AUTHORIZED DOCUMENTATION

Endpoint Security Client 4.0 使用者指南

December 22, 2008

Novell®
ZENworks® Endpoint Security Management

4.0

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。

Copyright © 2007-2008 Novell, Inc. 版權所有。在未獲得發行者的書面同意前，不得對本出版品的任何部分進行任何重製、影印、儲存於檢索系統或進行傳輸動作。

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

關於本指南

本 *《Novell® ZENworks® Endpoint Security Client 4.0 使用者指南》*可指導最終使用者進行 Endpoint Security Client 4.0 for Microsoft Windows* Vista* 與 Windows Server 2008* 的操作。

本指南中的資訊是以下列方式編排：

- 第 1 章 「介紹」(第 9 頁)
- 第 2 章 「Endpoint Security Client 4.0 綜覽」(第 11 頁)
- 第 3 章 「使用 Endpoint Security Client 4.0」(第 15 頁)

使用對象

本指南可傳送給企業中的所有員工，以協助他們瞭解如何使用 Endpoint Security Client。

意見反應

我們希望得到您對本手冊以及本產品隨附之其他文件的意見和建議。您可以使用線上文件各頁底部的「使用者意見」功能，或造訪 Novell 文件的意見反應網站 (http://www.novell.com/documentation/feedback.html)，寫下您的意見。

其他文件

此外，您還可以透過 ZENworks Endpoint Security Management 的其他支援文件 (包括 PDF 與 HTML 格式)，來瞭解本產品並加以實作。如需更多文件，請參閱 ZENworks Endpoint Security Management 3.5 文件網站 (http://www.novell.com/documentation/zesm35)。

文件慣例

在 Novell 文件中，大於符號 (>) 是用來分隔步驟中的動作，以及交互參照路徑中的項目。

商標符號 (®、™ 等) 表示 Novell 的商標。標註星號 (*) 者，代表協力廠商的商標。

雖然在寫入單一路徑名稱時，有些平台採用反斜線，其他平台採用正斜線，但在本文中，路徑名稱一律使用反斜線。要求使用正斜線之平台 (例如 Linux*) 的使用者，應依據軟體的要求使用正斜線。

介紹

1

Novell® ZENworks® Endpoint Security Client 4.0 是可支援以 32 位元模式執行之 Microsoft Windows Vista (含 Support Pack 1) 與 Windows Server 2008 的用戶端版本。Endpoint Security Client 4.0 使用 ZENworks Endpoint Security Management 3.5 Server 與管理主控台。

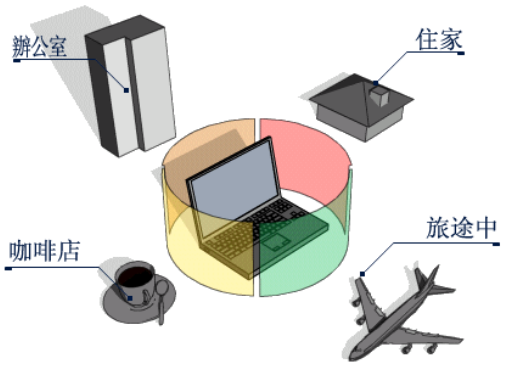
Novell ZENworks Endpoint Security Management (ESM) 的設計可透過稱爲 ZENworks Security Client 的中央管理工具來保護公司的資料資產。ZENworks Endpoint Security Client 4.0 是安裝在 Windows Vista 與 Windows Server 2008 企業電腦上，並強制執行透過 ESM 管理和配送系統撰寫與傳送的安全性規則。這可讓大小企業在公司安全性周邊內部與外部的電腦上建立、部署、強制執行和監看電腦安全性規則。

以下幾節包含其他資訊：

1.1 行動電腦的安全性強制執行

安全性會在全域上和依照網路位置強制執行。安全性規則中所列出的的每個位置都可決定該網路環境的使用者許可，以及要啓動何種防火牆設定。防火牆設定會決定要將網路存取權限授予哪一個網路連接埠、網路位址以及應用程式，並決定許可該存取的方式。

圖 1-1 ESM 會根據偵測到的網路環境調整安全性設定。

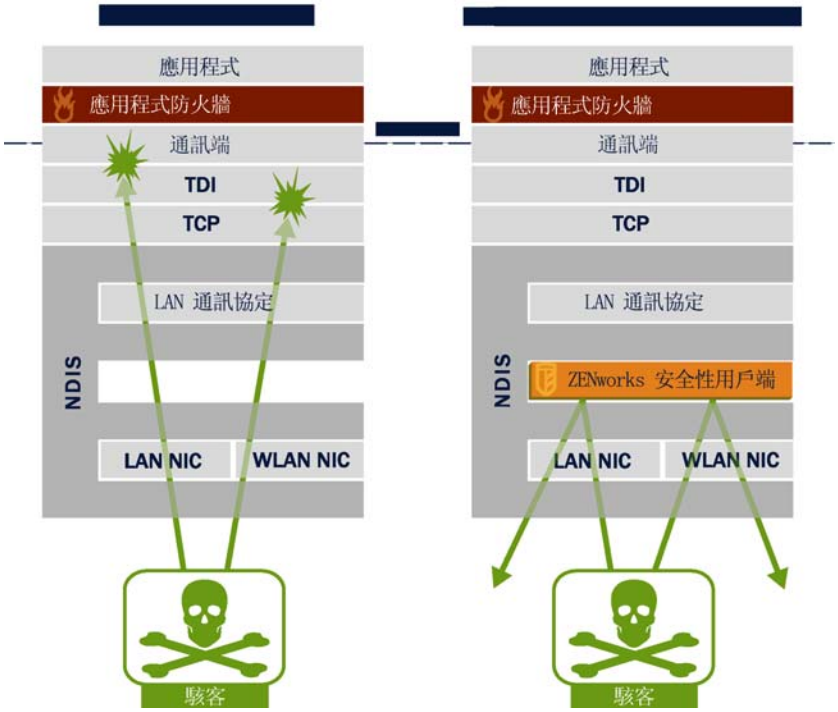


在定義網路環境之後，使用者是不會察覺 Endpoint Security Client 4.0 的一般運作的。有時候 Endpoint Security Client 4.0 保護機制會中斷一般操作，當發生此情況時，系統會顯示訊息和超連結以通知使用者相關的安全性規則、已採取的保護步驟，並提供額外的資訊以協助修正該問題。

1.2 NDIS 層防火牆保護

在保護行動裝置時，ESM 會優於僅在應用程式層運作、或以 Firewall-Hook 驅動程式運作的一般個人防火牆技術。ESM 用戶端安全性已整合至每張網路介面卡 (NIC) 的 Network Driver Interface Specification (NDIS) 驅動程式中，並且可以在流量進入電腦時便開始提供安全性保護。特性 1-2, 「NDIS 層防火牆的效用」, 第 10 頁 顯示了 ESM 與應用程式層防火牆和篩選器驅動程式之間的差異。

圖 1-2 *NDIS 層防火牆的效用*



當安全性實作以通訊協定堆疊的最低適用層級運作時，安全性決定和系統效能將可獲得最佳化。透過 Endpoint Security Client 4.0，系統會使用 Adaptive Port Blocking (可設定狀態的封包檢查) 技術，在 NDIS 驅動程式堆疊的最低層級捨棄來路不明的流量。此方法可防止以通訊協定爲基礎的攻擊，包括未經授權的連接埠掃描、SYN 流量攻擊以及其他方式的攻擊。

我們建議您遵循此文件所提出的所有操作和維護建議，以確保端點安全性環境可獲得保障。

Endpoint Security Client 4.0 綜覽

2

無論在家裡、工作場所，或者出外旅行時，ZENworks® Security Client 都能透過強制執行由企業 Endpoint Security Management (ESM) 管理員所建立的安全性規則，保護電腦的資料不會遭到入侵。當筆記型電腦使用者從公司網路移至家庭網路，或者在外出時登入公共或開放網路時，系統會自動調整指定給個別位置的防火牆設定。

安全性層級會套用至各種使用者位置，而使用者並不需要具備與網路安全性、連接埠組態、隱藏的共用檔案或其他技術詳細資料的專業技巧或知識。即時取得可用位置與規則的相關資訊，只要將滑鼠移到工作列圖示上就可以檢視 Endpoint Security Client 工具提示 (請參閱圖 2-1)。

圖 2-1 *Endpoint Security Client 工具提示*

以下幾節包含其他資訊：

- 「ESM 術語」(第 11 頁)
- 「登入 Endpoint Security Client 4.0」(第 12 頁)

2.1 ESM 術語

本文件中經常使用以下術語：

位置：位置是一種簡單的定義，可協助使用者識別其所在的網路環境、提供即時的安全性設定 (由管理員定義)、允許使用者儲存環境並變更已套用的防火牆設定。

每個位置都會獲得唯一的安全性設定，以在較有威脅性的環境中拒絕某些對於網路功能和硬體的存取，並且在受信任的環境中允許較廣泛的存取。位置會定義以下資訊：

- Endpoint Security Client 在此位置上多久檢查一次規則更新
- 授予使用者的位置管理許可
- 在此位置上使用的防火牆設定
- 允許進行連接的通訊硬體
- 允許使用者使用抽取式儲存裝置 (例如，隨身碟或記憶卡) 和使用 CD/DVD-RW 磁碟機的層級
- 可協助定義位置的任何網路環境

防火牆設定：防火牆設定可控制所有網路連接埠 (1-65535)、網路封包 (ICMP、ARP 等)、網路位址 (IP 或 MAC) 的連接性，以及允許哪些網路應用程式 (檔案共享、即時通訊軟體等) 可在套用設定後取得網路連接。ESM 依預設包含三種防火牆設定，並可在位置上進行實作。ESM 管理員也可建立特定防火牆設定 (無法在此列出)。

- **All Adaptive (全部可調整)：**此防火牆設定會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，並允許所有外傳網路流量)。允許 ARP 和 802.1x 封包，並允許所有網路應用程式的網路連接。
- **All Open (所有開啓的)：**此防火牆設定會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)：**此防火牆設定會關閉所有網路連接埠，並限制所有封包類型。

介面卡：表示端點上常用的三種通訊介面卡：

- 有線介面卡 (LAN 連接)
- Wi-Fi 介面卡 (PCMCIA Wi-Fi 網路卡和內建 Wi-Fi)

亦表示電腦中所包含的其他通訊硬體，例如紅外線、藍牙 *、FireWire* 以及序列和平行連接埠。

儲存裝置：表示當您將資料複製至儲存裝置 (或從中讀取資料) 時，可能造成安全性威脅的外接式儲存裝置。USB 隨身碟、快閃記憶卡和 SCSI PCMCIA 記憶卡，以及傳統的 Zip* 磁碟機、軟碟機、外接式 CDR 光碟機和安裝的 CD/DVD 光碟機 (包括 CD-ROM、CD-R/RW、DVD、DVD R/RW) 全都可在單一位置上設定爲封鎖、許可或者唯讀。

網路環境：網路環境是一種網路服務與識別網路位置所需之服務位址的集合。

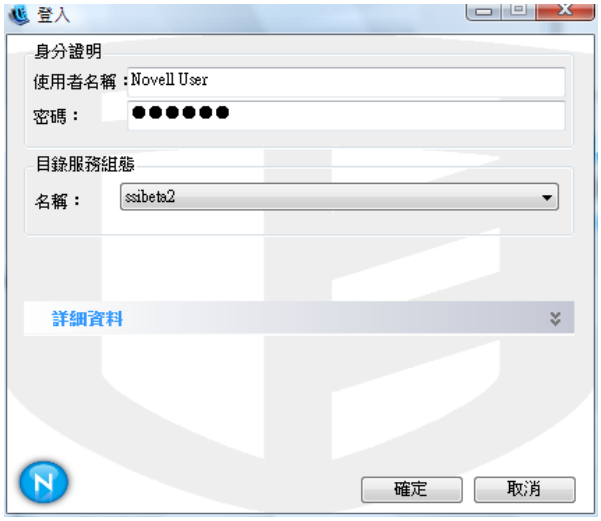
2.2 登入 Endpoint Security Client 4.0

如果您是公司 Active Directory 領域的成員，Endpoint Security Client 4.0 將使用您的 Windows* 使用者名稱和密碼登入「規則配送服務」(不會顯示任何快顯視窗)。如果您是 Novell eDirectory 網路樹的成員，Endpoint Security Client 4.0 會提示您輸入網路樹的使用者名稱和密碼 (請參閱圖 2-2)。

附註：搭配 Novell eDirectory 使用時，安裝 Endpoint Security Client 4.0 之後使用者會看到快顯登入視窗。這可讓您提供網路樹的使用者名稱和密碼。

如果您不是代管「規則配送服務」領域中的成員，Endpoint Security Client 4.0 將會提示您輸入該領域的使用者名稱和密碼 (請參閱圖 2-2)。

圖 2-2 *Endpoint Security Client 4.0 登入*



輸入網域或 eDirecic4tory 網路樹的使用者名稱和密碼，然後按一下「*確定*」。

「目錄服務組態名稱」必須符合您要向其驗證身分的目錄服務。使用下拉式功能表檢視是否有多個服務可用。

附註：當 Endpoint Security Client 是以獨立模式執行時，您將不需要登入 Endpoint Security Client。ESM 管理員會使用不同方式將規則分派給獨立的使用者。

使用 Endpoint Security Client 4.0

3

以下各節包含的資訊是關於您使用 Novell® ZENworks® Endpoint Security 最終使用者應用程式 (Endpoint Security Client 4.0) 所能執行的動作：

附註：管理員可在任何位置上限制上面列出的動作。

3.1 在網路環境之間移動

最終使用者所經歷的每個網路，可能都需要不同的安全性機制。在由可用的網路連接所識別的位置中，Endpoint Security Client 4.0 都能提供安全保障與保護。Endpoint Security Client 4.0 可偵測網路環境參數並切換至適當的位置，然後根據目前的安全性規則套用需要的保護層級。

網路環境資訊已儲存或預先設定於位置中。這可讓 Endpoint Security Client 4.0 在偵測到環境參數時自動切換至位置。

- **儲存的環境：**由使用者定義 (請參閱 「儲存網路環境」(第 16 頁))。
- **預先設定的環境：**由企業 ESM 管理員經由已發佈的安全性規則進行定義。

當使用者進入新的網路環境時，用戶端會將偵測到的網路環境與安全性規則中任何已儲存或預先設定的值進行比對。若發現符合的項目，Endpoint Security Client 4.0 將會啓動指定的位置。當偵測到的環境無法識別爲已儲存或預先設定的環境時，用戶端會啓動預設的 「不明」位置。

「不明」的位置將包含以下預設值：

- 變更位置 = 允許
- 變更防火牆設定 = 不允許
- 儲存位置 = 不允許
- 更新規則 = 允許
- 預設防火牆設定 = 所有開啓的

根據預設，「不明」位置允許所有介面卡類型 (有線、Wi-Fi 與數據機)。這可讓電腦其周邊網路環境互動，並嘗試與上述之位置規則產生關聯。

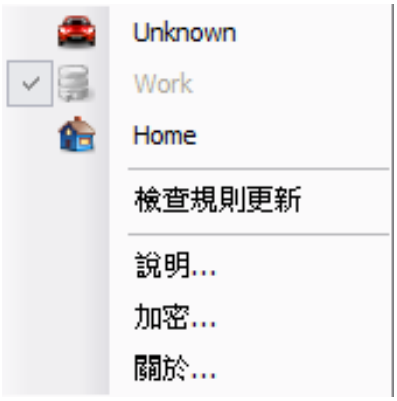
3.2 變更位置

在啓動時，Endpoint Security Client 4.0 將切換至「不明」的位置。然後它將會嘗試偵測目前的網路環境，並自動變更位置。如果網路環境無法辨識或沒有預設值，則必須手動變更位置。

如果您無法執行以下步驟，可能是 ZENworks Endpoint Security 管理員已禁止您手動變更位置。

若要變更位置：

1 在工作列中的「*Endpoint Security Client 4.0*」圖示上按一下滑鼠右鍵，以顯示選項的功能表。



2 按一下適當的位置。

3.2.1 儲存網路環境

網路環境必須先在安全性規則中完成預先設定，或者由最終使用者儲存後，Endpoint Security Client 4.0 才能自動變更位置。儲存網路環境會將網路參數儲存至目前的位置，並允許 Endpoint Security Client 4.0 在下次使用者進入網路環境時自動切換至該位置。當套用至 Wi-Fi 網路環境時，Endpoint Security Client 4.0 將 LockOn™ (鎖定) 至已選取的單一存取點。

若要儲存環境：

1 在工作列中的「*Endpoint Security Client 4.0*」圖示上按一下滑鼠右鍵以顯示功能表。

2 按一下您所要變更至的位置。

3 在「*Endpoint Security Client 4.0*」圖示上按一下滑鼠右鍵，並將滑鼠移至目前位置上方以顯示子功能表，然後按一下「儲存網路環境」以儲存環境。

如果此網路環境已儲存在之前的位置中，Endpoint Security Client 4.0 將會詢問使用者是否要儲存新的位置。選擇「*是*」將環境儲存至目前的位置並清除其先前位置中的環境，或選擇「*否*」將環境留在先前位置中。

附註：ESM 管理員可在任何位置上限制「*儲存網路環境*」功能。

您可將其他的網路環境儲存至位置中。例如，如果定義爲「機場」的位置是目前規則的一部分，行動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，當行動使用者返回至儲存的機場環境時，Endpoint Security Client 4.0 都會自動切換至「機場」位置。

3.2.2 儲存 Wi-Fi 環境

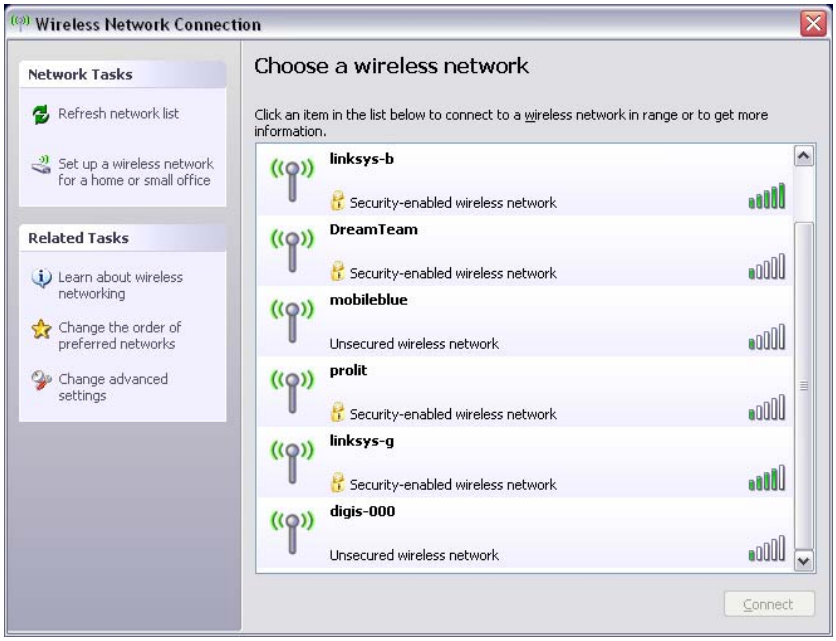
當使用者啓動 Wi-Fi 介面卡時，他們可能會看到許多可用的存取點。Wi-Fi 介面卡通常會先鎖定在單一存取點上，但如果介面卡鄰近範圍內存在太多存取點時，則可能會中斷已連接的存取點，無線連接管理員也會提示介面卡切換至訊號最強的存取點。當發生此情況時，目前的網路活動將會中止；使用者通常會被強制重新傳送某些封包，並將 VPN 重新連接至公司網路。

如果將存取點儲存爲位置上的網路環境參數，使用者在實際離開存取點前，介面卡將鎖定至該存取點且不會失去連接。回到存取點時，介面卡將自動建立與存取點的關聯，位置也會改變，在無線連接管理軟體中也不會再出現所有其他的存取點。

若要儲存 Wi-Fi 環境：

1 開啓連線管理軟體並選取想要的存取點。

附註：當您設定使用 ESM 安全性規則來管理無線連接性時，可使用位置來置換連線管理軟體。



2 指定任何必要的安全性資訊 (WEP 或其他安全性金鑰)，並按一下「*連接*」。

3 完成在 「儲存網路環境」(第 16 頁) 列出的步驟以儲存此環境。

3.2.3 移除儲存的環境

若要從位置中移除儲存的環境：

1. 在工作列中的「*Endpoint Security Client*」圖示上按一下滑鼠右鍵以顯示功能表。
2. 變更至適當的位置。
3. 在「*Endpoint Security Client*」圖示上按一下滑鼠右鍵，然後選取目前的位置以顯示子功能表。
4. 按一下「*清除網路環境*」以清除環境。

附註：這將會清除此位置中所有已儲存的網路環境。

3.3 資料加密

當由規則所啓用時，Endpoint Security Client 4.0 會管理位於端點上特定目錄以及位於抽取式儲存裝置中的檔案加密。

以下指示將協助您在端點上使用 ZENworks Endpoint Security。

- 「管理非系統卷冊上的檔案」(第 18 頁)
- 「管理抽取式儲存設備中的檔案」(第 18 頁)

3.3.1 管理非系統卷冊上的檔案

安裝在電腦中的所有非系統卷冊磁碟機，以及硬碟機中的任何分割區都可定義爲「固定磁碟」。端點上的每個固定磁碟都有「安全庇護」資料夾 (根據預設，此資料夾名稱爲「加密的檔案」)，而且存在於每個非系統卷冊或磁碟機的根目錄。位於此資料夾中的所有檔案都會透過目前的加密金鑰進行加密。只有電腦上的已授權使用者才能解密這些檔案。

當您儲存檔案時，請在目標磁碟機的可用資料夾中選取「安全庇護」資料夾。

3.3.2 管理抽取式儲存設備中的檔案

「抽取式儲存設備」定義爲「連接」至電腦的任何儲存設備。這包括 (但不限於) USB 隨身碟、快閃記憶卡、PCMCIA 記憶卡，以及傳統的 Zip 磁碟機、軟碟機、外接式 CDR 光碟機、具備儲存空間的數位相機和 MP3 播放器。

當您執行 ZENworks Endpoint Security 時，儲存在這些設備中的檔案將會在作業系統或使用者存取時進行加密。複製至設備中的檔案將會立即加密。當抽取式儲存設備連接至未受 ZENworks Endpoint Security 系統管理的電腦時，這些檔案將維持加密狀態且無法解密。

抽取式儲存設備的加密會在插入設備時進行 (請參閱 「如果我不想加密設備時該怎麼做？」(第 20 頁))。不過，當您將檔案新增至其他機器上的已加密抽取式儲存設備時，這些檔案將不會加密，您必須手動將其加密。

以下幾節中包含了更詳細的資訊：

- 「加密檔案」(第 19 頁)
- 「如果我不想加密設備時該怎麼做？」(第 20 頁)

- 「使用共享檔案資料夾」(第 20 頁)
- 「爲共享檔案資料夾中的檔案變更密碼」(第 21 頁)

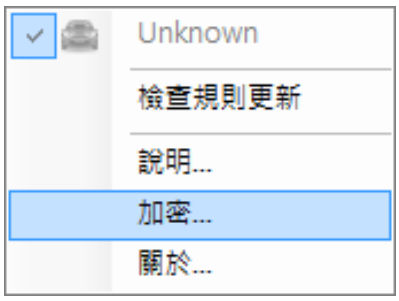
加密檔案

若要加密在抽取式儲存設備中新增的檔案：

1 將儲存設備插入電腦上適當的連接埠。

2 在工作列中的「*Endpoint Security Client*」圖示上按一下滑鼠右鍵。

3 在功能表中選取「*加密*」。



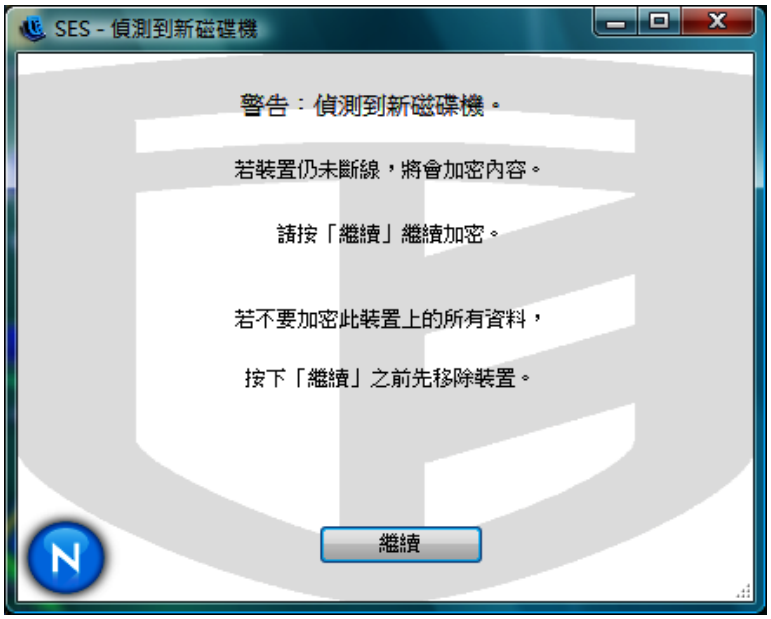
4 按一下「*加密 RSD*」。這將會使用目前的加密金鑰將抽取式儲存設備上的所有檔案加密。

加密檔案所需的時間將視儲存在設備中的資料數量而定。

如果我不想加密設備時該怎麼做？

當您插入抽取式儲存裝置時，Endpoint Security Client 將提示您是否要加密磁碟機，或者要將其移除且不加密所有檔案。

圖 3-1 插入新設備時的加密警告



警告：若要防止加密，請在按一下「*繼續*」之前先移除磁碟機。按一下「*繼續*」以加密磁碟機，或者在移除設備後關閉視窗。

使用共享檔案資料夾

當規則允許時，在執行 ZENworks Endpoint Security 的電腦中，其所附加的任何抽取式儲存設備中都會建立一個「共享檔案」資料夾。其他規則群組中的使用者可透過由使用者建立的密碼來存取此資料夾中的檔案。未執行 ZENworks Endpoint Security 的使用者可使用 ZENworks File Decryption 公用程式並輸入密碼來存取這些檔案。如需 ZENworks File Decryption 公用程式的詳細資訊，請聯絡 Novell 支援。

附註：每次重新開機時都會清除密碼。在重新開機後，新增至「共享檔案」資料夾的檔案都會被提示輸入密碼。

若要使用「共享檔案」資料夾。

1. 將檔案移動或儲存至「共享檔案」資料夾。
2. 在出現密碼提示時，輸入密碼和確認密碼。
3. 輸入密碼的提示。

未受規則管理的 ZENworks Endpoint Security 使用者可輸入密碼來存取這些檔案。未受 ZENworks Endpoint Security 管理的使用者將需要 ZENworks File Decryption Utility 與密碼來存取檔案。

爲共享檔案資料夾中的檔案變更密碼

您可以使用加密控制爲新增至 「共享檔案」資料夾中的檔案變更密碼。

附註：這將不會變更任何現有的密碼，而只會變更未來檔案的密碼。

若要變更密碼：

1. 將儲存設備插入電腦上適當的連接埠。
2. 在工作列中的 「*Endpoint Security Client*」圖示上按一下滑鼠右鍵。
3. 在功能表中選取 「*加密*」。
4. 按一下 「*清除密碼*」。

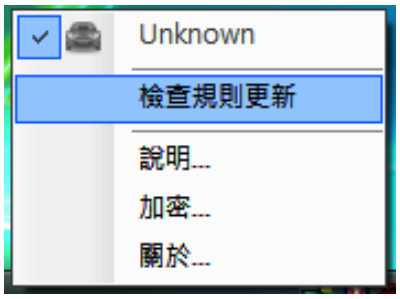
5. 將檔案拖曳至 「共享檔案」資料夾並輸入新密碼和提示。

所有新增至資料夾的新檔案都需要新密碼進行存取。

3.4 更新規則

新的安全性規則會在發佈時傳送給受管理的使用者。Endpoint Security Client 會依照 ESM 管理員所決定的間隔自動接收更新。但是，受管理的使用者可以隨時檢查規則更新 (如果規則允許)。

1. 在工作列中的 「*Endpoint Security Client*」圖示上按一下滑鼠右鍵以顯示功能表。
2. 按一下 「*檢查規則更新*」。

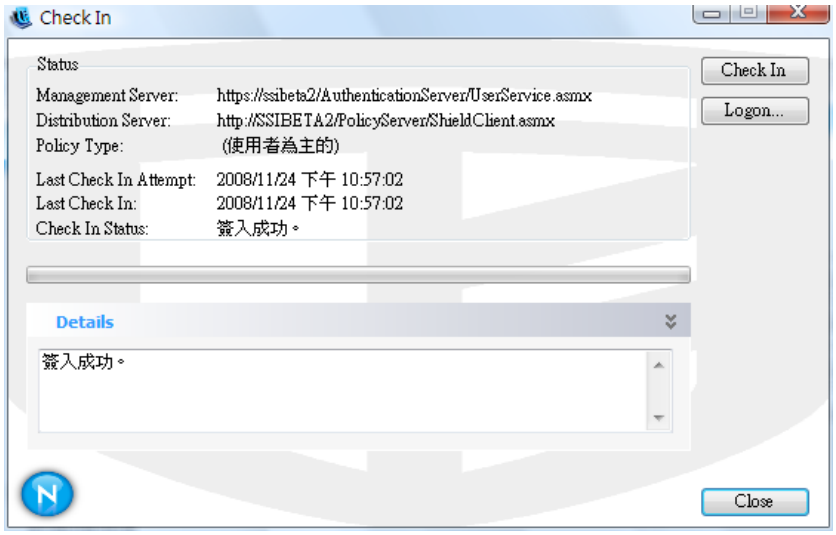


附註：當 Endpoint Security Client 是以獨立模式執行時，「自動更新」與「檢查規則更新」功能將無法使用。ESM 管理員會使用不同方式將規則更新分派給這些使用者。

當規則更新時，Endpoint Security Client 會通知您。

如果您的 ZENworks Endpoint Security 管理員允許，您也可以手動簽入。

1. 在工作列上的「*Endpoint Security Client*」圖示上按一下滑鼠右鍵以顯示功能表然後按一下「*關於*」，或連按兩下「*Endpoint Security Client*」圖示。
2. 按一下「*簽入*」。



如果沒有權限可以執行簽入，則「*簽入*」按鈕會呈現灰色。

「簽入」視窗會顯示簽入程序的目前狀態。它會顯示管理與配送伺服器 (如果這是受管理的用戶端)、規則類型、上次嘗試簽入時間與上次成功簽入時間，以及簽入狀態。

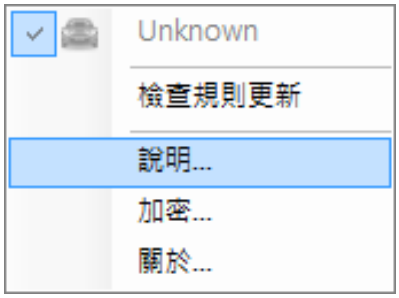
3. 如果要執行手動簽入，請按一下「*手動簽入*」按鈕。「簽入」視窗中的資訊會對應地更新。

「*登入*」按鈕可讓您登入「規則配送服務」。如需詳細資料，請參閱「登入 Endpoint Security Client 4.0」(第 12 頁)。

3.5 檢視說明

1 在工作列中的「*Endpoint Security Client*」圖示上按一下滑鼠右鍵以顯示功能表。

2 按一下「*說明*」。



3.6 置換密碼

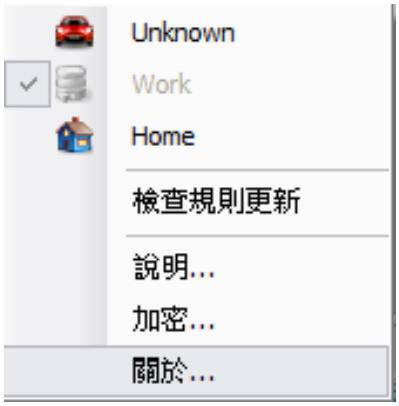
強制執行 Endpoint Security Client 4.0 安全性規則可能對連接性、軟體或隨身碟造成限制，並可能對使用者的生產力造成中斷。變更位置或防火牆設定通常可以解除這些限制，並恢復已中斷的功能。不過在某些情況中，限制的執行可能會影響所有位置和防火牆設定。此時您必須暫時解除這些限制才能繼續進行原來的操作。

Endpoint Security Client 4.0 提供的「密碼置換」功能可暫時停用目前的安全性規則以允許必要的活動。「安全性管理員」僅於必要時分派只使用一次的密碼金鑰，並獲悉與安全性規則有關的任何問題。密碼金鑰的時間限制 (由管理員所設定) 過期後，就會還原保護端點的安全性規則。將端點重新開機也可以還原安全性設定。

若要啓動密碼置換：

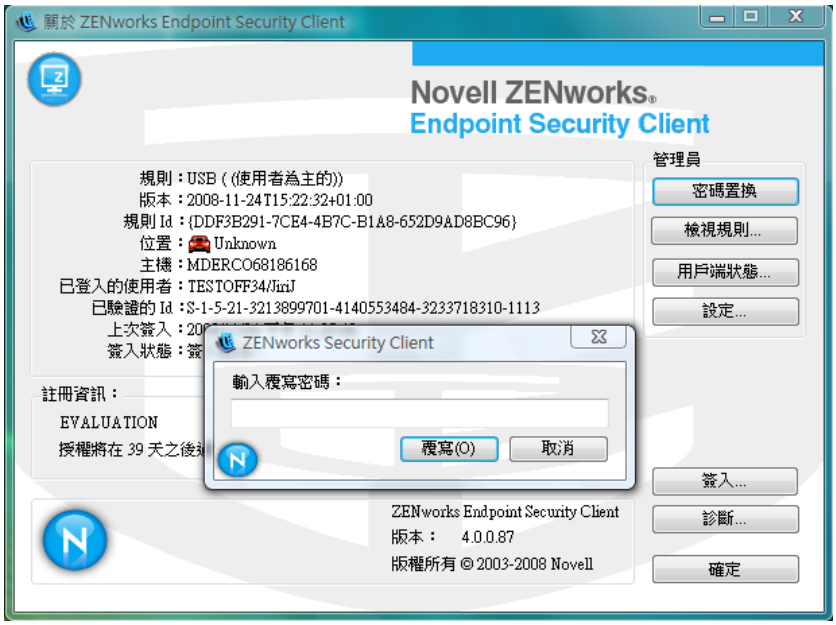
1 聯絡公司的 ESM 管理員以取得密碼金鑰

2 在工作列上的「*Endpoint Security Client*」圖示上按一下滑鼠右鍵以顯示功能表然後按一下「*關於*」，或連按兩下「*Endpoint Security Client*」圖示。



3 按一下「*密碼置換*」以顯示密碼視窗。

附註：如果畫面中未顯示「*密碼置換*」按鈕，表示您目前的規則中並沒有密碼置換功能。



4 鍵入 ZENworks Endpoint Security 管理員所提供的密碼鑰。

5 按一下 「*確定*」。在指定的時間內，目前的規則會由預設 「所有開啓的」的規則所取代。

按一下 「*關於*」視窗中的 「*載入規則*」(取代 「*密碼置換*」按鈕) 將可還原之前的規則。如果管理員已更新您的規則來解決現有的問題，您應另行使用 「*檢查規則更新*」來下載新規則。

警告：永遠不會置換加密服務。

3.7 診斷

Novell 已提供診斷工具，使管理員可進行各種 Endpoint Security Client 問題的疑難排解。ZENworks Endpoint Security 管理員將引導您逐步完成診斷程序。如果有進一步的問題，請聯絡 Novell 支援。

您可能會被要求提供診斷套件。ZENworks Endpoint Security 管理員會告訴您必須在其中納入哪些資訊。若要建立診斷套件：

1 在工作列上的 「*Endpoint Security Client*」圖示上按一下滑鼠右鍵以顯示功能表然後按一下 「*關於*」，或連按兩下 「*Endpoint Security Client*」圖示。

2 按一下 「*診斷*」按鈕。

3 檢查「診斷套件」面板中的所有資訊，或只檢查您的 ZENworks Endpoint Security 管理員所要求的項目，然後按一下「*建立套件*」。

ZENworks Endpoint Security 用戶端會在您的桌面上建立 zesmdiagnostics*.enc 檔案，您可以將這個檔案傳送給您的 ZENworks Endpoint Security 管理員。