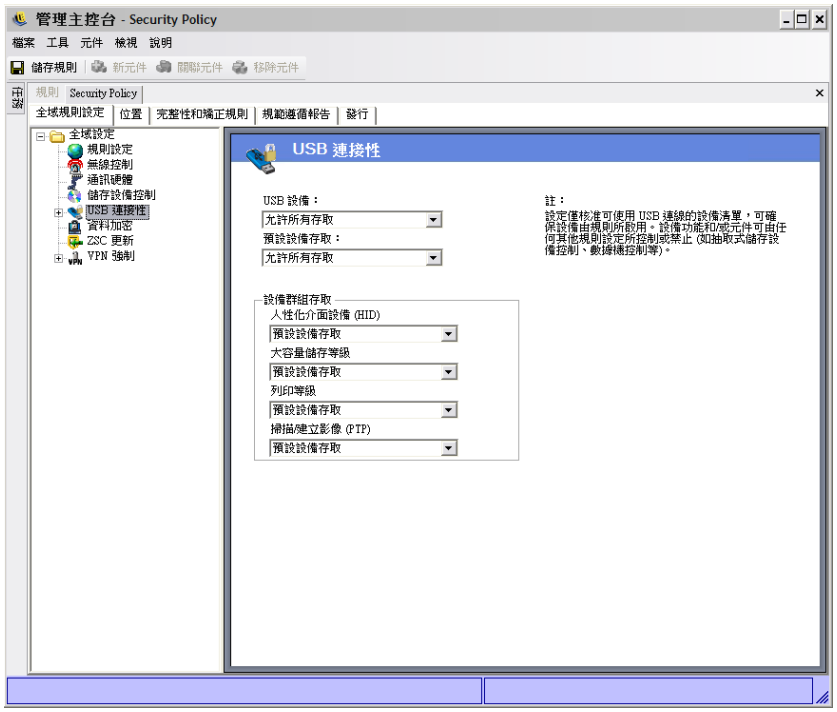
Novell USB Drive Scanner 應用程式會產生一個包含序號的設備清單 (「USB Drive Scanner」(第 41 頁))。若要輸入此清單，請按一下 「*輸入*」並瀏覽清單。該清單將會填入 「*敘述*」和 「*序號*」欄位。

USB 連接性

規則可允許或拒絕透過 USB BUS 連接的所有設備。您可以將這些設備從 USB 設備庫存報告掃描至規則中，或者掃描目前連接至機器的所有設備。您可以依照製造商、產品名稱、序號、類型等來篩選這些設備。管理員可以基於支援的目的，依照製造商類型 (例如允許所有 HP 設備) 或產品類型 (允許所有 USB 人體介面設備 [滑鼠和鍵盤]) 來設定規則以接受一組設備。此外，您可以允許個別的設備以避免將不支援的設備導入網路中 (例如，不允許本印表機以外的所有印表機)。

若要存取此控制，請按一下「*全域規則設定*」索引標籤，並按一下左邊規則樹中的「*USB 連接性*」。

圖 2-1 *「USB 連接性」頁面。*



評估是否允許存取的第一個條件，就是此匯流排是否在使用中。這是由「*USB 設備*」設定所決定。如果這個設定已設爲「*停用所有存取*」，則會停用此設備並停止評估。如果此設定已設爲「*允許所有存取*」，則用戶端會繼續評估程序，並尋找篩選相符的項目。針對某個位置設定「*USB 設備*」值的時候，此欄位就和 ZENworks 管理主控台的許多其他欄位一樣，也可以設爲「*套用全域設定*」，這時就會改用此欄位的全域值。

用戶端根據位置和全域設定收集從規則套用的篩選器。接著用戶端會根據存取條件把篩選器歸類爲下列群組：

- **永遠阻擋：**永遠阻擋此設備。您無法覆寫此設定。
- **永遠允許：**永遠允許存取，除非此設備符合「*永遠阻擋*」篩選器。
- **阻擋：**阻擋存取，除非此設備符合「*永遠允許*」篩選器。
- **允許：**允許存取，除非此設備符合「*永遠阻擋*」或「*阻擋*」篩選器。
- **預設設備存取：**如果找不到其他相符項目，則讓此設備的存取層級與「*預設設備存取*」相同。

評估設備時所用的條件就是上述各群組，且依據以上的順序 (先是 「*永遠阻擋*」群組，接著是 「*永遠允許*」，依此類推)。如果某設備符合某群組的至少一個篩選器，則會將此設備設定爲該存取層級，並且停止評估。如果根據所有篩選器評估後都找不到此設備的相符項目，則會套用 「*預設設備存取*」層級。

在 「*設備群組存取*」區域中設定的 「設備存取」，也會隨著用於該位置的其他所有篩選器一起被當作評估標準。作法是趁著把規則發佈到用戶端時，針對每個群組產生相符的篩選器。這些篩選器如下：

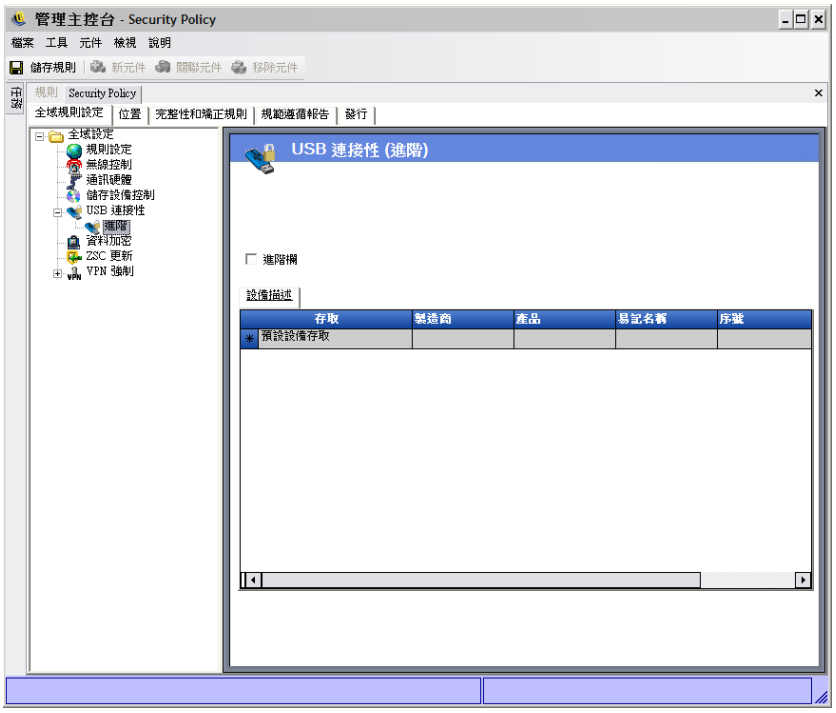
設備群組存取：	**篩選器：**
人體介面設備 (HID)	「設備類別」等於 3。
大量儲存類別	「設備類別」等於 8。
列印類別	「設備類別」等於 7。
掃描 / 影像處理 (PTP)	「設備類別」等於 6。

進階

在大部分情況下，「USB 連接性」頁面列出的四個設備群組 (人體介面設備、大量儲存類別、列印類別和掃描 / 影像處理) 就足以允許或拒絕他人存取大部分的 USB 設備。如果您的設備不屬於以上任何群組，則可在 「USB 連接性進階設定」頁面中設定組態。即使某些設備因爲 「USB 連接性」頁面的設定而拒絕他人存取，您也可以使用 「進階設定」頁面的設定把這些設備列入存取白名單。

如果要存取 「USB 連接性進階設定」選項，請按一下 「*全域設定*」樹中 「*USB 連接性*」旁的加號，然後按一下 「*進階設定*」。您可以利用 「USB 設備稽核」報告取得也許能用在 「USB 連接性控制進階設定」頁面的所有資訊。

圖 2-2 *「USB 連接性進階設定」頁面。*



預設欄列出如下：

- **存取：**請把滑鼠游標移到「*預設設備存取*」上方，然後指定存取層級：
  - **永遠阻擋：**永遠阻擋此設備。您無法覆寫此設定。
  - **永遠允許：**永遠允許存取，除非此設備符合「*永遠阻擋*」篩選器。
  - **阻擋：**阻擋存取，除非此設備符合「*永遠允許*」篩選器。
  - **允許：**允許存取，除非此設備符合「*永遠阻擋*」或「*阻擋*」篩選器。
  - **預設設備存取：**如果找不到其他相符項目，則讓此設備的存取層級與「*預設設備存取*」相同。
- **製造廠商：**請按一下「*製造商*」欄，然後輸入您要加入篩選器的製造商名稱 (例如 Canon)。
- **產品：** 請按一下「*產品*」欄，然後輸入您要加入篩選器的產品名稱。
- **易記名稱：**請按一下「*易記名稱*」欄，然後輸入您要加入篩選器的易記名稱。
- **序號：**請按一下「*序號*」欄，然後輸入您要加入篩選器的設備序號。
- **註解：**請按一下「*註解*」欄，然後輸入您要加入篩選器的註解 (例如 Canon)。

您可按一下「*進階欄*」方塊新增下列欄：*USB 版本*、*設備類別*、*設備子類別*、*設備協定*、*廠商 ID*、*產品 ID*、*BCD 設備*、*O/S 設備 ID* 和 *O/S 設備類別*。

設備會提供一組屬性給作業系統，接著由用戶端把這些屬性比對到篩選器要求的欄位。篩選器的所有欄位都必須與設備提供的屬性相符，才能比對成功。如果此設備並未提供篩選器要求的屬性或欄位，該篩選器就會比對失敗。

例如，假設某設備提供下列屬性：製造商：Acme、類別：8、序號：「1234」。

「類別 == 8」篩選器能與此設備相符。「產品 == "Acme"」篩選器則不相符，因爲此設備並未向作業系統提供「產品」屬性。

下列欄位是相符的子字串：製造商、產品與易記名稱。所有其他欄位都完全相符。

順便一提，依規格，如果要把 USB 序號 (SN) 欄位視爲唯一，則除了 SN 以外還必須連帶指定「USB 版本」、「廠商 ID」、「生產 ID」和「BCD 設備」等欄位。

目前 USB 版本的有效十進位值爲 512 - USB 2.0、272 - USB 1.1、256 - USB 1.0。

以下幾節中包含了更詳細的資訊：

- 「手動新增設備」(第 55 頁)
- 「依產品類型將設備列入白名單或黑名單：」(第 56 頁)

手動新增設備

以下的方法可讓您填入清單，以允許或拒絕透過 USB 連接這些設備：

若要手動新增設備：

1 將設備插入機器 (已安裝「管理主控台」) 的 USB 連接埠中。

2 待設備就緒之後，按一下「*掃描*」按鈕。如果設備具有序號，其「描述」和「序號」將會顯示在清單中。

3 在下拉式清單中選取設定 (「*全域抽取式設備*」設定將不會套用在此規則中)：

- **啓用：**偏好清單中的設備將允許完整的讀取 / 寫入功能，而其他的 USB 和外部儲存設備都會停用
- **唯讀：** 偏好清單中的設備將允許唯讀功能，而其他的 USB 和外部儲存設備都會停用

您可以爲要在此規則中允許的每個設備重複這些步驟。所有設備都會套用相同的設定。

依產品類型將設備列入白名單或黑名單：

下一節說明如何依 USB 設備的產品類型將 USB 設備列入白名單或黑名單。

附註：下列程序是範例，用於說明您如何找到您的 USB 抽取式儲存設備的產品類型。程序是否作用視您的設備製造商提供的資訊而定。您可以利用「USB 設備稽核」報告取得也許能用在「USB 連接性控制進階設定」頁面的所有資訊。

若要決定 USB 抽取式儲存設備的產品類型：

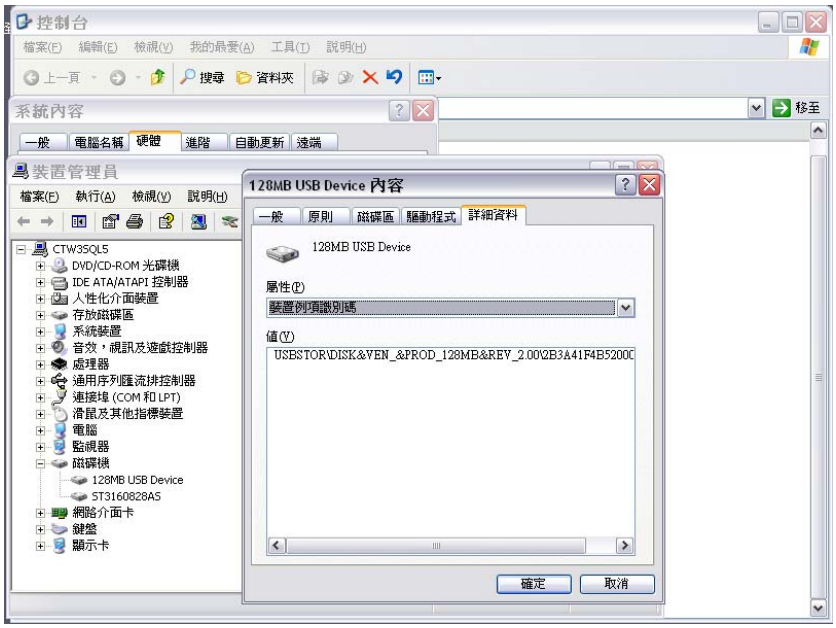
1 在 Microsoft Windows Computer Management 主控台中，按一下「*裝置管理員*」。

2 按一下「*磁碟機*」旁的 + 號以展開樹狀結構。

3 在 USB 設備上按一下滑鼠右鍵，然後按一下「*內容*」以顯示設備的「內容」對話方塊。

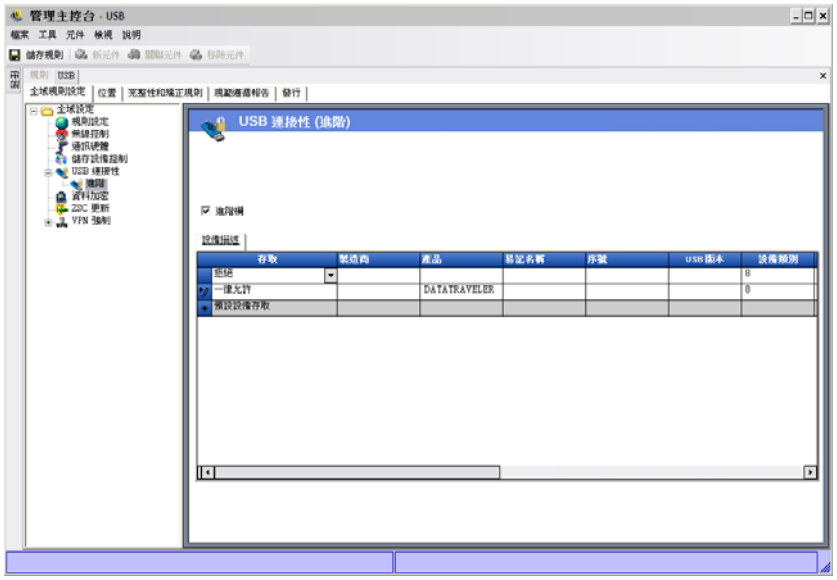
4 按一下「*詳細資料*」索引標籤，然後從下拉式清單中選取「*設備執行個體 ID*」。

產品類型列在「設備執行個體 ID」中的「產品 (&P)」後。在下列範例中，DATATRAVELER 是產品類型。



將 USB 設備列入白名單：將「USB 連接性頁面」上的設定保留在預設值。在「進階」頁面上，建立兩列。在第一列中，在「*存取*」欄中指定「*拒絕*」，在「*設備類別*」欄中指定 8 (如果無法使用「*設備類別*」，請選取「*進階欄*」核取方塊)。在第二列中，在「*存取*」欄中指定「*永遠允許*」，在「*產品*」欄中指定產品類型 (在此範例爲 DATATRAVELER)，在「*設備類別*」欄中指定 8。

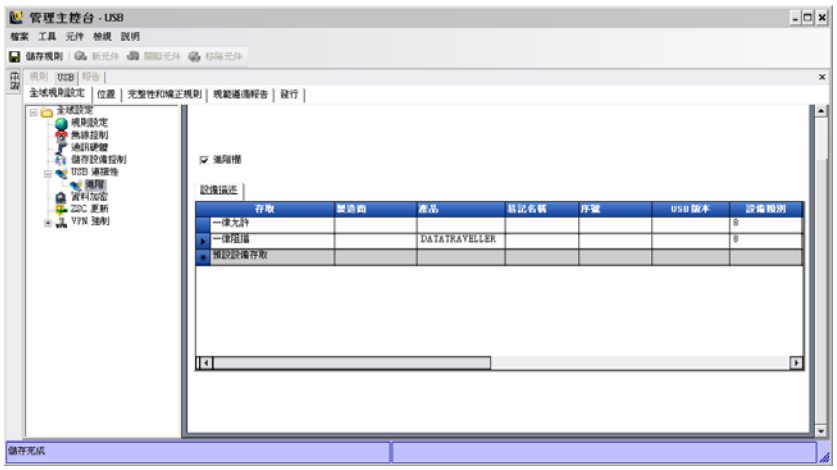
USB 連接性 (進階) 頁面看起來應該如以下範例所示：



DATATRAVELER USB 裝置現在已列入白名單中，表示 ZENworks Endpoint Security Management 允許其存取，但拒絕所有其他 USB 抽取式儲存設備的存取。

將 USB 設備列入黑名單：將「USB 連接性頁面」上的設定保留在預設值。在「進階」頁面上，建立兩列。在第一列中，於「*存取*」欄中指定「*永遠允許*」，在「*設備類別*」欄中指定 8 (如果「*設備類別*」無法使用，請選取「*進階欄*」核取方塊)。在第二列中，於「*存取*」欄中指定「*永遠封鎖*」，在「*產品*」欄中指定產品類型 (在此範例爲 DATATRAVELER)，在「*設備類別*」欄中指定 8。

USB 連接性 (進階) 頁面看起來應該如以下範例所示：



DATATRAVELER USB 裝置現在已列入黑名單中，表示 ZENworks Endpoint Security Management 拒絕其存取，但允許所有其他 USB 抽取式儲存設備的存取。

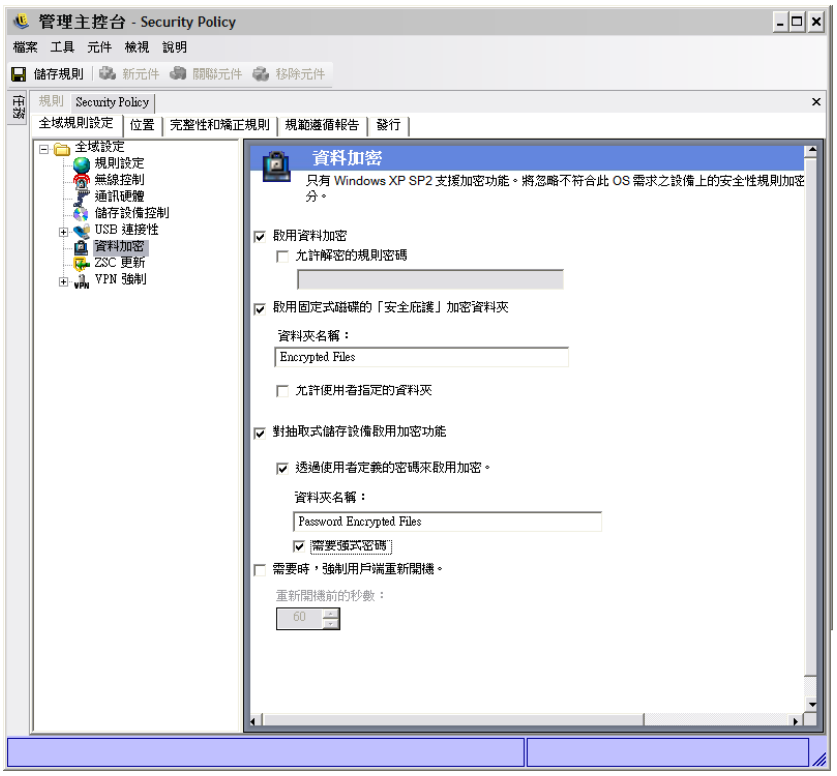
資料加密

「資料加密」會決定是否要在端點上強制執行檔案加密，以及要使用哪種加密類型。您可以將資料加密以允許檔案共享 (含密碼保護)，或者在執行 「ZENworks 儲存加密解決方案」的電腦上將加密的資料設爲唯讀。

附註：只有 Windows XP SP2 支援加密。在不符合此作業系統需求的設備上忽略安全性規則的加密部分。

當啓動 「ZENworks 儲存加密解決方案」時，將不允許 「ZENworks Endpoint Security Management 儲存設備控制」。

若要存取此控制，請按一下 「*全域規則設定*」索引標籤，並按一下左邊規則樹中的 「*資料加密*」。



若要啓用個別控制，請按一下 「*啓用資料加密*」核取方塊。

附註：系統會將加密鑰配送給從 「規則配送服務」接收規則的所有機器 (無論是否已啓用資料加密)。不過此控制會指示 ZENworks Security Client 啓動其加密驅動程式，因此使用者可讀取傳送給他們的檔案，而不需要檔案加密公用程式。請參閱 「使用 ZENworks 檔案解密公用程式」(第 39 頁)，以取得詳細資料。

決定此規則所允許的加密層級：

- **允許加密的規則密碼：**指定一個密碼，要求所有使用者在解密儲存於「安全庇護」資料夾的任何加密檔案之前，都必須使用此規則來輸入該密碼。

  此爲選擇性的設定。若保留空白時將不需要密碼。

- **爲固定磁碟 (非系統卷冊) 啓用「安全庇護」加密資料夾：**在端點上非系統卷冊的根目錄產生一個名爲「加密保護檔案」的資料夾。位於此資料夾中的所有檔案都會由 ZENworks Security Client 進行加密與管理。此資料夾中的所資料都會自動加密，而且只有在此機器上獲得授權的使用者才能存取這些資料。

  如果您想要變更資料夾名稱，請按一下「*資料夾名稱*」欄位，選取目前的文字，然後指定想要的名稱。

  - **加密使用者的「我的文件」資料夾：**選取此方塊，將使用者的「我的文件」資料夾設爲加密資料夾 (這是「安全庇護」以外的資料夾)。這只適用於本機的「我的文件」資料夾。
  - **允許使用者指定的資料夾 (非系統卷冊)：**選取此方塊以允許使用者在電腦中選取要加密的資料夾。這只適用於本機資料夾，您無法加密抽取式儲存裝置或網路磁碟機。

  警告：在停用資料加密之前，請確定使用者已取出所有儲存在這些資料夾中的資料，並將其儲存在其他位置中。

- **啓用抽取式儲存設備的加密：**從受規則保護的端點寫入抽取式儲存設備的所有資料都會進行加密。在機器上使用此規則的使用者都可以讀取資料，因此可以在規則群組內經由抽取式儲存設備進行檔案共享。規則群組外的使用者將無法在磁碟機中讀取加密的檔案，並且只能使用提供的密碼存取「共享檔案」資料夾 (如已啓用) 中的檔案。

  - **透過使用者定義密碼來啓用加密：**此設定可讓使用者將檔案儲存在抽取式儲存設備的「共享檔案」資料夾中 (當套用此設定時，系統會自動產生該資料夾)。使用者將檔案新增至此資料夾時可指定一個密碼，讓目前規則群組之外的使用者可使用該密碼將檔案取出。

    如果您想要變更資料夾名稱，請按一下「*資料夾名稱*」欄位，選取目前的文字，然後指定想要的名稱。

  - **需要強式密碼：**此設定會強制使用者爲「共享檔案資料夾」設定強式密碼。強式密碼必須包含下列項目：
    - 七個以上的字元
    - 下列四類字元的其中一個字元：
      - A 到 Z 的大寫字母
      - a 到 z 的小寫字母
      - 0 到 9 的數字
      - 至少一個特殊字元 ~!@#$%^&*()+{}[]:;<>?,./

    例如：y9G@wb?

  警告：在停用資料加密之前，請確定使用者已取出所有儲存在抽取式儲存設備中的資料，並將其儲存在其他位置中。

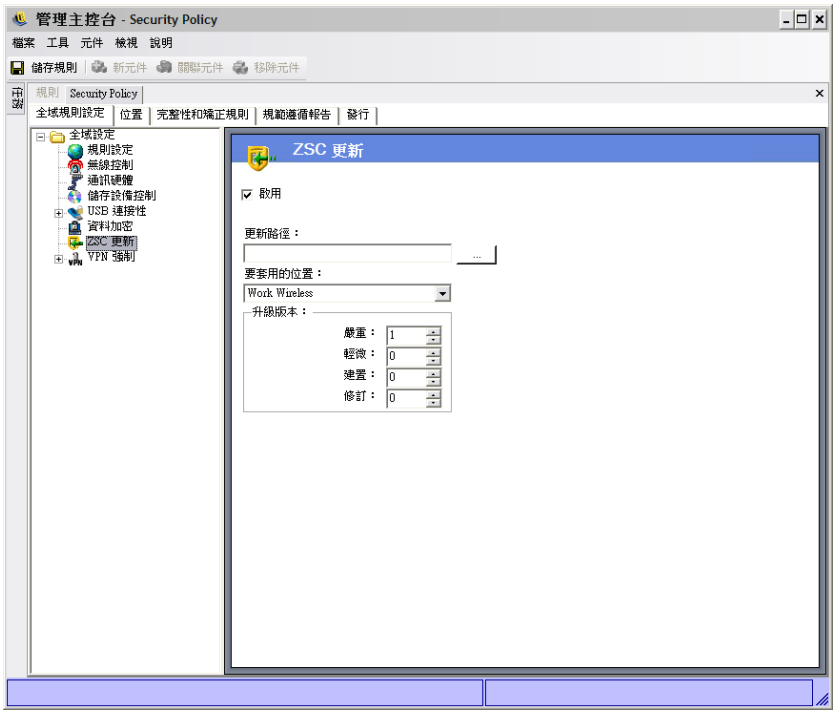
- **視需要強制用戶端重新開機：**當您將加密新增至規則中時將無法啓用，直到端點重新開機爲止。此設定會強制執行必要的重新開機，並顯示一個倒數計時器，警告使用者機器將在指定的秒數之後重新開機。使用者可在機器重新開機前的這段時間內儲存其工作。

第一次於規則中啓動加密時需要重新開機，啓動「安全庇護」或抽取式儲存加密時必須再次重新開機 (如果不是和加密同時啓動)。例如第一次套用加密規則時需要重新開機兩次：第一次負責啓始化驅動程式，第二次則對安全庇護進行加密。如果在套用規則後選取其他的安全庇護，則只要重新開機一次就能讓安全庇護套用規則。

ZSC 更新

您可以定期進行 ZENworks Security Client 更新，以使用修補程式來修復 ZENworks Security Client 中的任何小瑕疵。「ZENworks Security Client 更新」可讓管理員不需再透過 MSI 將新的安裝程式配送給所有的端點，而是在網路上建立專門區域，將更新修補程式配送給與該網路環境相關聯的最終使用者。

若要存取此控制，請按一下「*全域規則設定*」索引標籤，並按一下左邊規則樹中的「*ZSC 更新*」。



若要將這些修補程式更輕鬆且更安全地配送至所有 ZENworks Security Client 使用者：

1. 勾選「*啓用*」以啓動畫面和規則。
2. 指定 ZENworks Security Client 尋找更新程式的位置。

   基於下一步驟中的建議，我們建議您使用與企業環境 (例如「工作」位置) 相關聯的位置。
3. 指定已儲存修補程式的 URI。

   您必須將其指向修補檔案，例如 ZENworks Security Client 的 setup.exe 檔案，或者是從 .exe 建立的 MSI 檔案。基於安全性考量，我們建議您將這些檔案儲存在公司防火牆內的安全伺服器中。
4. 在提供的欄位中指定此檔案的版本資訊。

您可以在安裝 ZENworks Security Client 後，開啓「關於」對話方塊取得版本資訊 (請參閱《*ZENworks Endpoint Security Management 安裝指南*》以取得詳細資料)。STEngine.exe 的版本號碼就是您將在欄位中輸入的版本號碼。

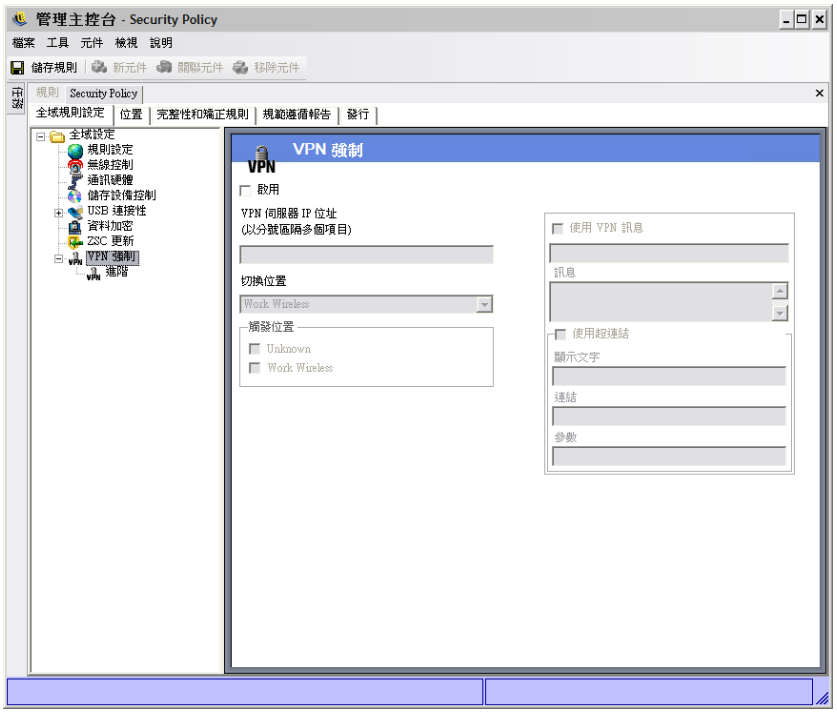
每次當使用者進入指定的位置時，ZENworks Security Client 將會檢查 URL 以尋找符合該版本資訊的更新程式。ZENworks Security Client 將會下載並安裝可用的更新程式。

VPN 強制執行

此規則將強制執行 SSL 或以用戶端爲基礎的 VPN (虛擬私有網路)。此規則通常會套用在無線上網熱點中，它可讓使用者連接至公用網路，同時該規則將嘗試進行 VPN 連接，然後將使用者切換至已定義的位置和防火牆設定。所有的參數都是由管理員決定。所有的參數都會置換現有的規則設定。使用者必須先連接網路才能啓動「VPN 強制執行」元件。

附註：只有安裝 ZENworks Endpoint Security Management 才提供此功能，且無法用於 UWS 安全性規則。

若要存取此控制，請按一下「*全域規則設定*」索引標籤，並按一下左邊規則樹中的「*VPN 強制執行*」。



若要使用 VPN 強制執行規則，必須至少有兩個位置存在。

若要將 VPN 強制執行新增至新的或現有的安全性規則：

1. 選取「*啓用*」以啓動畫面和規則。
2. 在提供的欄位中指定 VPN 伺服器的 IP 位址。在指定多個位址時，請使用分號以分隔每個位址 (範例：10.64.123.5;66.744.82.36)。
3. 從下拉式清單中選取「*切換至位置*」。

這是在啓動 VPN 時 ZENworks Security Client 要切換到的位置。您可以在此位置中加上一些限制，並只預設單一限制性防火牆設定。

若您需要嚴格的 VPN 強制執行，我們建議您使用「*全部關閉*」防火牆設定，關閉所有的 TCP/UDP 連接埠。此設定將可防止任何未獲授權的網路連接，而 VPN IP 位址可做爲 VPN 伺服器的 ACL 並允許網路連接性。

4 選取將套用 VPN 強制執行規則的「觸發位置」。若要進行嚴格的 VPN 強制執行，您必須在此規則中使用預設的「不明」位置。在經過網路驗證之後，VPN 規則將會啓用並切換至指定的「切換至位置」

附註：在經過網路驗證之後，系統會在連接 VPN 之前進行位置切換。

5 輸入當 VPN 驗證網路時顯示的自訂使用者訊息。對於非用戶端的 VPN 來說，這應該已經足夠。

對連接用戶端的 VPN 來說，將包含一個指向 VPN 用戶端的超連結。

範例：C:\Program Files\Cisco Systems\VPN Client\ipsecdialer.exe

此連結將啓動應用程式，但使用者仍必須登入。您可以在「*參數*」欄位中輸入切換，或建立並指向一個批次檔案，而不是用戶端可執行檔。

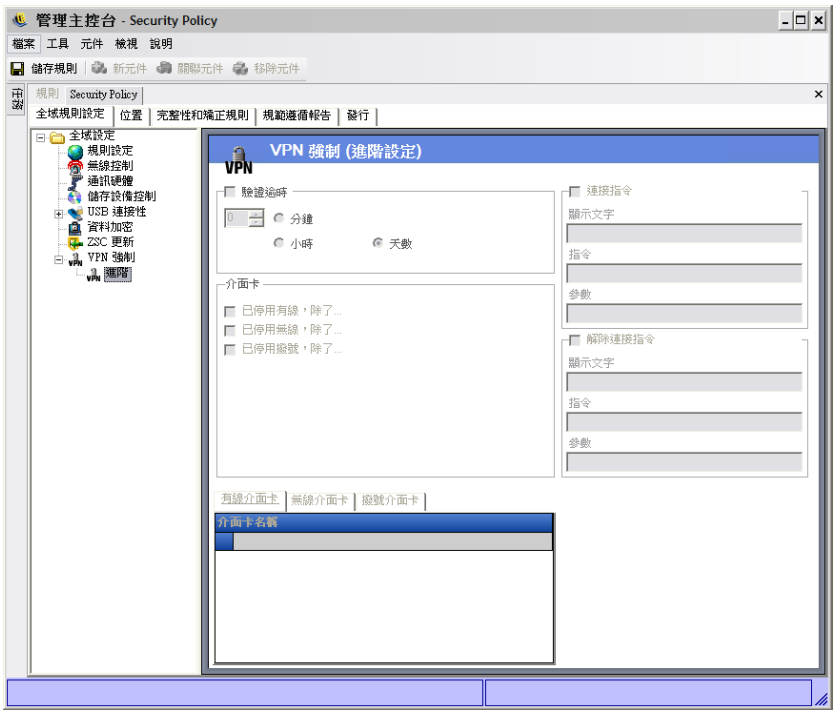
附註：可產生虛擬介面卡的 VPN 用戶端 (例如 Cisco Systems* VPN Client 4.0) 將會顯示「規則已更新」的訊息。規則實際上並未更新，ZENworks Security Client 只是將虛擬介面卡與目前規則中的任何介面卡限制進行比對。

上述標準「VPN 強制執行」設定會將 VPN 連接性列爲選項。無論使用者是否啓動 VPN 都可連接至目前的網路。如需要更嚴格的強制執行，請參閱「進階 VPN 設定」。

進階 VPN 設定

進階 VPN 控制可用來設定「驗證逾時」以防止 VPN 失敗、以用戶端爲基礎的 VPN 連接指令，以及使用介面卡控制以控制允許 VPN 存取的介面卡。

若要存取此控制，請按一下「*全域規則設定*」索引標籤，並按一下「*VPN 強制執行*」旁邊的 + 號，然後按一下左邊規則樹中的「*進階*」。



您可以設定以下的進階 VPN 強制執行設定：

驗證逾時：管理員可將端點置於安全的防火牆設定中 (「*切換至位置」的防火牆設定*)，以確保 VPN 連接性不會出現任何失敗。「*驗證逾時*」是 ZENworks Security Client 取得 VPN 伺服器驗證所等待的時間量。您必須將此參數設爲 1 分鐘以上，以允許在速度較慢的連接上進行驗證。

連接 / 切斷連接指令：當使用驗證計時器時，「*連接*」和「*切斷連接*」指令會控制以用戶端爲基礎的 VPN 啓用。在「*參數*」欄位中指定 VPN 用戶端的位置和必要的切換。「切斷連接」是選擇性的指令，可提供給 VPN 用戶端要求使用者在登出網路之前先切斷連接。

附註：可產生虛擬介面卡的 VPN 用戶端 (例如 Cisco Systems VPN Client 4.0) 將會顯示 「規則已更新」的訊息，並暫時從目前的位置上切換至別處。規則實際上並未更新，ZENworks Security Client 只是將虛擬介面卡與目前規則中的任何介面卡限制進行比對。當您在執行此類型的 VPN 用戶端時，請不要使用 「切斷連接」指令超連結。

介面卡：這是 VPN 強制執行所特有的迷你介面卡規則。

如果選取一種介面卡時 (將其變更爲已啓用、排除)，這些介面卡 (尤其是 「無線」介面卡類型) 都可連接至 VPN。

排除清單中的介面卡將無法連接 VPN，而該類型的其他介面卡都可進行連接。

如果未選取介面卡 (「已停用」、「排除」)，則只有在排除清單中輸入的介面卡才可連接 VPN。系統將拒絕其他的連接。

例如，與 VPN 不相容的介面卡，或者 IT 部門不支援的介面卡都可以使用此控制。

此規則將會置換 「切換位置」的介面卡規則集。

自訂使用者訊息

當使用者遭遇規則所強制執行的限制時，自訂使用者訊息可讓 ZENworks Endpoint Security Management 管理員建立訊息以直接回答與安全性規則有關的問題。自訂使用者訊息也可提供使用者特定的指示。您可以在規則的各種元件中使用使用者訊息控制。

若要建立自訂使用者訊息：

1. 指定訊息的標題。這將會顯示在訊息方塊的標題列上。
2. 指定訊息。訊息長度限制在 1,000 個字元內。
3. 如需插入超連結，請選取「*顯示超連結*」方塊並指定必要的資訊。

附註：在共享元件中變更訊息或超連結將會變更該元件的其他執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

超連結

管理員可在自訂訊息中加入超連結以說明安全性規則，或提供軟體更新的連結以維護完整性規範。超連結可以在多個規則元件中使用。您可以建立 VPN 超連結以指向 VPN 用戶端的可執行檔，或者指向可執行並將使用者完整登入 VPN 的批次檔 (請參閱 「VPN 強制執行」(第 61 頁) 以取得詳細資料)。

若要建立超連結：

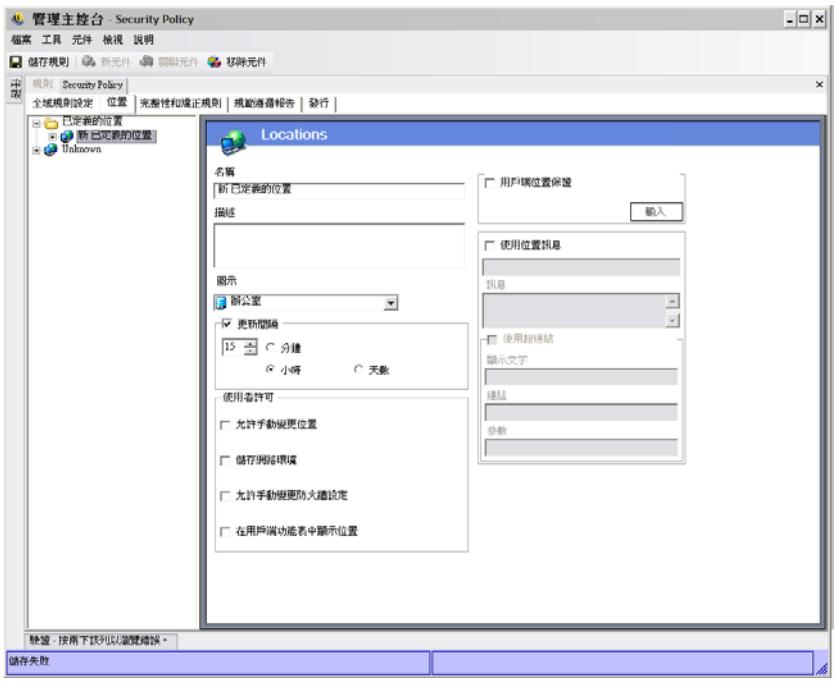
1. 指定連結的名稱。這是顯示在訊息下方的名稱。這也是「進階 VPN」超連結的必要名稱。
2. 指定超連結。
3. 指定該連結的任何切換或其他參數。

附註：在共享元件中變更訊息或超連結將會變更該元件的其他執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

2.2.2 位置

「位置」是指定給網路環境的規則群組。這些環境可以在規則中設定 (請參閱 「網路環境」(第 81 頁))，或者由獲得授權的使用者進行設定。每個位置都會獲得唯一的安全性設定，可在較不友善的網路環境中拒絕某些對於網路和硬體的存取，並且在受信任的環境中允許較大量的存取。

若要存取「位置」控制，請按一下「*位置*」索引標籤。



以下幾節中包含了更詳細的資訊：

- 「關於「位置」」(第 66 頁)
- 「通訊硬體」(第 68 頁)
- 「儲存設備控制」(第 69 頁)
- 「防火牆設定」(第 71 頁)
- 「網路環境」(第 81 頁)
- 「USB 連接性」(第 82 頁)
- 「Wi-Fi 管理」(第 83 頁)
- 「Wi-Fi 安全性」(第 87 頁)

關於「位置」

您可以設定以下的位置類型：

不明位置：所有規則都有預設的「不明」位置。當使用者離開已知的網路環境時，ZENworks Security Client 會將使用者切換至該位置。「不明」位置對於每個規則來說都是唯一的，且不能做爲共用元件。您無法設定或儲存此位置的「網路環境」。

若要存取「不明位置」控制，請按一下「*位置*」索引標籤，並按一下左邊規則樹中的「*不明*」位置。

定義的位置：您可以在規則中建立定義的位置，或者建立與現有位置 (爲其他規則所建立的位置) 的關聯。

若要建立新位置：

1 按一下「*定義的位置*」，然後按一下工具列上的「*新元件*」按鈕。

2 爲位置命名並進行描述 .

3 定義位置設定：

圖示： 選取一個位置圖示，以提供使用者視覺提示來識別目前的位置。位置圖示會顯示在通知區域的工作列上。使用下拉式清單來檢視並選取可用的位置圖示。

更新間隔：進行設定以決定 ZENworks Security Client 在進入此位置時檢查規則更新的頻率。您可以設定頻率的分鐘、小時和天數。當取消核取此參數時，表示 ZENworks Security Client 將不會在此位置上檢查更新。

使用者許可：指定使用者名稱：

- **允許手動位置變更：**允許使用者變更爲此位置 (或變更此位置)。您必須將此許可授予不受管理的位置 (例如，無線上網熱點、機場、飯店等)。在已知網路參數的受控制環境中可停用此許可。當停用此許可時使用者將無法在任何位置上進行切換；相反的，ZENworks Security Client 將依照在此位置上指定的網路環境參數。
- **儲存網路環境：**這可讓使用者將網路環境儲存至此位置，並可在使用者返回時允許自動切換至位置上。我們建議您在使用者必須切換到的任何位置上使用此設定。您可以爲單一位置儲存多個網路環境。例如，如果定義爲「機場」的位置是目前規則的一部分，使用者所拜訪的每個機場都可儲存爲此位置的網路環境。如此一來，行動使用者可回到儲存的機場環境，ZENworks Security Client 也會自動切換至「機場」位置，並套用定義的安全性設定。當然，使用者也可變更位置而不儲存環境。
- **允許手動防火牆設定變更：**允許使用者變更防火牆設定。
- **在用戶端功能表中顯示位置：**允許在用戶端功能表中顯示位置。如果未選取該選項，則不會顯示位置。

用戶端位置保證：由於用來判定位置的網路環境資訊很容易造假，使端點遭受潛在的侵入風險，因此您可以選擇透過「用戶端位置保證服務」(CLAS) 來對位置進行密碼驗證。本服務只有在由企業完整且單獨地控制之網路環境中時才能穩定可靠。將「用戶端位置保證」新增至位置，表示端點可能位在網路防火牆之後且受到保護，因此可對此位置設定較寬鬆的防火牆設定及許可。

ZENworks Security Client 會使用一個固定、企業設定的連接埠，將驗證要求傳送至 Client Location Assurance Service。Client Location Assurance Service 可解密封包並回應驗證要求，證明其具有符合公用金鑰的私密金鑰。任務列圖示將會包含一個核取記號，表示使用者位於正確的位置中。

除非 ZENworks Security Client 偵測到 CLAS 伺服器，否則不會切換位置。如果未偵測到 CLAS 伺服器，即使所有其他的網路參數都符合，ZENworks Security Client 仍會留在「不明」位置上以保護端點。

若要啓用該位置的 CLAS，請選取「*用戶端位置保證*」核取方塊，按一下「*輸入*」，然後瀏覽並選取檔案。當成功輸入金鑰時，將會顯示「已設定」的字樣。

「不明」位置上不提供此選項。

使用位置訊息：當 ZENworks Security Client 切換至此位置時，允許顯示選擇性的自訂使用者訊息。此訊息可提供最終使用者所需的指示、此位置下的規則限制相關詳細資料，或者包含更多資訊的超連結。

4 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

若要建立與現有位置的關聯：

1 按一下「*定義的位置*」，然後按一下工具列上的「*關聯元件*」按鈕。

2 從清單中選取所需位置。

3 依需要編輯設定。

附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

您必須在規則中定義多個定義的位置 (除了簡易的「工作」和「不明」位置以外的位置)，當使用者連接至企業防火牆以外的地方時，可提供其不同的安全性許可。指定易記的位置名稱 (例如咖啡店、機場、家裡等)，並透過位置的任務列提供視覺提示，可協助使用者輕鬆切換至每個網路環境所需的適當安全性設定。

通訊硬體

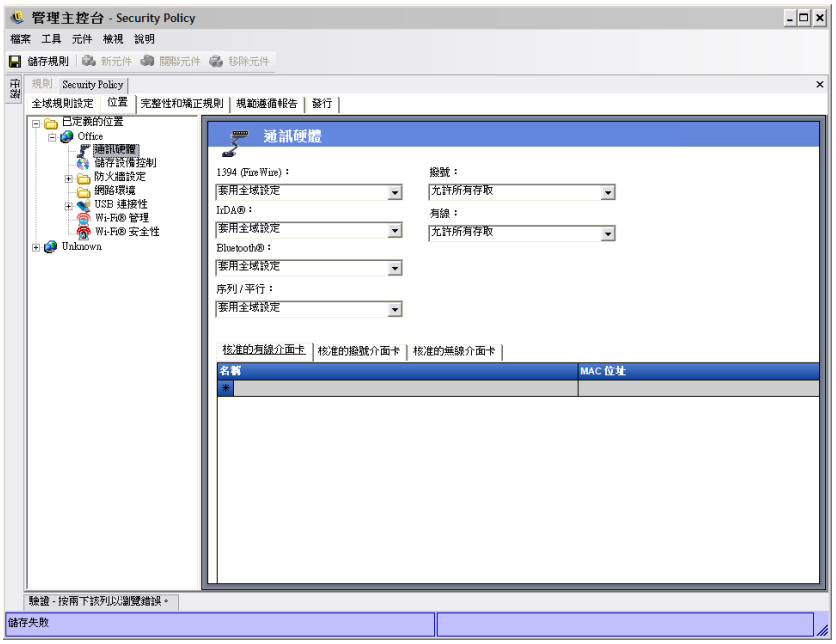
按位置的通訊硬體設定可控制要在此網路環境中允許哪個硬體類型的連接。

附註：您可以透過「*全域規則設定*」標籤設定全域的通訊硬體控制，或者透過「*位置*」索引標籤進行個別位置的設定。

若要設定個別位置的通訊硬體控制，請按一下「*位置*」索引標籤，在樹狀結構中展開想要的位置，然後按一下「*通訊硬體*」。

或

若要設定全域的通訊硬體控制，請按一下「*全域規則設定*」索引標籤，在樹狀結構中展開「*全域設定*」，然後按一下「*通訊硬體*」。如需詳細資訊，請參閱 「通訊硬體」(第 49 頁)。



爲每個列出的通訊硬體設備選擇要啓用、停用或套用全域設定：

- **1394 (FireWire)**：控制端點上的 FireWire* 存取連接埠。
- **IrDA**：控制端點上的紅外線存取連接埠。
- **藍牙**：控制端點上的藍牙 * 存取連接埠。

- **序列 / 平行：**控制端點上的序列和平行連接埠存取。
- **撥接：**依位置控制數據機連接性。當您透過 「*全域規則設定*」以全域爲基礎設定通訊硬體設定時，將無法使用此選項。
- **有線：**依位置控制 LAN 網路卡連接性。當您透過 「*全域規則設定*」以全域爲基礎設定通訊硬體設定時，將無法使用此選項。

啓用可進行通訊連接埠的完整存取。

「停用」將拒絕所有通訊連接埠的存取。

附註：您可以在全域中控制 Wi-Fi 介面卡，或使用 「Wi-Fi 安全性控制」在本地停用。您可以使用允許的無線介面卡清單按廠牌指定介面卡。

允許的撥接介面卡清單：ZENworks Security Client 可封鎖所有的連接，但可允許指定之撥接介面卡 (數據機) 進行連接。例如，管理員可建置一個規則，僅允許使用特定廠牌或類型數據機。這將可減少因員工使用不受支援硬體所耗費的成本。

允許的無線介面卡清單：ZENworks Security Client 可封鎖所有的連接，但可允許指定之無線介面卡進行連接。例如，管理員可建置一個規則，僅允許使用特定廠牌或類型的無線介面卡。這將可減少因員工使用不受支援硬體所耗費的服務成本，並且可更佳支援並強制執行以 IEEE 標準爲基礎的安全性計劃，以及 LEAP、PEAP、WPA、TKIP 等。

使用 AdapterAware 功能：

當您將網路設備安裝在系統時，ZENworks Security Client 會接收通知，並判定該設備是否獲得授權。如果設備未獲授權，解決方案將會停用設備驅動程式，使該新設備無法使用，並將此情況通知使用者。

附註：當未獲授權的新介面卡 (撥接或無線) 第一次將驅動程式安裝在端點上時 (透過 PCMCIA 或 USB)，該介面卡在系統重新開機前都會在 Windows 裝置管理員中顯示爲啓用 (雖然所有的網路連接都會被阻擋)。

指定每個允許的介面卡名稱。您可以輸入部分介面卡名稱。介面卡名稱限制在 50 個字元內，並區分大小寫。Windows 2000 作業系統需要此設備名稱以提供此功能。如果未輸入介面卡，則系統將會允許所有同類型的介面卡。如果只輸入一個介面卡，則此位置上將只會允許單一介面卡。

附註：如果端點所在位置只將存取點的 SSID 定義爲網路識別，則 ZENworks Security Client 會在停用未獲授權介面卡之前先切換至該位置。若發生此情況，您必須使用密碼置換以提供手動的位置切換。

儲存設備控制

儲存設備控制可設定規則的預設儲存設備設定，其中所有的外部檔案儲存設備都可讀取或寫入檔案並在唯讀狀態中運作，或者處於完全停用的狀態。這些設備在停用時將無法從端點取回任何資料，而硬碟和所有的網路磁碟機仍可進行存取與操作。

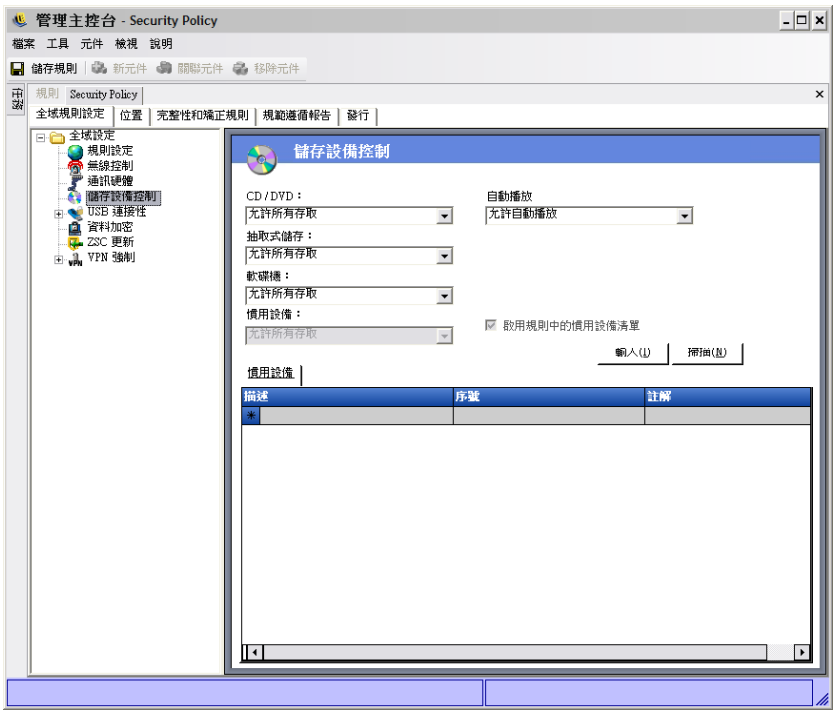
當啓動 「ZENworks 儲存加密解決方案」時，將不允許 「ZENworks Endpoint Security Management 儲存設備控制」。

附註：您可以透過「*全域規則設定*」標籤設定全域的儲存設備控制，或者透過「*位置*」索引標籤進行個別位置的設定。

若要設定個別位置的儲存設備控制，請按一下「*位置*」索引標籤，在樹狀結構中展開想要的位置，然後按一下「*儲存設備控制*」。

或

若要設定全域的儲存設備控制，請按一下「*全域規則設定*」索引標籤，在樹狀結構中展開「*全域設定*」，然後按一下「*儲存設備控制*」。如需詳細資訊，請參閱 「儲存設備控制」(第 50 頁)。



儲存設備控制可區分爲以下種類：

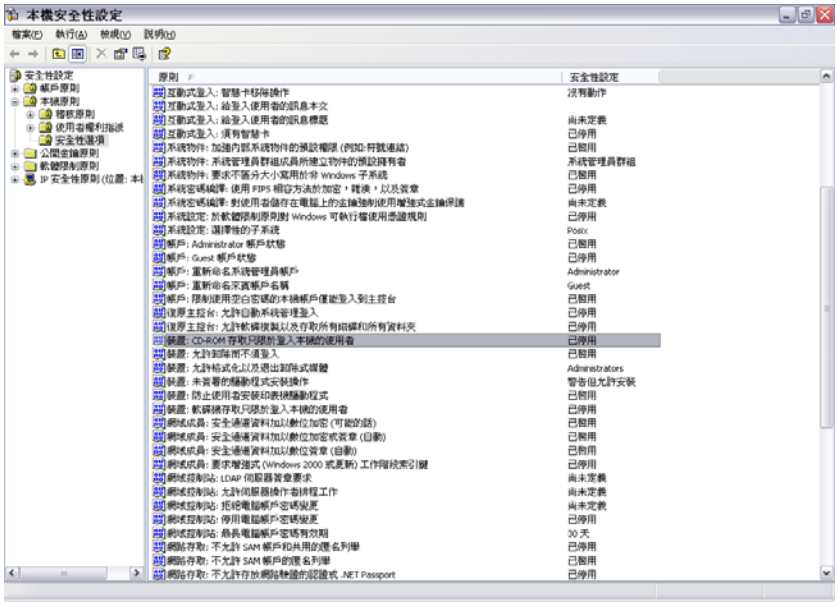
- **CD/DVD：**控制列於 Windows 裝置管理員 *DVD/CD-ROM 光碟機* 中的所有設備。
- **抽取式儲存設備：**控制 Windows 裝置管理員的*磁碟機*中報告爲抽取式儲存設備的所有設備。
- **軟碟機：**控制列於 Windows 裝置管理員*軟碟*中的所有設備。

一律允許固定儲存設備 (硬碟) 和網路磁碟機 (如可用時)。

若要設定儲存設備的規則預設值，請在下拉式清單中選取兩種類型的全域設定：

- **啓用：**依照預設值，允許使用此設備類型。
- **停用：**不允許使用此設備類型。當使用者嘗試在已定義的儲存設備中存取檔案時，他們會從作業系統收到存取動作失敗的錯誤訊息，或者從嘗試存取本地儲存設備的應用程式收到該訊息。
- **唯讀：** 設備類型設爲「唯讀」。當使用者嘗試寫入此設備時，他們會從作業系統收到寫入動作失敗的錯誤訊息，或者從嘗試存取本地儲存設備的應用程式收到該訊息。

附註：如果您要在一組端點上停用 CD-ROM 或軟碟，或者將其設爲「唯讀」，您必須將兩種「本地安全性設定」(透過目錄服務群組規則物件傳送)「*設備：限制僅本地登入的使用者可存取 CD-ROM*」和「*設備：限制僅本地登入的使用者可存取軟碟*」設爲停用。若要進行驗證，請開啓群組規則物件，或開啓機器上的「管理工具」。檢視「本地安全性設定 - 安全性選項」，並確認兩種設備都已停用。預設值爲停用。



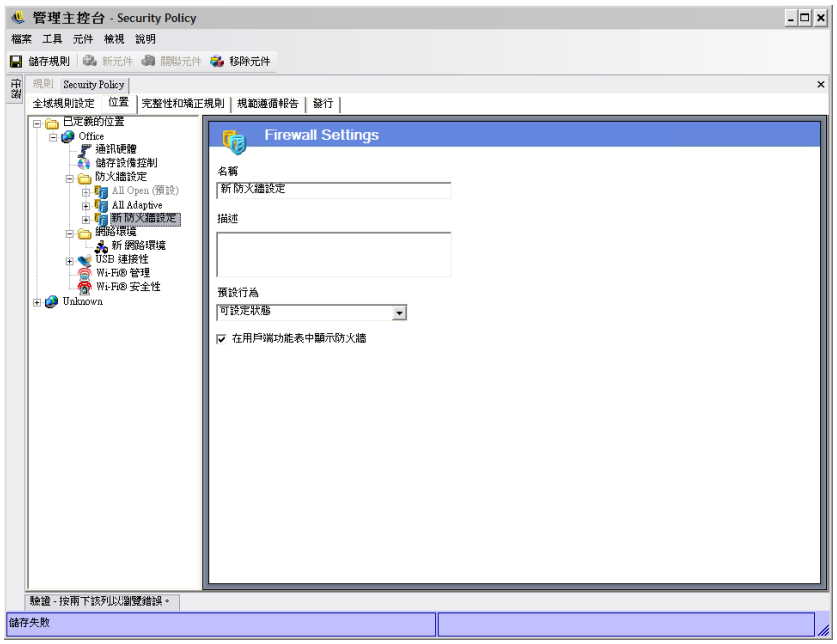
防火牆設定

「防火牆設定」可控制所有網路連接埠的連接性、存取控制清單、網路封包 (ICMP、ARP 等) 並決定在套用防火牆設定時，可取得插槽與可執行的應用程式。

附註：只有安裝 ZENworks Endpoint Security Management 才提供此功能，且無法用於 UWS 安全性規則。

若要存取此控制，請按一下「*位置*」索引標籤並按一下左邊規則樹中的「*防火牆設定*」圖示。

每個防火牆設定的元件都是個別設定的，只有 TCP/UDP 連接埠的預設行爲需要進行設定。在啓用此設定時將會影響所有的 TCP /UDP 連接埠。您可以使用不同的設定建立個別或一組連接埠。



若要新建防火牆設定：

1 在元件樹中選取「*防火牆設定*」，並按一下「*新元件*」按鈕。

2 爲防火牆設定命名並進行描述 .

3 在元件樹中的 *TCP/UDP 連接埠*上按一下滑鼠右鍵，然後按一下「*新增新的 TCP/UDP 連接埠*」以選取所有 TCP/UDP 連接埠的預設行爲。

   您可以在防火牆設定中新增其他連接埠和清單，而您指定的行爲將會置換預設設定。

   例如，所有連接埠的預設行爲都會設爲「全部可設定狀態」。這表示串流媒體和 Web 瀏覽的連接埠清單已新增至防火牆設定中。「串流媒體」連接埠行爲設爲「關閉」，「Web 瀏覽」連接埠行爲設爲「開啓」。經由 TCP 連接埠 7070、554、1755 和 8000 的網路流量都會被封鎖。經由 TCP 連接埠 80 和 443 的網路流量都會開放，並可顯示在網路上。其他的連接埠將以「全部可設定狀態」的模式運作，且必須先請求取得經過這些連接埠的流量。

   如需詳細資訊，請參閱「TCP/UDP 連接埠」(第 73 頁)。

4 在「*存取控制清單*」上按一下滑鼠右鍵，然後按一下「*新增新的存取控制清單*」以新增可能有來路不明流量通過的位址 (無論目前的連接埠行爲爲何)。

   如需詳細資訊，請參閱「存取控制清單」(第 76 頁)。

5 在「*應用程式控制*」上按一下滑鼠右鍵，然後按一下「*新增新的應用程式控制*」以防止應用程式獲得網路存取或者封鎖其執行。

   如需詳細資訊，請參閱「應用程式控制」(第 79 頁)。

6 決定是否要在 ZENworks Security Client 功能表中顯示此防火牆 (如果未選取此選項，使用者將看不到此防火牆設定)。

7 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱「錯誤通知」(第 99 頁)。

若要建立與現有防火牆設定的關聯：

1 在元件樹中選取「*防火牆設定*」，並按一下「*關聯元件*」按鈕。

2 在清單中選取想要的防火牆設定，

3 如有必要，請變更預設行爲設定。

附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

單一位置內可包含多個防火牆設定。其中一個已定義爲預設設定，其餘的設定則可用來做爲使用者可以切換的選項。使用者通常在網路環境中需要特定的安全性限制，而且偶爾會有一小段時間需要解除或增加該限制 (例如，ICMP 廣播)，所以具備多個設定是非常有用的。

安裝中會包含以下防火牆設定：

- **All Adaptive (全部可調整)：**將所有網路連接埠設爲可設定狀態 (封鎖所有來路不明的內傳網路流量，並允許所有外傳的網路流量)，允許 ARP 和 802.1x 封包、允許所有網路應用程式的網路連接。
- **All Open (全部開啓)：**將所有網路連接埠設爲開啓 (允許所有網路流量)，並允許所有封包類型。允許所有網路應用程式的網路連接 .
- **All Closed (全部關閉)：**關閉所有的網路連接埠並限制所有的封包類型。

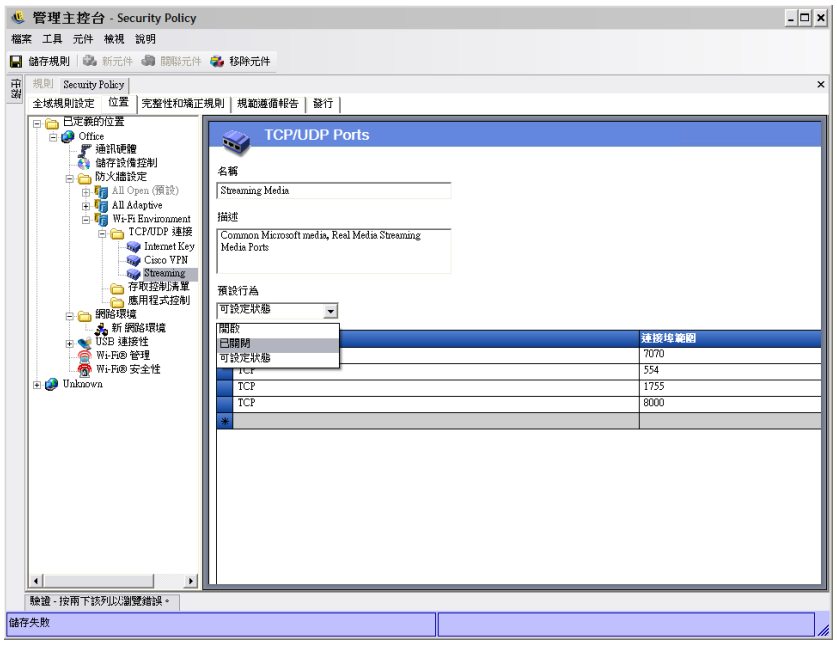
新位置會將單一防火牆設定「全部開啓」設爲其預設值。若要將不同的防火牆設定設爲預設值，請以滑鼠右鍵按一下想要的防火牆設定，然後選擇「*設成預設值*」。

TCP/UDP 連接埠

端點資料主要是藉由控制 TCP/UDP 連接埠活動來保護。此功能允許您建立 TCP/UDP 連接埠清單，且在此防火牆設定中將會以獨特的方式來處理此清單。清單包含連接埠與連接埠範圍的集合，並與其傳輸類型搭配使用，可定義範圍的功能。

附註：只有安裝 ZENworks Endpoint Security Management 才提供此功能，且無法用於 UWS 安全性規則。

若要存取此控制，請按一下「*位置*」索引標籤、按一下「*防火牆設定*」旁的 + 號、按一下所需「防火牆」旁的 + 號，然後按一下左側之規則樹狀結構中的「*TCP/UDP 連接埠*」圖示。



新的 TCP/UDP 連接埠清單可利用個別連接埠來定義，或依照清單中的每一行定義一個範圍 (1-100)。

若要定義新的 TCP/UDP 連接埠設定：

1. 在元件樹中的「*TCP/UDP 連接埠*」上按一下滑鼠右鍵，然後按一下「*新增新的 TCP/UDP 連接埠*」。
2. 爲連接埠清單命名並進行描述 .
3. 從下拉式清單中選取連接埠行爲：
   - **開啓：** 允許所有網路內傳和外傳流量。因爲允許所有的網路流量，所以對於此連接埠或連接埠範圍而言，您的電腦身分是可見的。
   - **已關閉：**已封鎖所有內傳和外傳網路流量。因爲所有網路識別要求均已遭封鎖，所以對於此連接埠或連接埠範圍而言，您的電腦身分是隱藏的。
   - **可設定狀態：**已封鎖所有來路不明的內傳網路流量。允許通過此連接埠或連接埠範圍上的所有外傳網路流量。
4. 按一下「*連接埠類型*」欄中的向下箭頭來指定傳輸類型：
   - TCP/UDP
   - Ether
   - IP
   - TCP
   - UDP
5. 輸入以下其中一種連接埠和連接埠類型：
   - 單一連接埠
   - 連接埠範圍，其格式爲第一個埠號之後緊接著一個破折號，然後是最後一個埠號 例如，1-100 將會新增介於 1 到 100 之間的所有連接埠

請造訪 Internet Assigned Numbers Authority (網際網路位址指派機構) 網頁 (http://www.iana.org)，以取得完整的連接埠與傳輸類型清單。

6 按一下「*儲存規則*」。

若要將現有的 TCP/UDP 連接埠關聯至此防火牆設定：

1 從元件樹中選取「*TCP/UDP 連接埠*」，然後按一下「*關聯元件*」按鈕。

2 從清單中選取所需連接埠。

3 設定預設的行爲設定。

變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。

安裝時已隨附數個 TCP/UDP 連接埠群組可供使用：

名稱	描述	輸送	值
所有連接埠	所有連接埠	全部	1-65535
BlueRidge VPN	Blue Ridge VPN 用戶端所使用的連接埠	UDP	820
Cisco VPN	Cisco* VPN 用戶端所使用的連接埠	IP	50、51
		UDP	500、4500
		UDP	1000-1200
		UDP	62514、62515、62517
		UDP	62519-62521
		UDP	62532、62524
一般網路	通常在建置防火牆時所需的「網路連接埠」	TCP	53
		UDP	53
		UDP	67、68
		TCP	546、547
		UDP	546、547
		TCP	647、847
		UDP	647、847

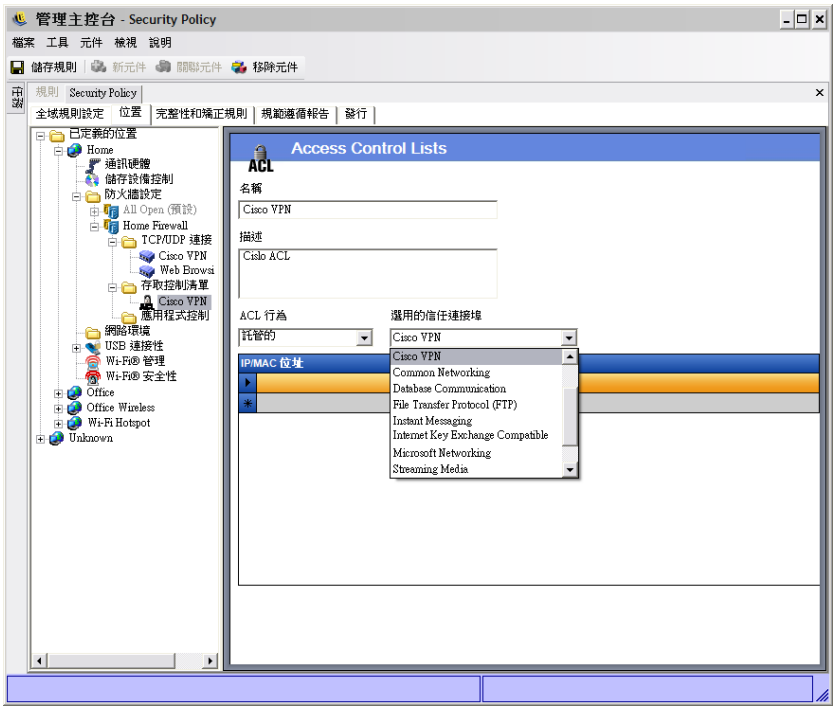
名稱	描述	輸送	值
資料庫通訊	Microsoft*、Oracle*、Siebel*、Sybase*、SAP* 資料庫連接埠	TCP	4100
		TCP	1521
		TCP	1433
		UDP	1444
		TCP	2320
		TCP	49998
		TCP	3200
		TCP	3600
檔案傳送協定 (FTP)	檔案傳送協定連接埠	TCP/UDP	21
即時訊息	Microsoft、AOL* 和 Yahoo* 即時訊息連接埠	TCP	6891-6900
		TCP	1863、443
		UDP	1863、443
		UDP	5190
		TCP	6901
		UDP	6901
		TCP	5000-5001
		UDP	5055
		TCP	20000-20059
		UDP	4000
		TCP	4099
		TCP	5190
Internet Key Exchange (網際網路金鑰交換) 相容 VPN	與 Internet Key Exchange (網際網路金鑰交換) 相容之 VPN 用戶端所使用的連接埠	UDP	500
Microsoft 網路	通用檔案共享 /Active Directory* 連接埠	TCP/UDP	135-139、445
開啓的連接埠	針對此防火牆開起的連接埠	TCP/UDP	80
串流媒體	一般 Microsoft 和 Real 串流媒體連接埠	TCP	7070、554、1755、8000
Web 瀏覽	一般 Web 瀏覽器連接埠，包括 SSL	全部	80、443

存取控制清單

無論目前的連接埠行爲爲何，某些位址可能會有來路不明的流量通過 (例如企業備份伺服器、交換伺服器等)。在需要將來路不明流量傳入和傳出信任伺服器時，存取控制清單 (ACL) 可解決此問題。

附註：只有安裝 ZENworks Endpoint Security Management 才提供此功能，且無法用於 UWS 安全性規則。

若要存取此控制，請按一下「*位置*」索引標籤、按一下「*防火牆設定*」旁的 + 號、按一下所需「防火牆」旁的 + 號、在左側之規則樹狀結構中的「*存取控制清單*」上按一下滑鼠右鍵，然後按一下「*新增新的存取控制清單*」。



若要新建 ACL 設定：

1. 在元件樹中的「*存取控制清單*」上按一下滑鼠右鍵，然後按一下「*新增新的存取控制清單*」。
2. 爲 ACL 命名並進行描述 .
3. 指定 ACL 位址或巨集。
4. 指定 ACL 類型：
   - **IP:** 此類型會將位址限制爲 15 個字元，並且只包含 0-9 的數字與句號，例如 123.45.6.189。您也可以輸入 IP 位址的範圍，例如 123.0.0.0 - 123.0.0.255。
   - **MAC：**此類型會將位址限制爲 12 個字元，並且只包含 0-9 的數字和 A-F 的字母 (大寫和小寫) 並使用冒號區隔，例如 00:01:02:34:05:B6。
5. 選取「ACL 行爲」下拉式清單，並決定列出的 ACL 應爲「*信任*」(即使所有 TCP/UDP 連接埠均已關閉，還是一律允許流量通過) 或「*不信任*」(封鎖存取)。
6. 如果選取「*信任*」，請選取此 ACL 將使用的「*選用的信任連接埠 (TCP/UDP)*」。這些連接埠將允許所有的 ACL 流量，而其他的 TCP/UDP 連接埠將維持其目前的設定。選取「*無*」，表示此 ACL 可能會使用任何連接埠。
7. 按一下「*儲存規則*」。

若要將現有的 ACL 或巨集關聯至此防火牆設定：

1 從元件樹中選取「*存取控制清單*」，然後按一下「*關聯元件*」按鈕。

2 從清單中選取 ACL 或巨集。

3 視需要進行 ACL 行爲設定。

附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。

網路位址巨集清單

以下爲特殊「存取控制」巨集的清單。這些巨集均可在防火牆設定中進行個別關聯，以做爲 ACL 的一部分。

表格 2-1 *網路位址巨集*

巨集	描述
[Arp]	允許 ARP (位址解析通訊協定) 封包。「*位址解析*」這個術語表示在網路上尋找電腦位址的程序。位址是使用通訊協定加以「解析」，其中一部分資訊是由在本機電腦上執行的用戶端程序傳送至在遠端電腦上執行的伺服器程序。伺服器所接收的資訊允許伺服器識別需要該位址的唯一網路系統，因而可提供所需的位址。在用戶端接收到來自包含所需位址之伺服器的回應時，即完成位址解析程序。
[Icmp]	允許 ICMP (網際網路控制訊息通訊協定) 封包。路由器、中繼裝置或主機可以使用 ICMP，與其他的路由器、中繼裝置或主機進行更新或錯誤訊息的通訊。ICMP 訊息會在數種情況中傳送，例如當資料包無法送達其目的地、當閘道不具備轉遞資料包的緩衝處理功能，以及當閘道可以指引主機在較短路徑上傳送流量。
[IpMulticast]	允許 IP 多路廣播封包。多路廣播爲一項節省頻寬的技術，可藉由同時傳遞單一資料流的資訊至數千個公司收件者及家庭，來降低流量。利用多路廣播的應用程式包括視訊會議、公司通訊、遠距學習，以及軟體、股市指數及新聞的配送。多路廣播封包可透過 IP 或乙太網路位址進行配送。
[EthernetMulticast]	允許乙太網路多路廣播封包。
[IpSubnetBrdcast]	允許子網路廣播封包。子網路廣播可用來將封包傳送至子網路、超網路，或其他無類別網路的所有主機。無類別網路的所有主機會監聽和處理送往子網路廣播位址的封包。
[Snap]	允許 SNAP 編碼封包。
[LLC]	允許 LLC 編碼封包。
[Allow8021X]	允許 802.1x 封包。爲了克服「有線等位私密」(WEP) 金鑰的缺點，Microsoft 與其他廠商運用 802.1x 做爲替代的驗證方式。802.1x 爲以連接埠爲基準的網路存取控制，會使用「可延伸式驗證通訊協定」(EAP) 或證書。目前大多數主要的無線網路卡廠商和許多存取點廠商都支援 802.1x。此設定也允許「輕量可延伸式驗證通訊協定」(LEAP) 和「Wi-Fi 保護存取協定」(WPA) 驗證封包。
[Gateway]	代表目前 IP 組態「預設閘道」位址。輸入此值時，ZENworks Security Client 允許來自目前 IP 組態「預設閘道」的所有網路流量做爲信任的 ACL。
[GatewayAll]	與 [Gateway] 相同，但適用於所有定義的閘道。

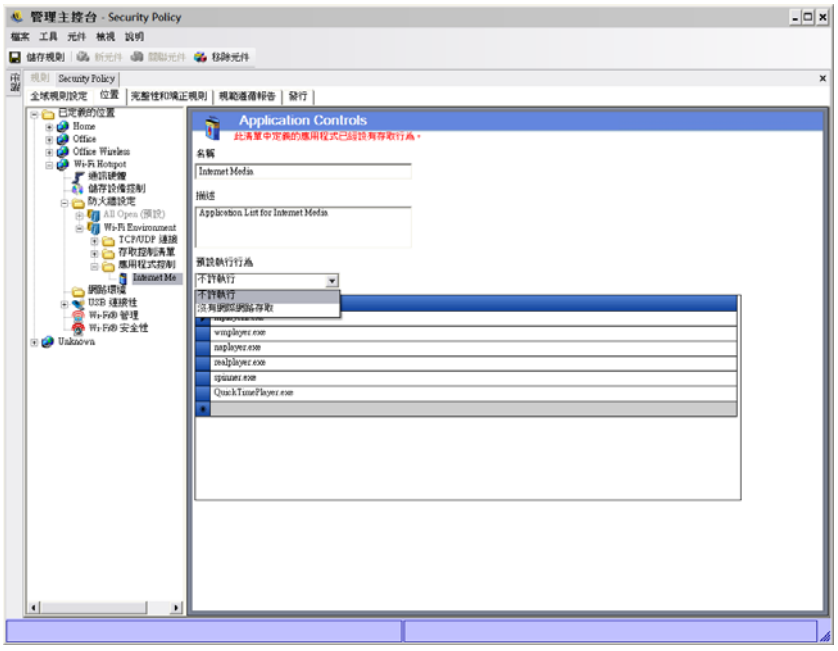
巨集	描述
[Wins]	代表目前用戶端 IP 組態「預設 WINS 伺服器」位址。輸入此值時，ZENworks Security Client 允許來自目前 IP 組態「預設 WINS 伺服器」的所有網路流量做爲信任的 ACL。
[WinsAll]	與 [Wins] 相同，但適用於所有定義的 WINS 伺服器。
[Dns]	代表目前用戶端 IP 組態「預設 DNS 伺服器」位址。輸入此值時，ZENworks Security Client 允許來自目前 IP 組態「預設 DNS 伺服器」的所有網路流量做爲信任的 ACL。
[DnsAll]	與 [Dns] 相同，但適用於所有定義的 DNS 伺服器。
[Dhcp]	代表目前用戶端 IP 組態「預設 DHCP 伺服器」位址。輸入此值時，ZENworks Security Client 允許來自目前 IP 組態「預設 DHCP 伺服器」的所有網路流量做爲信任的 ACL。
[DhcpAll]	與 [Dhcp] 相同，但適用於所有定義的 DHCP 伺服器。

應用程式控制

此功能可讓管理員封鎖應用程式，以防止獲得網路存取或者封鎖其執行。

附註：只有安裝 ZENworks Endpoint Security Management 才提供此功能，且無法用於 UWS 安全性規則。

若要存取此控制，請按一下「*位置*」索引標籤、按一下「*防火牆設定*」旁的 + 號、按一下所需防火牆旁的 + 號，然後按一下左側之規則樹狀結構中的「*應用程式控制*」圖示。



若要建立新的應用程式控制設定：

1 在元件樹中的「*應用程式控制*」按一下滑鼠右鍵，然後按一下「*新增新的應用程式控制*」。

2 爲應用程式清單命名並進行描述 .

3 選取執行行爲。此行爲將套用至列出的所有應用程式。如果需要多種行爲 (例如，拒絕某些網路應用程式的網路存取，同時拒絕執行所有檔案共享應用程式)，則需定義多個應用程式控制。選取下列選項之一：

- **所有允許的：**允許所有列出的應用程式執行並進行網路存取。
- **不執行：**所有列出的應用程式均不允許執行。
- **沒有網路存取：**拒絕所有列出的應用程式執行網路存取。從應用程式啓動的應用程式 (例如網路瀏覽器) 亦無法執行網路存取。

附註：封鎖應用程式的網路存取並不影響將檔案儲存至對應的網路磁碟機。允許使用者將檔案儲存至所有可以使用的網路磁碟機。

4 指定每個要封鎖的應用程式。每一行應輸入一個應用程式 .

重要：封鎖重要應用程式的執行，可能會對系統操作產生不利的影響。遭封鎖的 Microsoft Office 應用程式將會嘗試執行其安裝程式。

5 按一下「*儲存規則*」。

若要將現有的應用程式控制清單關聯至此防火牆設定：

1 選取元件樹中的「應用程式控制」，然後按一下「*關聯元件*」按鈕。

2 從清單中選取應用程式集 .

3 視需要設定應用程式和限制層級。

附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。

可用的應用程式控制已於下方列出。預設的執行行爲是「沒有網路存取」。

表格 2-2 *應用程式控制*

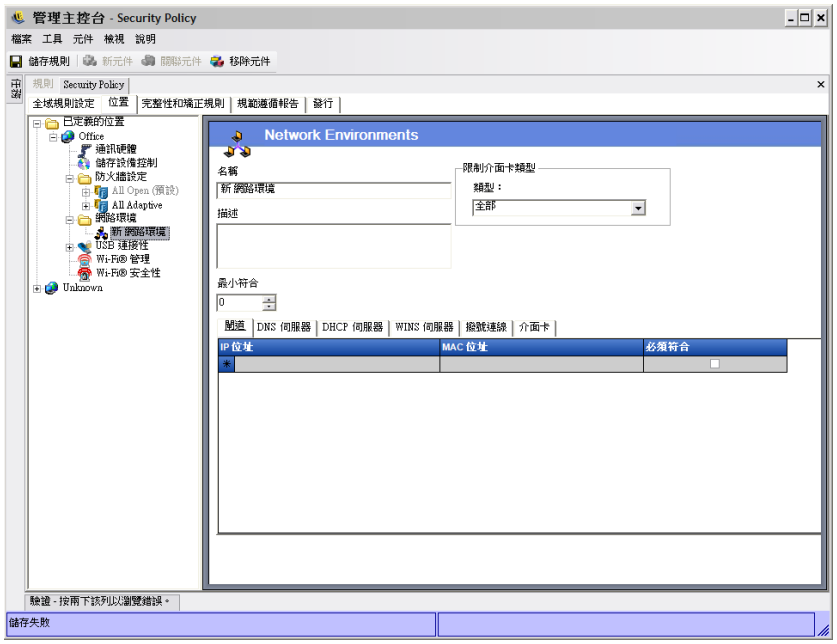
名稱	應用程式
Web 瀏覽器	explore.exe；netscape.exe；netscp.exe
即時訊息	aim.exe；icq.exe；msmsgs.exe；msnmsgr.exe；trillian.exe；ypager.exe
檔案共享	blubster.exe；grokster.exe；imesh.exe；kazaa.exe；morpheus.exe；napster.exe；winmx.exe
網際網路媒體	mplayer2.exe；wmplayer.exe；naplayer.exe；realplay.exe；spinner.exe；QuickTimePlayer.exe

如果將同一應用程式新增至相同防火牆設定中的兩個不同應用程式控制 (例如，在相同防火牆設定底下，已在其中一個應用程式控制中封鎖 kazaa.exe 的執行，並在另一個已定義應用程式控制中封鎖 kazaa.exe，以防止獲得網路存取)，則會將最嚴格的控制套用在指定的執行檔上 (例如，封鎖 kazaa 的執行).

網路環境

如果網路參數 (閘道伺服器、DNS 伺服器、DHCP 伺服器、WINS 伺服器、可用的存取點和 / 或特定介面卡連接) 在該位置上是已知的，您可以將用來識別網路的服務詳細資料 (IP 和 MAC) 輸入規則中，以提供立即的位置切換功能，使用者也不再需要將環境儲存爲位置。

若要存取此控制，請按一下「*位置*」索引標籤並按一下左邊規則樹中的「*網路環境*」資料夾。



該清單可讓管理員定義存在於環境中的網路服務。每個網路服務都可包含多個位址。管理員可決定在環境中必須符合的位址數以啓用位置切換。

您必須在每個網路環境定義中使用兩個或多個位置參數。

若要定義網路環境：

1. 在元件樹中選取「*網路環境*」，並按一下「*新元件*」按鈕。
2. 爲網路環境命名並進行描述 .
3. 在「*限制介面卡類型*」下拉式清單中選擇允許存取此網路環境的介面卡類型：
   - 無線
   - 全部
   - 數據機
   - 有線
   - 無線
4. 指定識別網路環境所需的網路服務最低數量。

   每個「網路環境」都有最低數量的位址供 ZENworks Security Client 進行識別。*「最低符合」中的數量不能超過在索引標籤式清單中識別爲必要的網路位址總數*。指定識別網路環境所需的網路服務最低數量。

5 針對每種服務指定以下資訊：

- **IP 位址：**指定最多 15 個字元，其中只能包含 0-9 和句號。例如，123.45.6.789
- **MAC 位址：** 您也可以選擇指定 12 個字元，並且只包含 0-9 的數字和 A-F 的字母 (大寫和小寫)，並使用冒號區隔。例如，00:01:02:34:05:B6
- 如果您需要此服務的識別來定義網路環境，請選取「*必須符合*」核取方塊。

6 在「*撥接連接*」和「*介面卡*」索引標籤中指定以下需求：

- 若使用「*撥接連接*」，則必須指定電話簿中的「RAS 項目」名稱，或撥接號碼。

  附註：電話簿項目必須包含字母和數字字元，且不能僅包含特殊字元 (@、#、$、%、- 等) 或數字字元 (1-9)。僅包含特殊和數字字元的項目將被視爲撥接號碼。

- 若使用介面卡，請爲每個允許的介面卡指定 SSID。您可以指定介面卡，以精確地限制可存取此網路環境的介面卡。如果未輸入 SSID，所有允許的介面卡類型都可獲得存取權限 .

若要建立現有「網路環境」與此位置的關聯：

附註：在相同的安全性規則中，將建立單一網路環境與兩個或多個位置建立關聯可能會產生未預期的結果，因此我們不建議您這樣做。

1 在元件樹中選取「*網路環境*」，並按一下「*關聯元件*」按鈕。

2 在清單中選取網路環境。

3 視需要設定網路環境參數。

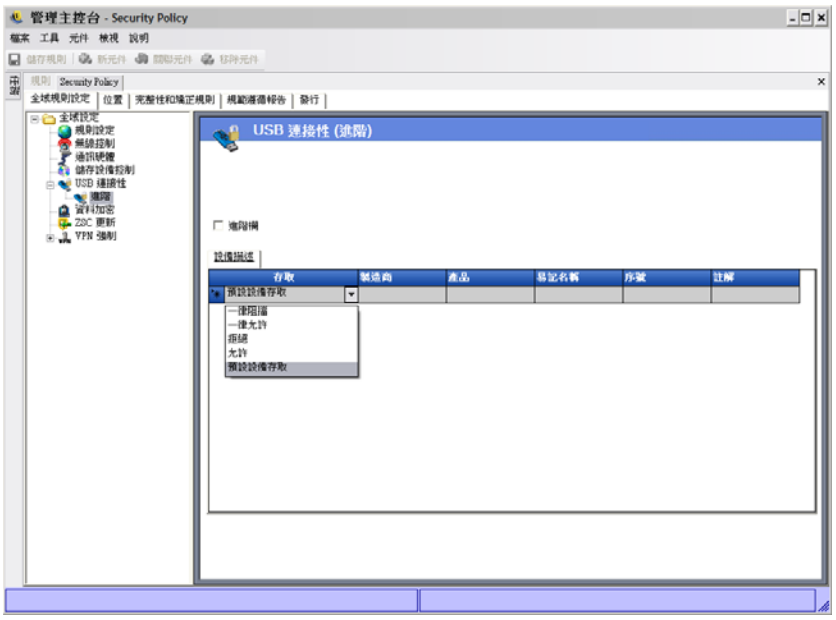
附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。

USB 連接性

規則可允許或拒絕透過 USB BUS 連接的所有設備。您可以將這些設備從 USB 設備庫存報告掃描至規則中，或者掃描目前連接至機器的所有設備。您可以依照製造商、產品名稱、序號、類型等來篩選這些設備。管理員可以基於支援的目的，依照製造商類型 (例如允許所有 HP 設備) 或產品類型 (允許所有 USB 人機介面設備，例如滑鼠和鍵盤) 來設定規則以接受一組設備。此外，您可以允許個別的設備以避免將不支援的設備導入網路中 (例如，不允許規則以外的所有印表機)。

若要存取此控制，請按一下「*全域規則設定*」索引標籤，並按一下左邊規則樹中的「*USB 連接性*」。



指定要允許或拒絕存取任何不在清單內的設備。

以下的方法可讓您填入清單，以允許或拒絕這些設備的 USB 連接。

- 「手動稽核設備」(第 83 頁)
- 「輸入裝置清單」(第 83 頁)

手動稽核設備

1. 將設備插入機器 (已安裝 「管理主控台」) 的 USB 連接埠中。
2. 待設備就緒之後，按一下 「*掃描*」按鈕。如果設備具有序號，其 「描述」和 「序號」將會顯示在清單中。
3. 在下拉式清單中選取設定 (「*全域抽取式設備*」設定將不會套用在此規則中)：
   - **啓用：**偏好清單中的設備將允許完整的讀取 / 寫入功能，而其他的 USB 和外部儲存設備都會停用。
   - **唯讀：** 偏好清單中的設備將允許唯讀功能，而其他的 USB 和外部儲存設備都會停用 。

您可以爲此規則所允許的每個設備重複這些步驟。所有設備都會套用相同的設定。

輸入裝置清單

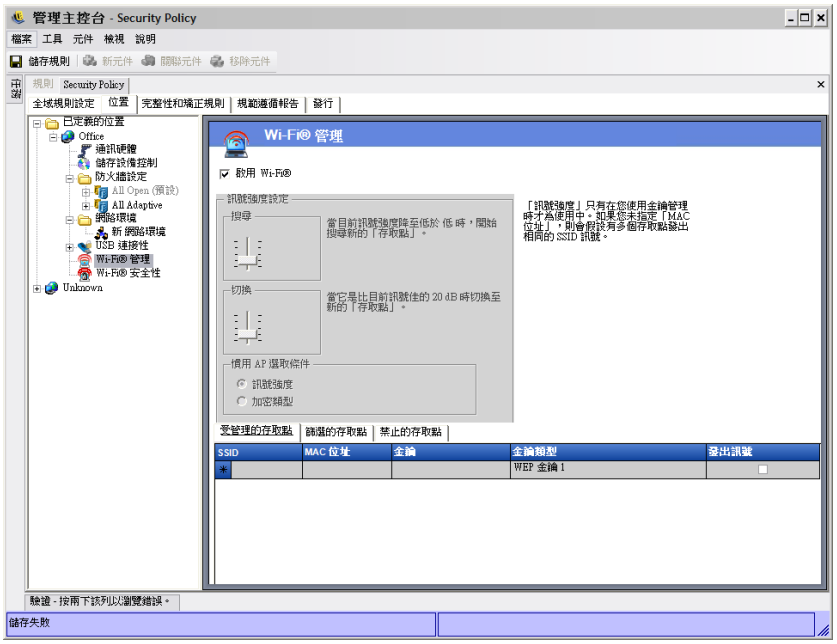
Novell USB Drive Scanner 應用程式會產生一個包含序號的設備清單 (「USB Drive Scanner」(第 41 頁))。若要輸入此清單，請按一下 「*輸入*」並瀏覽清單。該清單將會填入 「*敘述*」和 「*序號*」欄位。

Wi-Fi 管理

「Wi-Fi 管理」可讓管理員建立 「存取點」清單。輸入這些清單中的無線存取點將會決定端點可在位置中連接的存取點，並決定端點可在 Microsoft Zero Configuration Manager (Zero Config) 中檢視的存取點。此功能不支援第三方的無線組態管理員。如果未輸入存取點，則端點將可使用全部的存取點。

若要存取此控制，請按一下「*位置*」索引標籤，並按一下左邊規則樹中的「*Wi-Fi 管理*」。

附註：在 Wi-Fi 安全性或 Wi-Fi 管理中，取消選取「*啓用*」將會停用此位置中的所有 Wi-Fi 連接性。



將存取點輸入「*受管理的存取點*」清單將會關閉 Zero Config，並強制端點只能連接列出的存取點 (如果可使用)。如果無法使用受管理的存取點，ZENworks Security Client 將會退回至「篩選的存取點清單」。在「禁止的存取點」中輸入的存取點將不會顯示在 Zero Config 中。

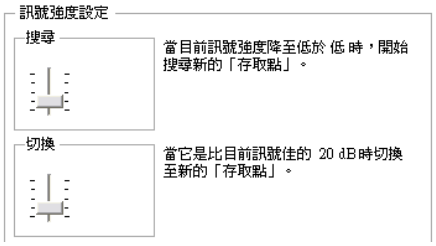
附註：僅 Windows* XP 作業系統支援存取點清單功能。在部署存取點清單前，我們建議您在所有端點上清除 Zero Config 中的偏好網路清單。

以下幾節中包含了更詳細的資訊：

- 「Wi-Fi 訊號強度設定」(第 84 頁)
- 「受管理的存取點」(第 86 頁)
- 「篩選的存取點」(第 86 頁)
- 「禁止的存取點」(第 87 頁)

Wi-Fi 訊號強度設定

當您在清單中定義多個 WEP 管理的存取點 (AP) 時，將可設定 Wi-Fi 介面卡的「訊號強度」切換。您可以按位置調整訊號強度限定值，以決定 ZENworks Security Client 何時將搜尋、丟棄和切換至在清單中定義的其他存取點。



您可以調整下列資訊：

- **搜尋：**當達到此訊號強度等級時，ZENworks Security Client 會開始搜尋新的存取點以進行連接。預設值爲「低」[-70 dB]。
- **切換：**爲了讓 ZENworks Security Client 連接新的存取點，該存取點必須以高於目前連接的指定訊號強度進行廣播。預設值爲 +20 dB。

透過電腦的 Miniport 驅動程式所報告的強度 (單位爲 dB)，可決定訊號強度限定值。由於每個 Wi-Fi 介面卡和無線電的「接收訊號強度指示」(Received Signal Strength Indication, RSSI) 對於 dB 訊號會有不同的標準，因此該數字可能會隨著介面卡的不同而有所改變。

您可以根據以下項目設定存取點選擇的偏好選項：

- 訊號強度
- 加密類型

與「管理主控台」中定義之限定值相關的預設數字，對於大多數的 Wi-Fi 介面卡來說都是通用的。您必須研究 Wi-Fi 介面卡的 RSSI 值以輸入正確的層級。Novell 的預設值爲：

名稱	預設值
非常好	-40 dB
很好	-50 dB
好	-60 dB
低	-70 dB
非常低	-80 dB

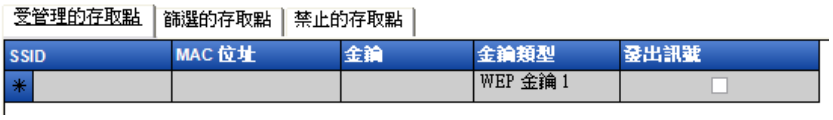
附註：雖然以上的訊號強度名稱與 Microsoft 的 Zero Configuration Service 所使用的名稱相符，但限定值可能不相符。Zero Config 會根據訊號雜訊比 (Signal to Noise Ratio, SNR)，而不僅僅是根據 RSSI 所報告的 dB 值來決定該值。例如，當 Wi-Fi 介面卡收到 -54 dB 的訊號時，雜訊等級爲 -22 dB，因此 SNR 報告爲 32dB (-54 - -22=32)，這在 Zero Configuration 等級中會視爲「非常好」的訊號強度；然而在 Novell 等級中，-54 dB (如果透過 Miniport 驅動程式進行報告) 的訊號代表的是「很好」的訊號強度。

您必須知道，最終使用者將無法看見 Novell 訊號強度，此資訊只會顯示使用者透過 Zero Config 所看到的，與實際發生之間的差異。

受管理的存取點

ZENworks Endpoint Security Management 可提供不需要使用者介入的自動配送並套用「有線等效加密 (WEP)」金鑰的簡易程序 (忽略並關閉 Microsoft Zero Configuration 管理員)。您不需要在電子郵件或便條紙中載明以進行傳送，因此可以保護金鑰的完整性。事實上，最終使用者將不需要知道金鑰就可以自動連接至存取點。這將可避免將金鑰洩露給未獲授權的使用者。

由於共享 WEP 金鑰驗證將無法避免地產生安全性漏洞，因此 Novell 僅支援公開的 WEP 金鑰驗證。透過共享驗證，用戶端 / 存取點金鑰驗證程序會傳送可輕易經由無線方式擷取的純文字和加密版本的驗證要求。這將提供駭客純文字和加密版本的文句。當他們取得這些資訊時，金鑰破解便無關緊要。



爲每個存取點提供以下資訊：

- **SSID**：識別 SSID 號碼。SSID 號碼會區分大小寫。
- **MAC 位址**： 識別 MAC 位址 (由於 SSID 之間具有共通性，因此建議此方式)。如果未指定此項目，則系統會假設有多個存取點都在相同的 SSID 號碼上加上信標。
- **金鑰**：指定存取點的 WEP 金鑰 (10 或 26 個十六進位字元)。
- **金鑰類型**：在下拉式清單中選取適當的層級以識別加密鑰索引。
- **信號發送**：檢查定義的存取點目前是否廣播其 SSID。如果這是未加上信標的存取點，則不要選取該選項。

附註：ZENworks Security Client 會嘗試先連接在規則中已加上信標的每個存取點。如果找不到加上信標的存取點，ZENworks Security Client 將嘗試連接已列於規則中，但未加上信標的存取點 (由 SSID 識別)。

當您在「*受管理的存取點*」清單中定義一個或多個存取點時，將可設定 Wi-Fi 介面卡的「訊號強度」切換。

篩選的存取點

Zero Config 僅顯示輸入至*篩選的存取點*清單中的存取點。這可避免端點連接未授權的存取點。

針對每個存取點輸入以下資訊：

- **SSID**：識別 SSID 號碼。SSID 號碼會區分大小寫。
- **MAC 位址**： 識別 MAC 位址 (由於 SSID 之間具有共通性，因此建議此方式)。如果未指定此項目，則系統會假設有多個存取點都在相同的 SSID 上加上信標。

禁止的存取點

在「禁止的存取點」清單中輸入的存取點將不會顯示在 Zero Config 中，系統也會禁止端點連接這些存取點。

針對每個存取點輸入以下資訊：

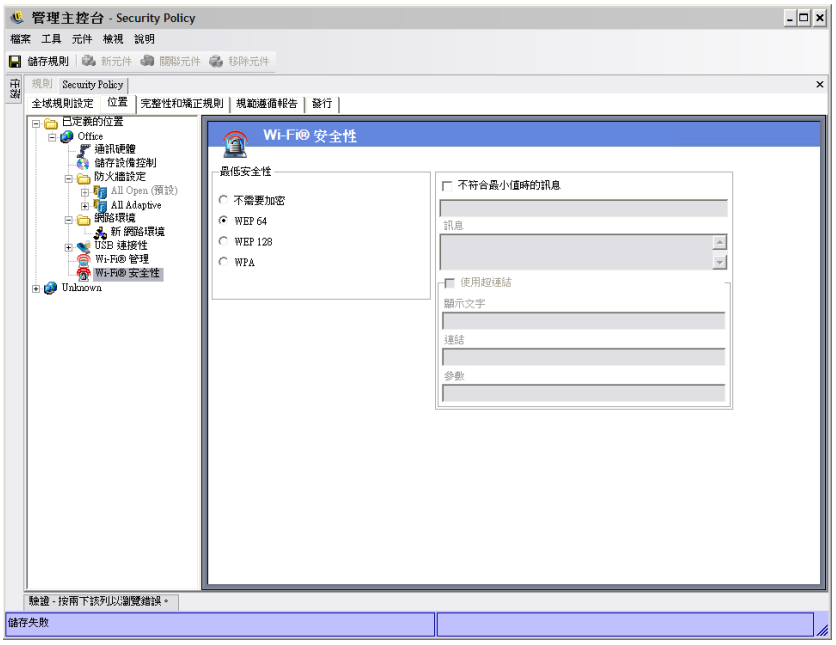
- **SSID**：識別 SSID 號碼。SSID 號碼會區分大小寫。
- **MAC 位址**：- 識別 MAC 位址 (由於 SSID 之間具有共通性，因此建議此方式。如果未指定此項目，則系統會假設有多個存取點都在相同的 SSID 上加上信標。

Wi-Fi 安全性

如果在全域中允許 Wi-Fi 通訊硬體 (Wi-Fi 介面卡 PCMCIA 或其他介面卡，和內建的 Wi-Fi Radio) (請參閱 「無線控制」 (第 48 頁))，您可在此位置將其他的設定套用至介面卡。

若要存取此控制，請按一下「*位置*」索引標籤，並按一下左邊規則樹中的「*Wi-Fi 安全性*」。

附註：在 Wi-Fi 安全性或 Wi-Fi 管理中，取消選取「*啓用*」將會停用此位置中的所有 Wi-Fi 連接性。



您可以設定 Wi-Fi 介面卡只能夠在指定的位置中，與具有特定加密層級的存取點進行通訊。

例如，如果您將 WPA 組態的存取點部署在分公司，便可限制介面卡只能與具有 WEP 128 (或更高) 加密層級的存取點進行通訊，以防止其意外連接至不安全的存取點。

當設定位於「不需要加密」之上時，您必須寫入「*自訂使用者訊息*」。

當您在「*受管理*」和「*篩選的存取點*」清單中輸入兩個或多個存取點時，可依照加密層級或訊號強度來設定連接至存取點的偏好選項。選取的層級將強制連接至符合最低加密需求 (或更高) 的存取點。

例如，如果加密需求爲 WEP 64 且偏好選項爲加密，則具有最高加密強度的存取點將優於其他的存取點。如果偏好選項爲訊號強度，則具有最強訊號的存取點將最先進行連接。

2.2.3 完整性和補救規則

ZENworks Endpoint Security Management 可提供驗證所需軟體是否正在端點上執行的功能，並在驗證失敗時，提供即時補救程序。

以下幾節中包含了更詳細的資訊：

- 「防毒軟體和間諜軟體規則」(第 88 頁)
- 「完整性測試」(第 90 頁)
- 「完整性檢查」(第 91 頁)
- 「進階程序檔規則」(第 92 頁)

防毒軟體和間諜軟體規則

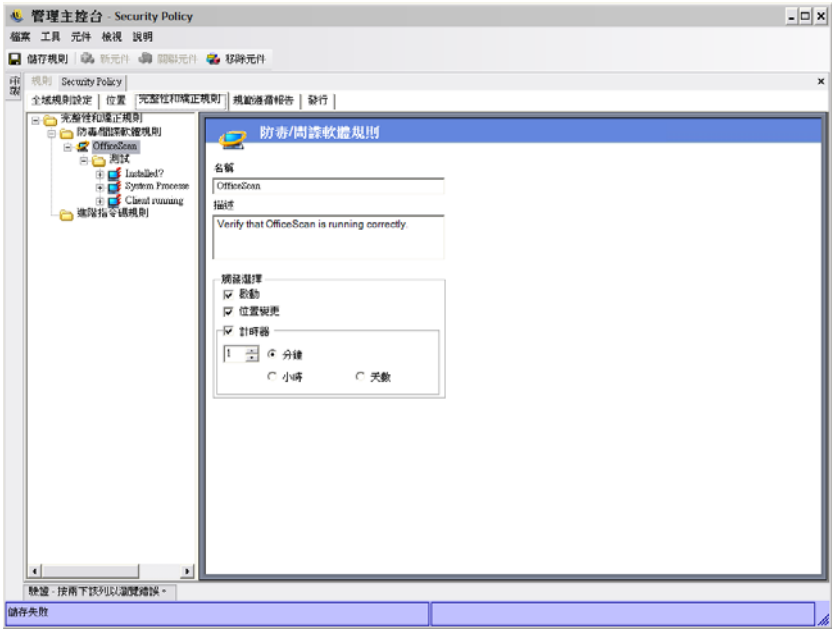
防毒 / 間諜軟體規則會驗證端點上指定的防毒軟體或防間諜軟體正在執行且爲最新版本。系統會執行測試以判斷軟體是否正在執行，以及是否爲最新版本。若這兩項檢查都成功，將允許端點切換至任何已定義的位置。若未通過其中一項測試，則會引起以下動作 (由管理員定義)：

- 傳送報告至「報告服務」。
- 自訂使用者訊息就會顯示，且可能具有啓動連結，提供如何修復規則衝突的相關資訊。
- 使用者會切換成「隔離狀態」，此狀態會限制使用者的網路存取且不允許特定程式存取網路，以防止使用者進一步感染網路。

一旦後續的測試判斷端點已符合規範，安全性設定即會自動返回其原始狀態。

附註：只有安裝 ZENworks Endpoint Security Management 才提供此功能，且無法用於 UWS 安全性規則。

若要存取此控制，請按一下「*完整性和補救規則*」索引標籤，並按一下左邊規則樹中的「*防毒 / 間諜軟體規則*」。



您可以針對不在預設清單上的軟體建立自訂測試。也可建立單一測試，針對相同規則內一或多個軟體執行檢查。每組「程序執行」和「檔案存在」檢查，將會有其自己的「成功 / 失敗」結果。

若要建立新的防毒或間諜軟體規則：

1 在元件樹中選取「*防毒 / 間諜軟體規則*」然後按一下「*新防毒 / 間諜軟體*」。

2 按一下「*新元件*」。

3 爲規則命名並進行描述。

4 選取規則的觸發：

- **啓動**：在系統啓動時執行測試。
- **位置變更**：每當 ZENworks Security Client 切換至新位置時執行測試。
- **計時器**：按分鐘、小時或日期在定義的排程中執行完整性測試。

5 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

6 定義「完整性測試」。

若要建立現有防毒軟體或間諜軟體規則的關聯：

1 選取「*防毒 / 間諜軟體規則*」，然後按一下「*關聯元件*」。

2 從清單中選取所需規則。

3 (選擇性) 重新定義測試、檢查和結果。

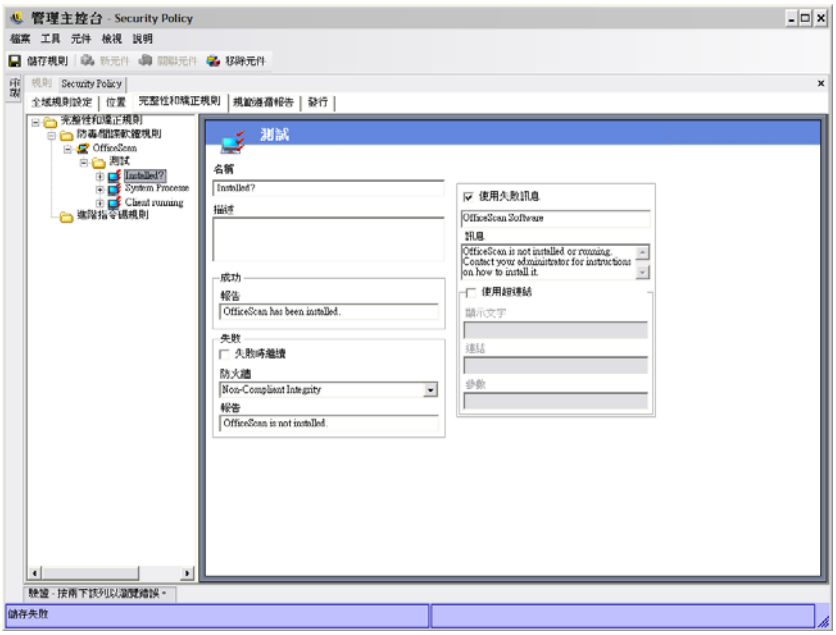
附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

4 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

完整性測試和檢查會自動包含在規則內，您並可視需要加以編輯。

完整性測試

每個完整性測試都可執行兩種檢查，分別爲「*檔案存在*」和「*程序執行*」。每個測試將有自己的成功和失敗結果。



所有已定義的防毒軟體和間諜軟體規則均具備預先撰寫的標準測試和檢查。您可以在完整性規則中加入其他測試。

系統會以此處所輸入的順序執行多個測試。第一個測試必須先成功完成，下一個測試才會執行。

若要建立完整性測試：

1. 在元件樹中選取「*完整性測試*」，按一下所需報告旁邊的 + 號，在「*測試*」上按一下滑鼠右鍵，後按一下「*新增新測試*」。
2. 爲測試命名並進行描述 .
3. 指定測試的成功報告文字。
4. 針對測試失敗，定義下列各項：
   - **失敗時繼續**：如果使用者可在測試失敗後繼續擁有網路連接性，請選取此選項；如果測試應繼續則請勿選取。
   - **防火牆**：如果測試失敗，將套用此設定。「全部關閉」、「不符規範的完整性」或自訂「隔離」防火牆設定，將可防止使用者連接至網路。
   - **訊息**：選取測試失敗時要顯示的自訂使用者訊息。這可包含補救步驟，以供最終使用者使用。
   - **報告**：提供傳送至報告服務的失敗報告。
5. 提供失敗訊息。此訊息只有在一或多個檢查失敗時才會顯示。按一下核取方塊，然後在提供的方塊中指定訊息資訊。
6. 您可加入超連結以提供補救選項。這可以是可取得更多資訊的連結，或是下載可用於測試失敗之修補程式或更新程式的連結 (請參閱 「超連結」(第 64 頁))。

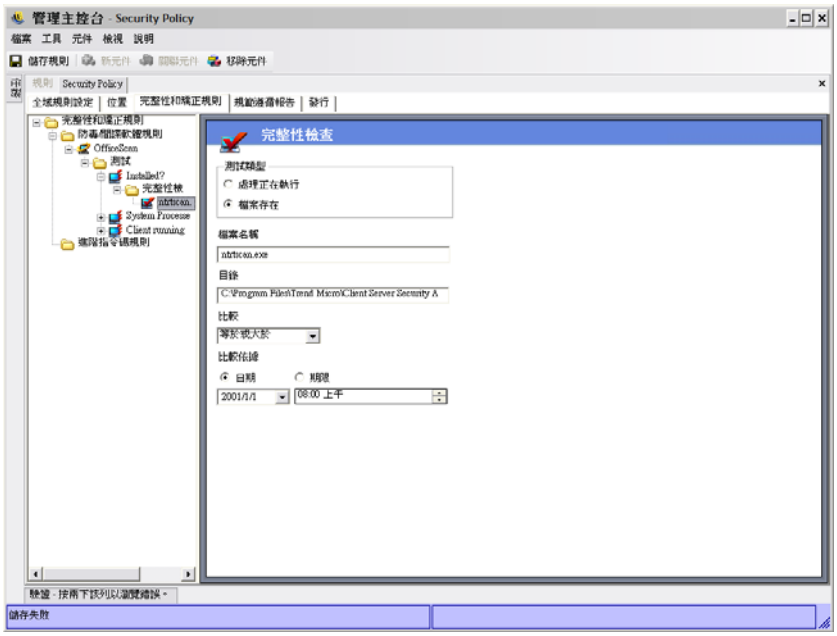
7 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

8 定義「完整性檢查」。

9 如有需要，可重複上述步驟以建立新的防毒軟體或間諜軟體測試。

完整性檢查

每個測試的檢查都會判斷是否正在執行一個或多個防毒軟體或間諜軟體，或是否存在基本檔案。您至少需要定義一項檢查，測試才能執行。



若要建立新檢查，請在左側規則樹中的「*完整性檢查*」上按一下滑鼠右鍵，然後按一下「*新增新的完整性檢查*」。選取兩個檢查類型之一，並提供資訊，如下所述：

程序正在執行：判定軟體在觸發事件時是否執行 (例如，AV 用戶端)。此項檢查需要的唯一資訊是執行檔名稱。

檔案存在：此檢查可用於判斷在觸發事件時，軟體是否爲目前且最新版本。

在提供的欄位中輸入下列資訊：

- **檔案名稱：**指定要檢查的檔案名稱。
- **檔案目錄：**指定檔案所在的目錄。
- **檔案比較：**從下拉式清單中選取日期比較：
  - 無
  - 等於
  - 等於或大於
  - 等於或小於
- **比較依據：**指定「*期限*」或「*日期*」。
  - 「*日期*」可確保檔案不會早於指定的日期和時間 (例如，最後更新的日期)。
  - 「*期限*」可確保檔案不會早於指定的時間期間 (以天數來衡量)。

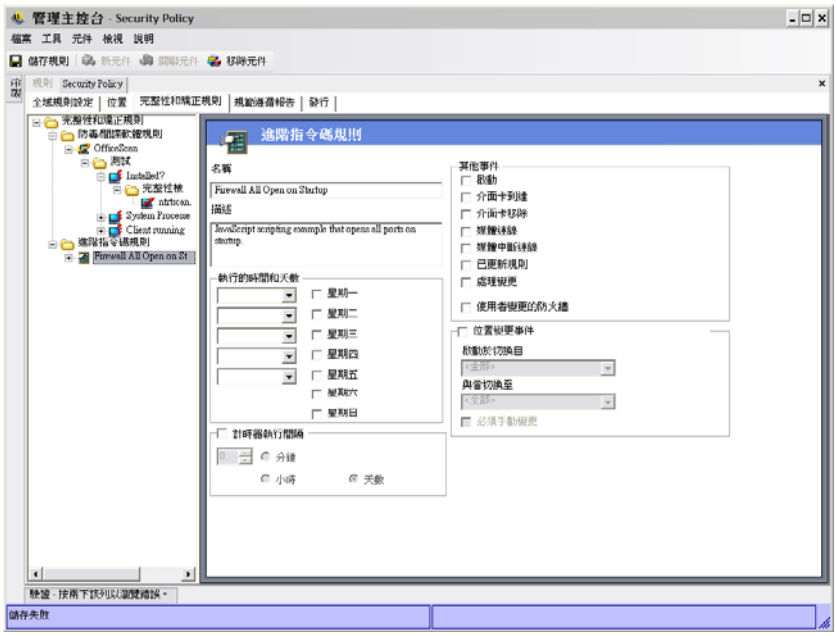
附註：使用「*期限*」檢查時，「等於」檔案比較會被視爲「等於或小於」。

檢查是依照其輸入的順序執行。

進階程序檔規則

ZENworks Endpoint Security Management 包括進階規則程序檔工具，讓管理員能夠建立極度有彈性且複雜的規則和補救動作。

若要存取此控制，請按一下「*完整性和補救規則*」索引標籤，然後按一下左邊規則樹中的「*進階程序檔規則*」圖示。



程序檔工具會使用一般的程序檔語言 VBScript 或 JScript 之一，來建立包含觸發 (執行規則的時機) 和實際程序檔 (規則邏輯) 的規則。管理員不會受限於要執行的程序檔類型。

系統會連續執行進階程序檔 (與其他的完整性規則一起)。因此，長期執行的程序檔會停止其他規則 (包括定時規則) 的執行，直到完成程序檔爲止。

若要建立新的進階程序檔規則：

1. 在元件樹中的「*進階程序檔規則*」上按一下滑鼠右鍵，然後按一下「*新增新的程序檔規則*」。
2. 爲規則命名並進行描述 .
3. 指定觸發事件
   - **執行時間和日期：**指定執行程序檔的五個不同時間。系統會在選取的日期中每週執行一次。
   - **計時器執行依照：**指定執行計時器的頻率。

- **其他事件：**指定觸發程序檔的端點上事件。
- **位置變更事件：**指定觸發程序檔的位置變更事件。這些並非獨立的事件，而是附加於上一個事件。
  - **檢查位置事件：**程序檔會在所有的位置變更事件中執行。
  - **從來源位置切換時啓動：**只有當使用者離開 (指定的) 位置並移至其他位置時才會執行程序檔。
  - **切換至目標位置時啓動：**當使用者從其他位置進入指定的位置時會執行程序檔。如果在「*從來源位置切換時啓動*」指定位置參數時 (例如「辦公室」)，只有當位置從辦公室切換至指定的位置時才會執行程序檔。
  - **必須是手動變更：** 只有當使用者手動切換至位置 (或從其他位置切換) 時才執行程序檔。

4 建立任何程序檔變數。如需相關資訊，請參閱 「程序檔變數」(第 93 頁)。

5 撰寫程序檔文字。如需詳細資訊，請參閱 「程序檔文字」(第 94 頁)。

6 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

若要關聯現有的進階程序檔規則：

1 在元件樹中選取「*進階程序檔規則*」，然後按一下「*關聯新增*」。

2 從清單中選取所需規則。

3 如有必要，請重新定義觸發事件、變數或程序檔。

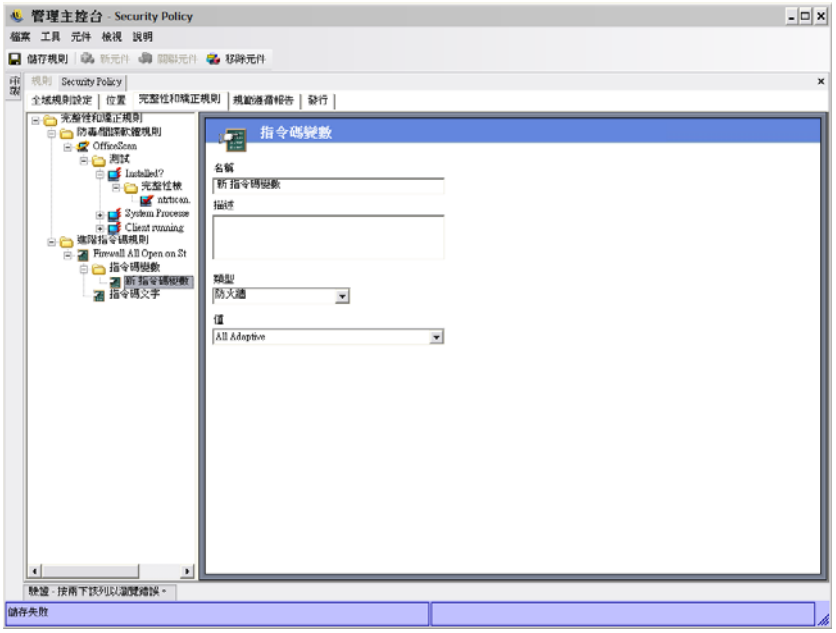
附註：變更共享元件中的設定將會影響相同元件的其他所有執行個體。使用「*顯示使用率*」指令來檢視與該元件相關聯的所有其他規則。

---

4 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

程序檔變數

此爲選擇性設定，可允許管理員針對程序檔定義變數 (var)，並且能夠使用 ZENworks Endpoint Security Management 功能 (例如，啓動已定義的自訂使用者訊息或超連結；切換至已定義的位置或防火牆設定)，或者不需變更程序檔本身便可隨意變更變數值。



若要建立新的程序檔變數：

1 在元件樹中的「*程序檔變數*」按一下滑鼠右鍵，然後按一下「*新增新的變數*」。

2 爲變數命名並進行描述 .

3 選取變數類型：

- **自訂使用者訊息**：定義可啓動爲動作的自訂使用者訊息。
- **防火牆**：定義可套用爲動作的防火牆設定。
- **超連結**：定義可啓動爲動作的超連結。
- **位置**：定義可套用爲動作的位置。
- **數字**：定義數值。
- **字串**：定義字串值。

4 指定變數的值：

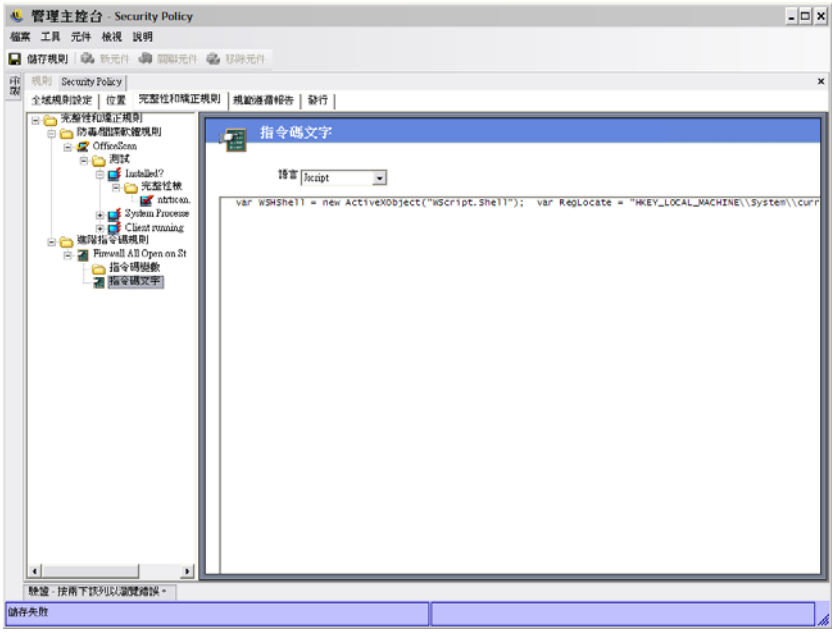
- 全部可調整
- 全部關閉
- 全部開啓
- 新防火牆設定
- 不符規範的完整性

5 按一下「*儲存規則*」。如果您的規則發生錯誤，請參閱 「錯誤通知」(第 99 頁)。

程序檔文字

系統並未限制 ZENworks Endpoint Security Management 管理員 ZENworks Security Client 可執行的程序檔類型。在配送規則之前可測試任何程序檔。

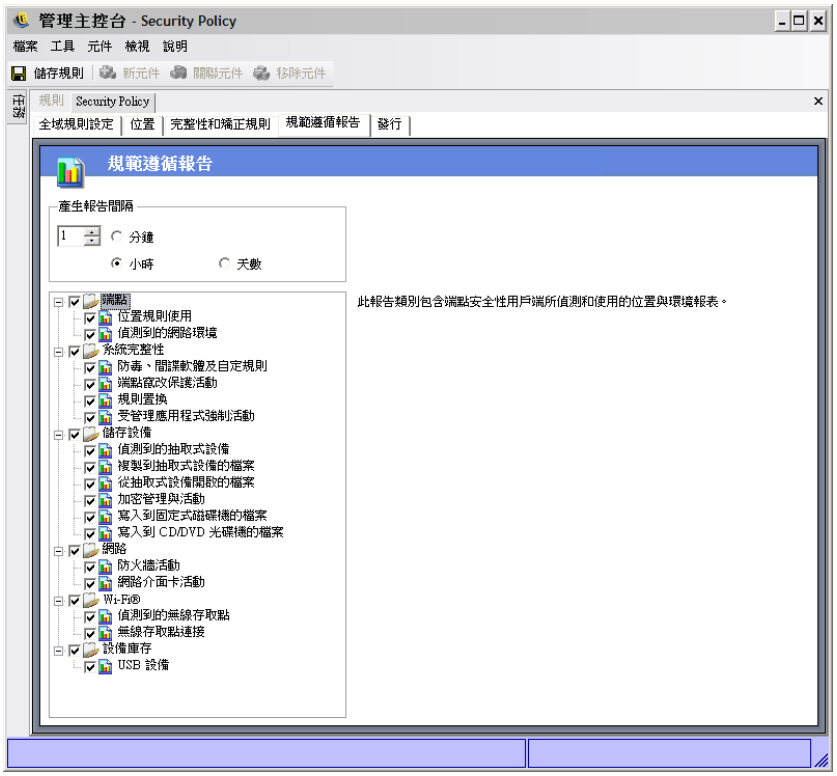
選取程序檔類型 (Jscript 或 VBscript)，並在欄位中提供程序檔文字。您可以從其他來源複製程序檔，並貼上至此欄位。



2.2.4 規範報告

因爲 ZENworks Security Client 驅動程式的層級和存取，所以實際上端點執行的每個交易都可納入報告。端點可以執行每個選擇性的系統清查，以用於疑難排解和規則建立等目的。若要存取這些報告，請按一下「*規範報告*」索引標籤。

附註：在執行「獨立式管理主控台」時，無法使用報告 .



若要執行此規則的規範報告：

1 指定產生報告的頻率。這是將資料從 ZENworks Security Client 上傳至「規則配送服務」的頻率。

2 勾選每個您要擷取的報告類別或類型。

下列是可用的報告：

端點

- **位置規則使用率：**ZENworks Security Client 將會報告強制執行的所有位置規則，以及該強制執行的持續期間。
- **偵測到的網路環境：**ZENworks Security Client 將會報告所有偵測到的網路環境設定。

系統完整性

- **防毒、間諜軟體及自訂規則：**ZENworks Security Client 將根據測試結果來報告已設定的完整性訊息。
- **防止端點被竄改的保護活動：**ZENworks Security Client 將報告任何竄改安全性用戶端的嘗試。
- **規則置換：**ZENworks Security Client 將報告所有在安全性用戶端上啟動管理置換的嘗試。
- **受管理的應用程式強制執行活動：**ZENworks Security Client 將報告受管理應用程式的所有強制執行活動。

儲存裝置

- **偵測到的抽取式設備：**ZENworks Security Client 將報告安全性用戶端偵測到的所有抽取式儲存設備。
- **複製到抽取式設備的檔案：**ZENworks Security Client 將報告複製到抽取式儲存設備的檔案。
- **從抽取式設備開啓的檔案：**ZENworks Security Client 將報告從抽取式儲存設備開啓的檔案。
- **加密管理和活動：**ZENworks Security Client 會使用 ZENworks 儲存設備加密解決方案報告加密 / 解密活動。
- **寫入固定磁碟機的檔案：**ZENworks Security Client 會報告寫入系統中固定磁碟機的檔案數。
- **寫入 CD/DVD 光碟機的檔案：**ZENworks Security Client 會報告寫入系統中 CD/DVD 光碟機的檔案數。

網路

- **防火牆活動 :** ZENworks Security Client 將報告由已針對套用之位置規則設定的防火牆所封鎖的所有流量。

  重要：啓用此報告，則可能會收集大量的資料。資料將非常快速地覆蓋整個資料庫。單一 ZENworks Security Client 的測試，報告在 20 個小時的期間內，有 1,115 筆封鎖的封包資料上載。您必須在進行大範圍部署之前，透過測試用戶端行監視和調整。

- **網路卡活動：**ZENworks Security Client 將報告受管理網路設備的所有流量活動。

Wi-Fi

- **偵測到的無線存取點：**ZENworks Security Client 將報告所有偵測到的存取點。
- **無線存取點連接：**ZENworks Security Client 將報告由端點進行的所有存取點連接。

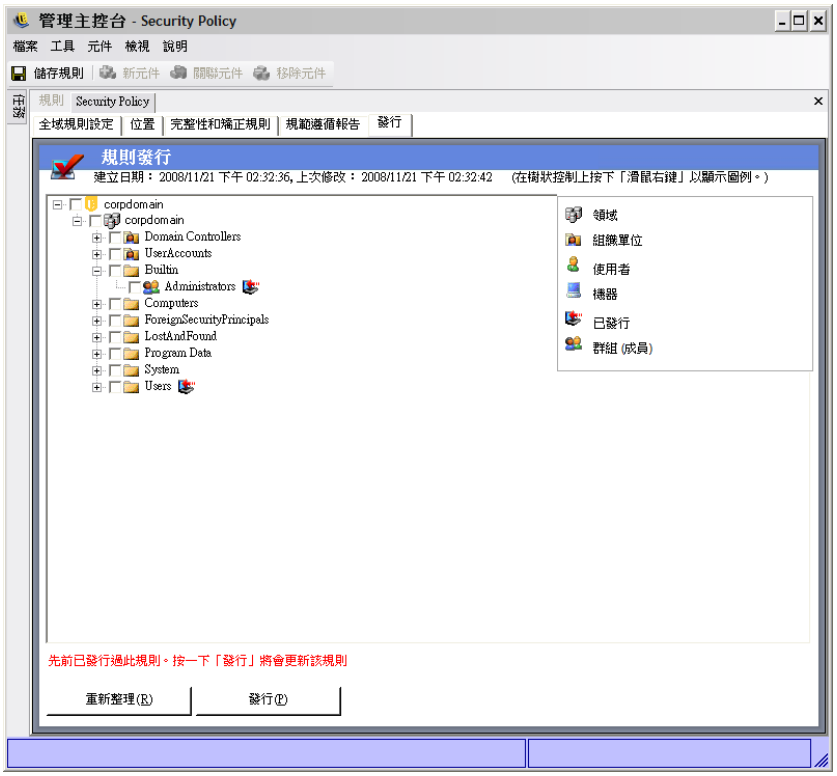
設備庫存

- **USB 設備：**ZENworks Security Client 將報告在系統中偵測到的所有 USB 設備。

2.2.5 發行

完成的安全性規則會透過發行機制傳送給使用者。規則發行之後，即可隨著收到更新的使用者，在其編程的登入期間，進一步更新。若要發行規則，請按一下「*發行*」索引標籤。下列資訊就會顯示：

- 目前目錄樹狀結構
- 規則的建立和修改日期
- 「*重新整理*」和「*發行*」按鈕



根據目前使用者的發行許可，目錄網路樹會以紅色來顯示一或多個選定的項目。系統將不允許使用者發行至以紅色顯示的任何使用者 / 群組。

在使用者及其關聯的群組驗證「管理服務」之前，都將不會顯示。公司目錄服務中的變更可能不會立即顯示於「管理主控台」中。*按一下「重新整理」，以更新「管理服務」的目錄網路樹*。

以下幾節中包含了更詳細的資訊：

- 「發行規則」(第 98 頁)
- 「更新發行的規則」(第 98 頁)

發行規則

1. 從左側的目錄網路樹，選取使用者群組 (或單一使用者)。按兩下使用者以進行選取 (若選取一個使用者群組，則會包含其中的所有使用者)。

   未收到規則的使用者將會在其名稱旁邊出現 圖示。如果使用者或群組已經收到規則，則在目錄網路樹中的名稱旁邊會出現 圖示。

   若要取消選取使用者或群組，可在其上連按兩下移除 圖示。
2. 按一下「*發行*」將規則傳送至「規則配送服務」。

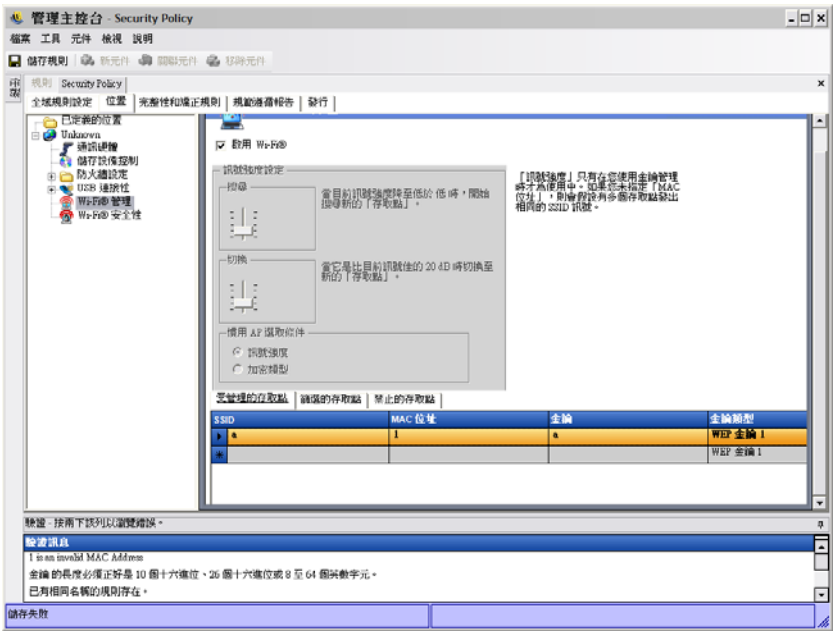
更新發行的規則

在將規則發行給使用者之後，您可以編輯規則中的元件並再次發行以維護簡易的更新。例如，如果 ZENworks Endpoint Security Management 管理員需要變更存取點的 WEP 金鑰，管理員只需要編輯金鑰、儲存規則，並按一下「*發行*」。受影響的使用者將會在其下一次登入時，收到更新的規則 (及新金鑰)。

2.2.6 錯誤通知

當管理員嘗試儲存規則時，若元件中的資料不完整或不正確，「管理主控台」下方將會顯示一個 「驗證」窗格，並反白每個錯誤。您必須修正這些錯誤後才能儲存規則。

在每個驗證列上連按兩下以瀏覽出現錯誤的畫面。錯誤會反白如下圖所示 。

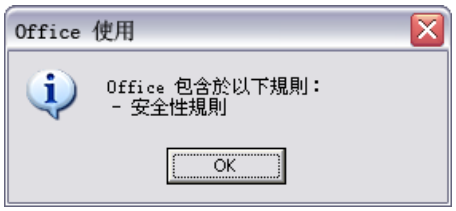


2.2.7 顯示使用率

變更共享的規則元件將會影響與其相關聯的所有規則。在更新或變更規則元件之前，您必須執行 「*顯示使用率*」指令以決定會受到變更影響的規則。

1 在元件上按一下滑鼠右鍵，然後按一下 「*顯示使用率*」。

會出現一個快顯視窗，顯示該元件在其他規則中的每個執行個體。



2.3 輸入及輸出規則

以下幾節中包含了更詳細的資訊：

- 「輸入規則」(第 100 頁)
- 「輸出規則」(第 100 頁)
- 「將規則輸出至不受管理的使用者」(第 100 頁)

2.3.1 輸入規則

規則可從可用網路上的任意檔案位置中輸入。

1. 在管理主控台中，按一下「*檔案*」>「*輸入規則*」。

   如果您目前正在編輯或草擬規則，則在開啓輸入視窗前，編輯程式將會關閉規則 (會提示您加以儲存)。
2. 瀏覽並指定檔案位置，然後在欄位中指定檔案名稱。

在輸入規則之後，即可進一步加以編輯，或者立即發行。

2.3.2 輸出規則

您可以從「管理主控台」輸出規則，並透過電子郵件或網路共享進行配送。這可在已佈署多個「管理服務」和「規則編輯器」的環境中，用來配送企業層級的規則。

若要輸出安全性規則：

1. 在管理主控台中，按一下「*檔案*」>「*輸出*」。
2. 指定目的地並提供副檔名爲 .sen 的規則名稱 (例如，C:\Desktop\salespolicy.sen)，您可以按一下瀏覽按鈕以瀏覽位置。
3. 按一下「*輸出*」。

已輸出兩個檔案。第一個檔案爲規則 (*.sen 檔)。第二個是必須在輸入時用來將規則解密的 setup.sen 檔案。

輸出的規則必須輸入至「管理主控台」，才能發行至受管理的使用者。

2.3.3 將規則輸出至不受管理的使用者

如果不受管理的 ZENworks Security Client 已部署在企業中，則必須安裝獨立的管理主控台以建立規則。請參閱《“ZENworks Endpoint Security Management 安裝指南”》取得詳細資料。

若要配送不受管理的規則：

1. 尋找「管理主控台」的 setup.sen 檔案，並將之複製到個別資料夾。

   setup.sen 檔案會在安裝「管理主控台」時產生，並置於 \Program Files\Novell\ESM Management Console 目錄。
2. 在「管理主控台」中建立規則。如需詳細資訊，請參閱 「建立安全性規則」(第 45 頁)。
3. 使用「*輸出*」指令將規則輸出至包含 setup.sen 檔案的相同資料夾。

   所有配送的規則都必須命名爲 policy.sen，使 ZENworks Security Client 能夠接受這些規則。
4. 配送 policy.sen 和 setup.sen 檔案。這些檔案必須複製到所有不受管理用戶端的 \Program Files\Novell\ZENworks Security Client 目錄中。

您必須使用第一個規則將 setup.sen 檔案複製到不受管理的 ZENworks Security Client (只能複製一次)。之後只需要配送新的規則。